

von Rechtsanwalt **Phil Salewski**

Datenschutzrechtliche Risiken beim Seitenhosting über US-Dienstleister: Standardvertragsklauseln alleine genügen nicht

Bei europäischen Seitenbetreibern stehen US-Hostinganbieter wie AWS, Squarespace, Webflow oder Weebly hoch im Kurs. Allerdings werden bei solchen Hostern personenbezogene Seitenbesucherdaten regelmäßig auch an Server in den USA übertragen, was gemäß der DSGVO – nach Wegfall des EU-US-Privacy Shields – nur noch in engen Grenzen zulässig ist. Viele US-Hosting-Anbieter rühmen sich damit, sog. „Standardvertragsklauseln“ implementiert zu haben und demnach DSGVO-konforme EU-US-Datentransfers sicherzustellen. Was es mit diesen Klauseln auf sich hat und warum trotz ihrer Implementierung beim Hosting über US-Dienstleister regelmäßig ein datenschutzrechtliches Risiko besteht, zeigt dieser Beitrag.

I. Nach Wegfall des Privacy Shield: Neue geeignete Datensicherheitsgarantien erforderlich

Soweit Hosting-Dienstleister für Seitenbetreiber personenbezogene Daten verarbeiten, agieren sie hierbei als Auftragsverarbeiter (Art. 28 DSGVO). Für Verarbeitungstätigkeiten des Hosting-Dienstleisters ist mithin der Seitenbetreiber als Auftraggeber datenschutzrechtlich verantwortlich.

Beim Einsatz von US-amerikanischen Hosting-Diensten kann es nun vorkommen, dass personenbezogene Daten an Server in den USA übertragen werden.

Die DSGVO schreibt für Datenübermittlungen aus der EU in Drittländer in Art. 44 und 46 DSGVO aber geeignete Garantien vor. Als eine solche Garantie (in Form eines Angemessenheitsbeschlusses) speziell für Datenübermittlungen in die USA galt bis zur Kassation durch den [EuGH \(Urteil vom 16.07.2020 – Az. C-311/18\)](#) das EU-US-Datenschutzschild „Privacy Shield“, auf das sich nahezu alle US-Hosting-Anbieter standardmäßig beriefen.

Nach dem Wegfall des Schutzschildes konnten Übermittlungen von EU-Daten in die USA durch Hosting-Anbieter aber nicht weiter gerechtfertigt werden. Sie drohten, rechtswidrig zu sein.

US-Hosting-Anbieter waren insofern gehalten, Abhilfe zu schaffen und eine andere, von der DSGVO anerkannte Transfergarantie zu schaffen.

Die DSGVO erkennt hierfür in Art. 46 DSGVO unter anderem

- verbindliche interne Datenschutzvorschriften (Art. 47 DSGVO)
- genehmigte Verhaltensregeln (Art. 40 DSGVO) und
- von der EU-Kommission genehmigte Standard-Datenschutzklauseln (auch „Standardvertragsklauseln“ oder auf Englisch „Standard Contractual Clauses“ – „SCC“ genannt)

an.

Die meisten Hosting-Anbieter (darunter AWS, Squarespace, Weebly und Webflow) entschieden sich für die Übernahme von der EU-Kommission genehmigter Standardvertragsklauseln (SCCs).

II. Standardvertragsklauseln alleine datenschutzrechtlich unzureichend

Aus datenschutzrechtlicher Sicht ist die Implementierung von Standardvertragsklauseln allein aber nicht ausreichend, um Datenschutzrisiken bei Übertragung von personenbezogenen Daten aus der EU in die USA wirksam zu unterbinden.

So betonte bereits die Datenschutzkonferenz der Bundesländer ausdrücklich, dass [bei Datenübertragungen in die USA die bloße Aufnahme von Standard-Datenschutzklauseln nicht ausreicht, um einen angemessenen Datenschutz auf der anderen Seite des Atlantik zu gewährleisten.](#)

[Auch für die neuen, mit Durchführungsbeschluss vom 04.06.2021 beschlossenen Standardvertragsklauseln der EU-Kommission bestehen die datenschutzrechtlichen Bedenken fort.](#)

Hintergrund (und auch ein maßgeblicher Tragfehler der Kassation des EU-US-Privacy Shield) ist, dass US-Sicherheitsbehörden weitreichende Zugriffsrechte auf Datenbestände haben, die in den USA verarbeitet werden (etwa nachrichtendienstliche Erhebungsbefugnisse aus Section 702 FISA und Executive Order 12 333).

Für Betroffene aus Europa kann dies mit einem hohen Datensicherheitsrisiko einhergehen, weil sie im Zweifel nicht wissen, ob, wie und zu welchen Zwecken ihre Daten behördlich genutzt werden. Auch haben sie keine Interventionsrechte, um vom Zugriff erfasste Daten nachträglich in Auskunft zu bringen, zu löschen oder zu berichtigen.

Die bloße Anwendung von genehmigten Standardvertragsklauseln kann die Verpflichtung von US-Unternehmen, auf behördliches Gesuch hin umfangreiche Daten zur Verfügung zu stellen, aber nicht aufheben. Die Klauseln gelten nur „inter partes“, also zwischen dem Datenexporteur und dem Datenimporteur, hebeln aber gesetzlich oder gewohnheitsrechtlich verankerte Zugriffs- und Dateninterventionsrechte von US-Behörden nicht aus.

Nach Ansicht führender Datenschützer sind daher auf Unternehmensebene zusätzliche Maßnahmen zum Schutz von EU-Daten erforderlich, etwa die vollständige Anonymisierung oder zumindest

Verschlüsselung von EU-Datenbeständen auf US-Servern, um behördliche Zugriffsmöglichkeiten auf Klardaten aus der EU zu verhindern.

Dem kommen Hosting-Dienstleister aus den USA wie AWS, Squarespace, Weebly oder Webflow derzeit aber noch nicht nach.

Weil die derzeit zur Einrichtung angemessener Datensicherheitsgarantien für EU-US-Datentransfers allein implementierten EU-Standardvertragsklauseln datenschutzrechtlich nicht ausreichen, ist die Inanspruchnahme von US-Hostingleistungen für Websites in der EU und die damit einhergehende Übertragung von personenbezogenen Daten der EU-Seitenbesucher in die USA mit einem rechtlichen Risiko für den Seitenbetreiber verbunden.

III. Potenzielle Bußgelder als Konsequenz

Wer die DSGVO-Vorgaben zur Einrichtung geeigneter Garantien für Drittstaatentransfers von personenbezogenen Daten nicht einhält, kann von den zuständigen Datenschutzbehörden mit Bußgeldern geahndet werden.

Bußgelder sind beim Einsatz von US-Hosting-Anbietern, die personenbezogene Daten allein auf Basis von Standardvertragsklauseln in die USA übertragen, potenziell möglich.

Zuständig sind hier die Datenschutzbehörden des Bundeslandes, in welchem der Seitenbetreiber seinen Sitz hat.

Decken Datenschutzbehörden einen Verstoß auf, leiten Sie zunächst ein Anhörungsverfahren ein, an welches sich gegebenenfalls ein Bußgeldverfahren anschließt.

Geldbußen bei Verstößen gegen die Datensicherheitspflichten bei Drittstaatenübermittlungen können monetär stark sanktioniert werden. Art 83 Abs. 5 lit. c) DSGVO erlaubt Bußgelder von bis zu 20.000.000 Euro oder 4% des weltweit erzielten Jahresumsatzes.

Es hat bereits Fälle gegeben, in denen Datenschutzbehörden gegen Seitenbetreiber wegen der Nutzung von US-Diensten, die keine geeigneten Datenschutzgarantien implementiert haben, vorgegangen sind.

[Ein Beispiel aus März 2021 ist ein Einschreiten gegen die Verwendung von „Mailchimp“ in einem bayerischen Online-Shop.](#)

IV. Fazit

Wer US-Dienstleistungen für das Hosting eines Internetauftritts in Anspruch nimmt, riskiert, dass dadurch personenbezogene Daten von EU-Betroffenen rechtswidrig in die USA übertragen werden.

Die vielfach von US-Hosting-Anbietern belobigten Standardvertragsklauseln („SCCs“) reichen alleine nicht aus, um potenzielle Sicherheitsrisiken durch Zugriffsbefugnisse von US-Behörden zu beseitigen.

Mangelnde Datensicherheitsgarantien von US-Hosting-Anbietern müssen sich Seitenbetreiber im Rahmen der Auftragsverarbeitung zurechnen lassen und können hier theoretisch mit empfindlichen

Bußgeldern belangt werden.

Autor:

RA Phil Salewski

Rechtsanwalt