

von Rechtsanwalt **Phil Salewski**

Österreichische Datenschutzbehörde: Nutzung von Google Analytics ist datenschutzwidrig

Google Analytics ist trotz wachsenden, regionalen Alternativangeboten nach wie vor das beliebteste Tracking- und Analysetool für Websites innerhalb der EU. Problematisch ist daher spätestens seit dem Wegfall des EU-US-Privacy-Shield die Übermittlung von personenbezogenen EU-Betroffendaten an US-Server von Google. Auf eine Musterbeschwerde der EU-Datenschutzorganisation "Noyb" hat nun die Österreichische Datenschutzbehörde die Verwendung von Google Analytics für datenschutzwidrig erklärt.

I. Das Problem: Nach Wegfall des Privacy Shield neue geeignete Datensicherheitsgarantien erforderlich

Soweit Google Analytics personenbezogene Daten verarbeitet, agiert Google Analytics zusammen mit dem Seitenbetreiber nach Ansicht der führenden Datenschutzschutzbehörden als gemeinschaftlich Verantwortlicher (Art. 26 DSGVO).

Für Verarbeitungstätigkeiten von Google Analytics sind also der Seitenbetreiber und Google innerhalb ihrer Wirkungsbereiche zusammen verantwortlich.

Beim Einsatz von Google Analytics kommt es nun standardmäßig vor, dass personenbezogene Daten, zumindest die Nutzer-IP-Adresse, an Server von Google 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 16.07.2021 - Az. C-311/18)** das EU-US-Datenschutzschild "Privacy Shield", auf das sich nahezu alle US- Anbieter standardmäßig beriefen.

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

Google war insofern gehalten, Abhilfe zu schaffen und eine andere, von der DSGVO anerkannte

Transfargarantie 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" - "SCCs" genannt)

an.

Google entschied sich für die Übernahme von von der EU-Kommission genehmigter Standardvertragsklauseln (SCCs)

II. Standardvertragsklauseln allein sind 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 Tragpfeiler 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.

III. Entscheidung der Österreichischen Datenschutzbehörde zu Google Analytics

Auf eine Musterbeschwerde der europäischen Datenschutzorganisation "Noyb" hin, deren Gründer der Datenschutzaktivist Max Schrems ist, der schon das Privacy Shield vor dem EuGH zu Fall brachte, erklärte die Österreichische Datenschutzbehörde am 22.12.2021 die Nutzung von Google Analytics durch Webseitenbetreiber für datenschutzwidrig.

Die von Google implementierten Standardvertragsklauseln seien ungeeignet, um ein angemessenes, wie von Art. 44 ff. DSGVO gefordertes Datenschutzniveau für EU-Daten in den USA zu gewährleisten.

Die Klauseln könnten, da sie eben nur zwischen Google und dem jeweiligen Analytics-Anwender verbindlich seien, Überwachungs- und Zugriffsbefugnisse durch US-Nachrichtendienste nach dem Foreign Intelligence Surveillance Act (FISA) nicht beseitigen.

Von Google zusätzlich eingerichtete Sicherheitsmaßnahmen wie Verschlüsselungstechniken und Überprüfungsmechanismen für behördliche Anfragen seien weitestgehend nutzlos, um gesetzlich durchsetzbaren Datenzugriffen durch US-Behörden entgegengehalten zu werden.

Die vollständige Entscheidung der Österreichischen Datenschutzbehörde kann [hier](#) eingesehen werden.

IV. Weitere Entscheidungen europäischer Datenschutzbehörden ausstehend

Noyb unter der Leitung von Max Schrems verfolgt die Durchsetzung des EU-Datenschutzrechts gegenüber US-Diensten mit insgesamt 101 Musterbeschwerden in nahezu allen EU-Mitgliedsstaaten.

Weil die Rechtslage hier objektiv eindeutig ist, ist es überaus wahrscheinlich, dass künftig weitere Entscheidungen von Datenschutzbehörden folgen werden, die Google Analytics die fehlende EU-Datenschutzkonformität bescheinigen.

Dasselbe Schicksal teilen in rechtlicher Hinsicht alle weiteren US-Dienste, die personenbezogene Daten auf Basis von Standardvertragsklauseln in die USA übermitteln. Auch der beliebte "Facebook Pixel", Newsletter-Versanddienstleister wie **Mailchimp** und diverse US-Hostingdienste sind betroffen.

V. Fazit

Nach Ansicht der österreichischen Datenschutzbehörde ist die Nutzung von Google Analytics in der EU datenschutzwidrig.

Korrekt folgert die Behörde, dass die von Google für die Sicherheit von EU-US-Datentransfers implementierten "Standardvertragsklauseln" nicht ausreichen, um Zugriffsbefugnisse von US-Geheimdiensten auszuhebeln. EU-Daten unterliegen in den USA daher einem latenten Sicherheitsrisiko, was Datenübermittlungen in die Nation nach Art. 44 ff. DSGVO rechtswidrig macht.

Seitenbetreibern kann nur angeraten werden, so umfanglich wie möglich von der Verwendung datenverarbeitender US-Dienste abzusehen und stattdessen auf europäische Pendanten umzuschwenken.

Autor:

RA Phil Salewski

Rechtsanwalt