MailChimp reagiert auf Schrems II mit einer **Anpassung des Auftragsverarbeitungs-vertrages**.

Der US-amerikanische Newsletter-Dienstleister "**MailChimp**" hat auf die Schrems-II - Entscheidung (EuGH C 311/18 16.7.2020) nun mit einer Anpassung des Data Processing Agreements reagiert.

Bis zum 16.7.2020 hat sich MailChimp im Empfang von personenbezogenen Daten aus EU auf das EU-US-Privacy Shield gestützt. Nun ist die Auftragsverarbeitungsvereinbarung in der Form abgeändert, dass die S**tandard-Datenschutz(vertrags)klauseln** einbezogen werden.

Es sind - nach der Schrems II - Entscheidung - auch **weitere Maßnahmen** zwischen den Vertragsteilen zu treffen, um ein angemessenes Datenschutzniveau in den USA erreichen zu können.

Auch hier hat sich MailChimp etwas "einfallen" lassen, und zwar
eine **Informationspflicht** gegenüber seinen Kunden **bei einem Zugriff von Behörden auf die Daten bei Konten,** von denen MailChimp davon ausgehen kann, dass es sich um **europäische Kunden** handelt.

Hier eine Übersetzung aus dem Addendum zum DPA:

Government data access requests (MailChimp Addendum to the Data Processing Agreement)	Übersetzung des Absatzes bezüglich **Anfragen der Regierung zum Zugriff auf Daten** (MailChimp Addendum zum Data Processing Agreement.
As a matter of general practice, Mailchimp does not voluntarily provide government agencies or authorities (including law enforcement) with access to or information about Mailchimp accounts (including Customer Data).	In der Regel gibt Mailchimp Regierungsbehörden oder Behörden (einschließlich Strafverfolgungs-behörden) nicht freiwillig Zugang zu oder Informationen über Mailchimp-Konten (einschließlich Kundendaten).
If Mailchimp receives a compulsory request (whether through a subpoena, court order, search warrant, or other valid legal process) from any government agency or authority	Wenn Mailchimp von einer Regierungsbehörde oder sonstigen Behörde (einschließlich Strafverfolgungsbehörden) eine verpflichtende Aufforderung (sei es

(including law enforcement) for access to or information about a Mailchimp account (including Customer Data) belonging to a Customer whose primary contact information indicates the Customer is located in Europe, Mailchimp shall:	durch Vorladung, Gerichtsbeschluss, Durchsuchungsbefehl oder ein anderes gültiges Mittel) für einen Zugriff auf oder zu Informationen über ein Mailchimp-Konto (einschließlich Kundendaten) bezüglich eines Kunden erhält, dessen primäre Kontaktinformationen darauf hinweisen, dass sich der Kunde in Europa befindet, wird Mailchimp:
(i) **inform the government agency** that Mailchimp is a processor of the data; (ii) **attempt to redirect the agency to request the data directly from Customer**; and (iii) **notify Customer** via email sent to Customer's primary contact email address of the request to allow Customer to seek a protective order or other appropriate remedy.	(i) die **Regierungsbehörde darüber informieren,** dass Mailchimp ein Auftragsverarbeiter ist; (ii) **versuchen, die Agentur aufzufordern die Daten direkt vom Kunden anzufordern**; und (iii) **den Kunden per E-Mail an die primäre Kontakt-E-Mail-Adresse des Kunden über die Anfrage informieren**, damit der Kunde eine Schutz-anordnung oder ein anderes geeignetes Rechtsmittel beantragen kann.
As part of this effort, Mailchimp may provide Customer's primary and billing contact information to the agency.	Im Rahmen dieser Bemühungen kann Mailchimp der Behörde die primären und Rechnungskontaktinformationen des Kunden zur Verfügung stellen.
Mailchimp shall not be required to comply with this paragraph 2 if it is legally prohibited from doing so, or it has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual, public safety, or Mailchimp's property, Sites, or Service.	Mailchimp ist nicht verpflichtet, diesen Absatz 2 einzuhalten, wenn dies gesetzlich verboten ist oder wenn nach vernünftigem Ermessen und nach Treu und Glauben ein dringender Zugang erforderlich ist, um das unmittelbare Risiko einer ernsthaften Schädigung der öffentlichen Sicherheit eines Einzelnen oder des Eigentums, der Websites oder der Leistungen von Mailchimp zu verhindern.

Ob diese "weitere Maßnahmen" ausreichend sind, um die Voraussetzungen zu erfüllen, einen Datentransfer in die USA auf Basis der Standard-Datenschutzklauseln durchführen zu können, ist mE damit nicht geklärt.
Jedenfalls aber ist es ein Schritt in die "richtige Richtung", und Verantwortliche, die sich des US-Dienstleisters bedienen, sollten umgehend folgende Schritte setzen:

- **Risikoabschätzung des Datentransfers** in die USA im Sinne einer **TIA (Transfer Impact Analysis)**
- Sicherstellung der ausreichende **Rechtsgrundlage** iSd Art 46 ff DSGVO - dh mE **Abschluss eine Data Processing Agreements mit Standard-Datenschutz(vertrags)klauseln** sowie w**eiteren Maßnahmen** ("supplementary meassures") iSd der Schrems II Entscheidung
- Ergänzung der **Einwilligungserklärung** um einen **Risikohinweis** iSd Art 49 Abs 1 lit a DSGVO
- **Ergänzung / Abänderung der Datenschutzinformation "Newsletter"**
- Überprüfung und eventuell **Anpassung des Verzeichnisses** gem. Art 30 DSGVO

Wir unterstützen Sie gerne bei Ihrer Datentransferstrategie und in rechtlicher Hinsicht, zB bei der Erfüllung der Informationspflichten.

Das Medienprivileg des § 9 DSG geht sehr weit. Nach Ansicht eines Beschwerdeführers bei der DSB ist es jedoch kein „Freibrief für Verächtlichmachungen“. Eine aktuelle Entscheidung (21.04.2020, 2020-0.239.741) thematisiert das **Verhältnis DSGVO und Medien** bzw. Internetveröffentlichungen zu journalistischen Zwecken.

Die Beschwerde

Eine betroffene Person verlangte die **Löschung eines Beitrages** auf **einer Plattform im Internet, und behauptete durch den Beitrag in seinen Rechten verletzt zu sein**. Der Betreiber der Plattform **verweigerte** dies unter Hinweis auf das „**Medienprivileg**“ des § 9 DSG.

Die betroffene Person wandte sich mit einer **Beschwerde wegen Verletzung des Rechts auf Löschung iSd Art 17 DSGVO** an die DSB.

Diese hat nun am 21.4.2020 das Verfahren entschieden, und die Beschwerde abgewiesen, insbes. da die DSB unzuständig ist..

Der Sachverhalt ist uU vielen aus den Medien bekannt. Der Verantwortliche betreibt eine Online-Tageszeitung, in welcher regelmäßig Online-Artikel zu aktuellen Themen veröffentlicht werden. Im Online-Portal des Verantwortlichen war ein Artikel abrufbar, der sich auf den Beschwerdeführer bezog, der ein hochrangiger Polizeimitarbeiter eines Bundeslandes war. Im Artikel gab es auch einen Link zu einem YouToube-Video, das ein Gespräch zwischen dem Beschwerdeführer und einem Mitarbeiter des Polizeinotrufdienstes wiedergibt. Weiters waren auch Twitterbeiträge eingebettet.

In der Entscheidung der DSB ist auch eine inhaltliche Wiedergabe des Gespräches enthalten:

> *Der an dieser Stelle im Bescheid vollständig wiedergegebene telefonischen Dialog, in dem der Beschwerdeführer beim Polizeinotruf anruft, um eine Polizeistreife anzufordern, und den Mitarbeiter, der ihn nicht sofort an der Stimme erkennt und seine Identität und Funktion anzweifelt, abkanzelt, für den nächsten Werktag in sein Büro zitiert, um ihm dort die Leviten zu lesen, und ihm ein Disziplinarverfahren androht, kann nicht sinnvoll pseudonymisiert werden. Von einer wörtlichen Wiedergabe wird daher Abstand genommen.*

Die Entscheidung der DSB.

§ 9 DSG regelt das „Medienprivileg“ und *„erweitert iSv Art. 85 Abs. 2 DSGVO den Geltungsbereich des Privilegs auf jede Verarbeitung personenbezogener Daten, die zu journalistischen (Abs. 1 leg. cit.) bzw. wissenschaftlichen, künstlerischen oder literarischen (Abs. 2 leg. cit.) Zwecken erfolgt. Man kann daher von einem **datenschutzrechtlichen Informationsfreiheitsprivileg** (in Folge nur: „Privileg“) sprechen.“*

Das DSG beschränkt das Informationsfreiheitsprivileg auf **Medienunternehmen** oder **Mediendiensten** zugänglich ist, sofern personenbezogene Daten **zu journalistischen Zwecken** durch **Medieninhaber, Herausgeber und Medienmitarbeiter** oder **Arbeitnehmer** eines Medienunternehmens oder Mediendienstes verarbeitet werden.

Personenbezogene Daten werden dann für **journalistische Zwecke** verarbeitet (Judikatur des EuGH zB , C-73/07 - Satakunnan Markkinapörssi und Satamedia, RZ 62), wenn die **Verarbeitung** ausschließlich das **Ziel** hat, **Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten**. **Journalismus ist weit auszulegen**, und personenbezogene Daten werden immer dann für journalistische Zwecke verarbeitet, wenn der Verantwortliche das Ziel hat, einen **unbestimmten Personenkreis zu informieren**, und dabei die Daten verarbeitet (und auch veröffentlicht).

Diese Voraussetzungen sind nach Ansicht der DSB erfüllt, und daher ist die **DSB** für das Verfahren **unzuständig, da § 9 Abs 1 DSG auch die Anwendung der Bestimmungen des Kap. II (Betroffenenrechte), dh auch Art 17 DSGVO, ausschließt**.

§ 9 Abs 1 DSG schließt zwar die Anwendung der Bestimmungen zu den Aufsichtsbehörden (Kap. VIII; Rechtsbehelfe, Haftung und Sanktionen) nicht aus, und in diesem Kapitel findet sich auch das Recht auf Beschwerde iSd Art 77 DSGVO, aber dieses Recht kann nicht losgelöst von Kapitel VI betrachtet werden.

Die **betroffene Person** ist **nicht „schutzlos“,** da sie sich auf **zivilrechtliche Bestimmungen des Persönlichkeitsrechts** (zB § 16 ABGB) oder auch das **MedienG** stützen kann, und gegen den Verantwortlichen vorgehen kann. Nur der (einfache) Weg zur DSB ist ihr verwehrt.

Frühere Entscheidungen zum Thema „Medienprivleg & DSGVO“:

Im Bescheid verweist die DSB auch auf eine bereits früher ergangene Entscheidung (DSB, DSB-D123.077/0003-DSB/2018, 13.8.2018; siehe auch unsren Blogbeitrag vom 21.09.2018 sowie Bescheid vom 27.6.2016, D122.455/0003-DSB/2016).