Dr. Thomas Schweiger, LL.M.

Google Analytics: Der nicht rechtskräftige Teilbescheid der DSB

Die österreichische Datenschutzbehörde (DSB) hat mit Teilbescheid vom 22.12.2021, GZ D155.027 2021-0.586.257, eine nicht rechtskräftige Entscheidung zum Einsatz von Google Analytics im August 2020 auf der Website eines österreichischen Verantwortlichen gefällt. Aufgrund der nicht zur Gänze erfolgten Anonymisierung durch die von NOYB als Vertreter des Beschwerdeführers veröffentlichte Entscheidung ist erkennbar, dass es sich um die Website „netdoktor.at" handelt. Die Aufsichtsbehörde folgert in ihrem 42seitigen Bescheid, dass „Website-Betreiber das Tool Google Analytics nicht in Einklang mit der DSGVO einsetzen können."

Websitebetreiber als Verantwortlicher

Wenig überraschend führt der Einsatz von Google Analytics auf der Website einer Organisation dazu, dass der Websitebetreiber als Verantwortlicher für die Verwendung des Tools auf der Website gilt.

Der (besondere) Sachverhalt

Die betroffene Person war während des Besuches der Website in ihrem Google Account eingeloggt. Der Verantwortliche hat im Verfahren zugestanden, dass das Tool „anonymize_ip", das von Google zur Verfügung gestellt wird, nicht korrekt implementiert war. Das Tool führt dazu, dass die IP-Adresse des Websitebesuchers anonymisiert wird. Es wurde für die Verarbeitung keine ausreichende Rechtsgrundlage i. S. d. Art. 6 Abs. 1 Satz 1 lit. a bis f DSGVO eingeholt. Hierfür käme m. E. nur die jederzeit widerrufbare und informierte Einwilligung der betroffenen Person in Frage. Die Übermittlung der Daten erfolgte an Google LLC in den USA und nicht, wie seit April 2021, an Google Ireland Ltd in der EU.

Die Problemlage

Seit der Schrems-II-Entscheidung des EuGH (Urt. v. 16.7.2020 – C-311/2) mit der das Privacy-Shield als Grundlage für die Übermittlung personenbezogener Daten in die USA ausgedient hat, bedarf die Datenübermittlung in ein unsicheres Drittland, d. h. ein Land, in dem kein angemessenes Datenschutzniveau herrscht, einer anderen Grundlage i. S. d. Art. 44 ff. DSGVO.

Das angemessene Schutzniveau ist in den USA nicht gegeben, da die US-Sicherheitsbehörden umfangreiche Befugnisse zum Datenzugriff, bei Google als Anbieter eines elektronischen Kommunikationsdienstes insbesondere auf Basis des 50 U.S. Code § 1881a („FISA 702"), haben. Nicht-US-Bürger können keine ausreichenden Rechtschutzmöglichkeiten ergreifen.

Auch die Standardvertrags- bzw. Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO, die zwischen dem Verantwortlichen und Google LLC vereinbart waren, reichen nicht aus. Es bedarf zusätzlicher vertraglicher, organisatorischer und technischer Maßnahmen, um die Einhaltung eines angemessenen Schutzniveaus im Empfängerland (USA oder anderes unsicheres Drittland) zu gewährleisten. Vertragliche Garantien allein sind nach Ansicht des EDSA nicht ausreichend, da durch vertragliche Zusagen die Zugriffsmöglichkeit der US-Behörden nicht beschränkt werden kann.

Die zusätzlichen Maßnahmen

Der Verantwortliche selbst hatte im konkreten Fall keine eigenen, zusätzlichen Maßnahmen implementiert, sondern sich auf die Maßnahmen von Google verlassen.

Google LLC argumentierte, dass die folgenden Maßnahmen zum Schutz der personenbezogenen Daten gesetzt wurden: die Veröffentlichung eines Transparenzberichts und Richtlinie für den Umgang mit Regierungsanfragen. Auch werde jede Datenzugriffsanfrage einer Behörde sorgfältig geprüft. Zudem hat Google auf den Schutz der Kommunikation zwischen Google-Diensten, den Schutz von Daten im Transit zwischen Rechenzentren, den Schutz der Kommunikation zwischen Nutzern und Websites und die „On-Site-Security" als technische Maßnahmen hingewiesen. Auch eine Verschlüsselung der in die USA exportierten Daten in den USA ist nicht geeignet, einen etwaigen Zugriff zu verhindern. Der Datenimporteur hat die direkte Verpflichtung, den US-Behörden einen Zugriff auf die Daten zu gewähren sowie den Schlüssel herauszugeben.

Die von Google implementierten zusätzlichen Maßnahmen wurden von der DSB als unzureichend beurteilt, da diese einen Zugriff der US-Behörden nicht verhindern können. Solange der Datenimporteur selbst weiterhin die Möglichkeit hat, auf Daten im Klartext zuzugreifen, sind nach Ansicht der DSB die technischen Maßnahmen nicht effektiv i. S. d. Schrems-II-Entscheidung umgesetzt.

Die Identifizierbarkeit als Personenbezug

Der Verantwortliche selbst war nicht in der Lage, aus den erhobenen und an Google übermittelten Daten einen Personenbezug herzustellen.

Die DSB geht in der Entscheidung jedoch davon aus, dass es nicht darauf ankommt, ob der Verantwortliche selbst den Personenbezug tatsächlich herstellt oder herstellen kann. Es reicht aus, dass ein Dritter, im konkreten Fall Google, mit vertretbarem und zumutbarem Aufwand eine Identifizierbarkeit herstellen kann.

Im entschiedenen Sachverhalt war der Websitebesucher in seinem Google-Konto eingeloggt, sodass der Personenbezug von Google über die E-Mail-Adresse herstellbar war. Selbst wenn der Nutzer während der Datenübermittlung nicht in seinem Google-Konto eingeloggt ist, gelangt man m. E. zu keinem anderen Ergebnis. Es ist davon auszugehen, dass die Möglichkeiten und die großen Datenmengen von Google aufgrund der zusätzlich übermittelten Metadaten, der Personenbezug auch in diesen Fällen hergestellt werden kann.

Die DSB verweist in ihrem Bescheid zudem darauf, dass es gar nicht darauf ankomme, dass Google den Personenbezug herstellen könne, sondern auch die US-Behörden in diese Beurteilung als mögliche Dritte einzubeziehen seien. „Nachrichtendienste der USA nehmen gewisse Online-Kennungen (z. B. die IP-Adresse oder einzigartige Kennnummern) als Ausgangspunkt für die Überwachung von Einzelpersonen."

Der Bescheid und Google LLC

Bezüglich Google LLC hat die DSB festgestellt, dass eine grenzüberschreitende Datenübermittlung von Österreich in die USA im August 2020 gegeben war. Zwar verfügt Google LLC über keine Niederlassung in mehreren EU-Staaten noch hat die konkrete Datenübermittlung eine Auswirkung auf betroffene Personen in mehreren EU-Staaten. Dadurch, dass die deutschsprachige Website mit .at-Domain sich vorwiegend an Personen in Österreich richtet, erachtete sich die österreichische DSB als zuständig.

Die weitere Beschwerde gegen Google LLC wurde jedoch abgewiesen, da die Verpflichtungen des Kapitel V der DSGVO bei einer Datenübermittlung in ein unsicheres Drittland für ein angemessenes Datenschutzniveau zu sorgen, nur den Datenexporteur, den Betreiber der Website, nicht aber den Datenimporteur, Google LLC, als Datenempfänger treffen. Google LLC legt die personenbezogenen Daten nicht i. S. d. Leitlinien 5/2021 des EDSA „offen", sondern erhält diese Daten nur.

Die DSB führt jedoch ein gesondertes amtswegiges Verfahren gegen Google LLC wegen der möglichen Verletzung der Art. 5 DSGVO (Grundsätze für die Verarbeitung personenbezogener Daten) i. V. m. Art. 28 Abs. 3 DSGVO bzw. Art. 29 DSGVO.

Möglichkeiten für die Verantwortlichen

Zusätzliche Maßnahmen i. S. d. Schrems-II-Entscheidung

Der EDSA hat in den Empfehlungen 01/2020 zu „Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten" auf 46 Seiten mögliche Schritte und Maßnahmen für Verantwortliche beim Transfer von Daten in unsichere Drittländer beschrieben.

In diesem Dokument kommt der EDSA zu dem Schluss, dass vertragliche Maßnahmen, die zwischen dem Datenexporteur und dem Datenimporteur vereinbart werden, die Behörden im Empfängerstaat, in dem kein angemessenes Datenschutzniveau besteht, nicht binden können. Dieser Ansicht folgt auch die österreichische DSB. Wenn daher nur vertragliche Maßnahmen gesetzt werden, wird dies nicht ausreichen, um die Anforderungen der DSGVO in Bezug auf das Anheben des Schutzniveaus im Empfängerstaat zu erfüllen.

Mehrfach verweist der EDSA darauf, dass die Verschlüsselung der Daten als technische Maßnahme eine Möglichkeit für die Verantwortlichen zur Erfüllung der Vorgaben sein kann. Der Schlüssel zur Decodierung der Daten muss dann beim Datenexporteur liegen, damit der Datenimporteur keinen Zugriff auf die Daten im Klartext hat.

Einsatz von anonymize_ip als „Verschlüsselung"

Google bietet an, dass der Verantwortliche nicht die ganze IP-Adresse verarbeitet, sondern nur einen Teil davon und somit dem Websitebesucher, wenn er diesen nicht aus anderen Gründen identifizieren kann, kein Gesicht zuordnen kann.

Diese technische Maßnahme ist m. E. nicht ausreichend, um die Vorgaben der Schrems-II-Entscheidung zu erfüllen, da die IP-Adresse von der Website des Verantwortlichen an Google gesendet und erst dort anonymisiert wird. Die IP-Adresse, die nach der sog. Breyer-Entscheidung ein personenbezogenes Datum darstellen kann, wird somit vollständig an Google übertragen.

Weiterhin werden andere umfangreiche Daten an Google übertragen und bei Google wird der Universal Unique Identifier (UUID) verarbeitet. Google ist daher nach Ansicht der DSB in der Lage, dem Websitebesucher „ein bestimmtes Gesicht" zuzuordnen.

Andere Grundlagen der Datenübermittlung in unsichere Drittländer als Ausweg

Die DSGVO normiert in Kapitel V (Art. 44 ff.) die Grundlagen für die Übermittlung in Drittländer. Diese Übermittlung ist z. B. zulässig, wenn für das Empfängerland ein sog. Angemessenheitsbeschluss vorliegt, der nach Prüfung der Gesetzeslage bescheinigt, dass in diesem Land das Niveau des Schutzes der personenbezogenen Daten ausreichend ist, um Daten in dieses Land zu übermitteln.

Wenn kein Angemessenheitsbeschluss als Grundlage dienen kann, dann bietet die DSGVO noch andere Möglichkeiten, „Garantien" i. S. d. Art. 46, zur Übermittlung in Drittländer. Beispiele sind die Binding Corporate Rules in Unternehmensgruppen oder Standarddatenschutzklauseln, d. h. eine Vereinbarung derselben zwischen den Parteien, wobei diese Möglichkeit durch die Judikatur zu Schrems-II eingeschränkt wurde. Wenn kein Angemessenheitsbeschluss vorliegt und es auch keine Garantien i. S. d. Art. 46 DSGVO gibt, kann sich der Verantwortliche auf die vorgesehenen Ausnahmen für bestimmte Fälle der Übermittlung (Art. 49 DSGVO) stützen.

Für Websitebetreiber, die Google Analytics einsetzen wollen, bleibt m. E. nur eine Einwilligung i. S. d. Art. 49 Abs. 1 lit. a DSGVO als möglicher Ausweg übrig. Der Websitebetreiber als Verantwortlicher teilt den Websitebesuchern – vor der Datenübermittlung – mit, dass er die Daten an Google Ireland Ltd. übermittelt und dass ein Zugriff der Sicherheitsbehörden in den USA aufgrund des CLOUD-Act (Clarifiying Lawful Overseas Use of Data Act) möglich ist. Weiterhin muss offengelegt werden, dass in den USA kein angemessenes Datenschutzniveau herrscht. Der Verantwortliche holt eine ausdrückliche Einwilligung mit Risikohinweis ein.

Ob diese Möglichkeit tatsächlich ausreichend i. S. d. DSGVO ist, bleibt fraglich. Der EDSA weist unter Bezugnahme auf ErwGr. 111 zur DSGVO in den Leitlinien 2/2018 zu den Ausnahmen nach Art. 49 DSGVO darauf hin, dass die Übermittlung auf dessen Basis nur gelegentlich und nicht wiederholt erfolgen dürfe. Eine generelle bzw. dauerhafte Einwilligung zur Datenübermittlung von der Website mit Zugriffsmöglichkeit der US-Sicherheitsbehörden bei weiteren Aufrufen derselben Website kann jedoch eine wiederholte Übermittlung darstellen.

In diesem Punkt ist m. E. noch nicht eindeutig geklärt, ob sich die Situation dadurch geändert hat, dass nicht Google LLC mit Sitz in den USA, sondern Google Ireland Ltd. in der EU der Auftragsverarbeiter ist und der Datenexport in das unsichere Drittland USA nur gelegentlich erfolgt, wenn die US-Sicherheitsbehörden im Rahmen des CLOUD-Act den Zugriff auf die Daten fordern.

Eine Einwilligung muss auch informiert erfolgen, d. h. die betroffene Person muss wissen, was mit den Daten nach der Einwilligung passiert. Kaum ein Websitebetreiber wird sämtliche Manipulationen der Daten durch Google in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erklären können. Überdies ist diese Erklärung von anderen Sachverhalten zu trennen. Es ist daher fraglich, ob die Bedingungen der Einwilligung i. S. d. Art. 7 Abs. 2 DSGVO erfüllt werden können.

Die Einwilligung muss mit einem Widerrufshinweis versehen werden und auch tatsächlich so einfach widerrufbar sein, wie sie erteilt wurde, Art. 7 Abs. 3 DSGVO. Dies bedingt m. E., dass auf der Website nicht nur mitgeteilt wird, dass die Einwilligung durch die Änderung der Browsereinstellungen widerrufen werden kann, sondern es müsste eine permanente Möglichkeit, z. B. in Form eines „sticky footer", gegeben werden, die Einwilligung zu widerrufen.

Zu diesen Fragen musste die DSB keine Stellung nehmen, da im konkreten Fall keine Einwilligung eingeholt wurde.

Wechsel von Google LLC auf Google Ireland Ltd.

Nach den Angaben von Google wird der Dienst Google Analytics seit April 2021 nicht mehr aus den USA, sondern aus Irland, daher aus der EU, betrieben. Dies führt dazu, dass es bei der direkten Datenübermittlung an Google nicht zu einem Datenexport in ein unsicheres Drittland kommt.

Meines Erachtens ist dadurch jedoch nicht viel gewonnen, da Google Ireland Ltd. als Tochterunternehmen zwar nicht unmittelbar FISA 702 unterliegen dürfte, jedoch der Zugriff der US-Behörden aufgrund des CLOUD-Act möglich ist. Dieser Umstand könnte lediglich im Rahmen der Einwilligung i. S. d. Art. 49 Abs. 1 lit. a DSGVO eine Rolle spielen, da erst dieser Zugriff die gelegentliche Übermittlung der Daten darstellt.

Handlungsempfehlungen

Ohne Anspruch auf Vollständigkeit sollte jeder Verantwortliche prüfen, ob auf seiner Website Google Analytics oder andere Tools verwendet werden, die Daten in unsichere Drittländer übermitteln. Nach der grundsätzlichen Feststellung sollte der tatsächliche Einsatz und der konkrete Nutzen in der Organisation geprüft und analysiert werden, wer welche Handlungen auf Basis der erhobenen Daten setzt.

Sollte sich herausstellen, dass nur die Reichweite der Website und die besuchten Unterseiten mit Verweildauer und Absprungrate oder die „Referrer-Seiten" für die Weiterentwicklungen der Webpräsenz erforderlich sind, dann empfiehlt sich der Umstieg auf datenschutzfreundliche Alternativen. Wenn Google Analytics als unerlässlich für die

Organisation definiert wird, sind einige Schritte zu beachten, um die Compliance mit den geltenden Datenschutzvorschriften zu verbessern:

- Abschluss eines dokumentierten Auftragsverarbeitungsvertrages mit Google
- Einsatz von anonymize_ip
- Einholung einer dokumentierten, ausdrücklichen Einwilligung mit Risikohinweis mit ausreichender Widerrufsmöglichkeit
- Erstellung eines Transfer Impact Assesment (TIA) zur Analyse der Risiken, die auf die übermittelten Daten einwirken können
- Anpassung der Datenschutzinformation in Bezug auf den Einsatz von Google Analytics
- Prüfung, ob eine „middleware" eingesetzt werden könnte, die es technisch ermöglicht, dass personenbezogene Daten von der Website nicht an Google übermittelt werden, jedoch die Funktionen des Analyse-Tools weiterhin verwendet werden können. Beim Einsatz derartiger Tools kann jedoch u. U. die Möglichkeit des Retargeting eingeschränkt sein.

Autor: **Thomas Schweiger ist Rechtsanwalt in der Wirtschaftskanzlei SMP Schweiger Mohr & Partner in Linz, Österreich und Prokurist sowie Datenschutzbeauftragter der dp dataprotect gmbh.**