von Rechtsanwalt **Jan Lennart Müller**

Österreichische Datenschutzbehörde: Die Verwendung von Google Analytics ist unzulässig

Google stellt mit seiner heutigen Online-Präsenz eine der meistbesuchten Seiten der Welt dar und bietet Informationen über alles und jeden. Was sich viele jedoch nicht bewusst sind, ist das Google der Überwachung der US-Nachrichtendienste unterliegt, welche Informationen über Personen sammeln können. Im vorliegenden Fall beschäftigte sich die österreichische Datenschutzbehörde mit der Datenübermittlung an das amerikanische Unternehmen Google LLC aufgrund des von diesem angebotenen Tools „Google Analytics“. Die Entscheidung hierzu finden sie in diesem Beitrag.

Sachverhalt

In dem zugrundeliegenden Fall besuchte der Beschwerdeführer die Webseite des Erstbeschwerdegegners, eines Vergleichsportals, während er in seinem Google-Konto eingeloggt war. Dieses war unter anderem mit seiner E-Mail-Adresse verknüpft.

Auf der Internetseite hatte der Erstbeschwerdegegner einen HTML Code für Google Dienste inklusive des Google Analytics Tool implementiert. Dieses stellt einen Messdienst des Anbieters Google dar, welcher die Traffic-Eigenschaften der Webseiten bzw. das Verhalten der Webseitenbesucher misst und auswertet. Während eines Besuchs der Webseite werden Daten wie IP-Adressen oder Cookies verarbeitet und an Google übermittelt, um dem Webseiten-Betreiber eine Auswertung der gemessenen Daten zu erstellen. Hierbei wurden auch Daten des Beschwerdeführers verarbeitet und an Google übermittelt.

Er erhob daraufhin eine Datenschutzbeschwerde bei der Datenschutzbehörde und berief sich auf eine Verletzung der allgemeinen Grundsätze der Datenübermittlung gem. Art. 44 DSGVO sowohl durch die Webseiten-Betreiberin als Erstbeschwerdegegnerin als auch gegen Google LLC als Zweitbeschwerdegegner, da Daten ohne Rechtsgrundlage übermittelt wurden.

Die Erstbeschwerdegegnerin gab an, dass sie das Tool lediglich zur Auswertung des Verhaltens der Webseiten-Besucher verwende und die Auswertung der Daten anonym erfolge, somit keine personenbezogenen Daten übermittelt wurden. Zudem seien zwischen ihr und Google eine Auftragsverarbeitungsvereinbarung, Standarddatenschutzklauseln sowie weitere Vorkehrungen getroffen worden, um ein hohes Datenschutzniveau zu gewährleisten.

EuGH: Urteil vom 16.07.2020 (Rs. C 11/18, „Schrems II“)

Mit Urteil von 16.07.2020 setzte sich der EuGH (Rs. C 11/18, „Schrems II“) bereits mit der Thematik der Übermittlung personenbezogener Daten an die USA auseinander und entschied, dass die sog. Angemessenheitsentscheidung (*„Privacy Shield“*) des Art. 45 DSGVO**ungültig** sei und man sich im Rahmen einer Datenübermittlung an die USA nicht mehr hierauf berufen könne.

Auch Standarddatenschutzklauseln könnten nur dann genügen, wenn Bestimmungsdrittländer den Anforderungen des Unionsrecht entsprechend einen angemessenen Schutz der Daten gewährleisten können.

Der EuGH hob jedoch hervor, dass Google im Sinne von 50 U.S.Code § 1881a („FISA 702“) als Anbieter elektronischer Kommunikationsdienste der Überwachung der US-Nachrichtendienste unterliege und ihnen deshalb Daten zur Verfügung stellen müsse, damit also keinen angemessenen Schutz der Daten gewährleisten könne. Eine Übermittlung sei dann unrechtmäßig.

Entscheidung der österreich. Datenschutzbehörde

Die zuständige österreich. Datenschutzbehörde entschied, dass die Erstbeschwerdegegnerin bei der Übermittlung der personenbezogenen Daten an Google durch die Implementierung des Google Analytics Tools **kein angemessenes Schutzniveau** gem. Art. 44 DSGVO gewährleistete und deshalb das subjektive Recht des Beschwerdeführers verletzte.

Browserdaten, IP-Adresse und Online-Kennungen = Personenbezogene Daten

Durch die Implementierung des Google Analytics Tools wurden Informationen des Beschwerdeführers wie **Browserdaten, die IP-Adresse und Online-Kennungen** an Google übermittelt. Diese müssten personenbezogene Daten darstellen, um von der DSGVO geschützt zu werden.

Nach Art. 4 Z 1 DSGVO sind personenbezogene Daten

> *"alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betreffende Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind."*

Auch wenn Daten wie Online-Kennungen es nicht ermöglichen, Benutzern ein genaues Gesicht

zuzuordnen, sei es dennoch möglich, sie zu unterscheiden und aus der Menge herauszusuchen. Sobald ein solches Aussondern aus der Menge ermöglicht werde, könne die Eigenschaft der Information als „personenbezogene Daten“**bejaht** werden.

Insbesondere bei Kombination aller gewonnenen Informationen wie Online-Kennungen, IP-Adressen und Browserdaten sei es aber umso wahrscheinlicher, die Person hinter ihnen zu identifizieren.

Zwar seien die Daten wie IP-Adressen im Zuge der Auswertung **anonymisiert** worden, jedoch geschehe dies nach den Feststellungen der Datenschutzbehörde **erst in einem zweiten Schritt**, nachdem die Daten auf die Server von Google übertragen wurden. Die persönlichen Daten seien also, wenn auch nur für einen kurzen Zeitraum, voll einsehbar.

Sollte man ein Aussondern aus der Menge für sich noch nicht als „personenbezogenes Datum“ ausreichen lassen, sei eine Identifikation der Person hinter den Daten unabhängig davon dennoch möglich.

Wie bereits öfter vom EuGH betont, ist der Anwendungsbereich der DSGVO sehr weit. Es sei demnach nicht erforderlich, dass die Beschwerdegegner einzeln in der Lage sind, die Person hinter den Daten zu identifizieren. Nötig sei nur, dass irgendjemand die Person mit den erlangten Daten mit vertretbarem und zumutbarem Aufwand **identifizieren könne**.

Hier komme einerseits Google in Betracht, da der Beschwerdeführer in seinem Google-Konto eingeloggt war und Google deshalb die Information erhalten könne, dass dieser Benutzer die konkrete Website besucht habe. Auch wenn hierfür zwar grundsätzlich eine gesonderte Einstellung auf dem Konto vorgenommen werden müsse, habe Google dennoch die technische Möglichkeit, den Benutzer zu identifizieren. Alleine das technische „Können“ sei also maßgeblich.

Anderseits unterliege Google, wie bereits von dem EuGH in seiner Entscheidung vom 16.07.2020 aufgezeigt, der **Überwachung der US-Nachrichtendienste**. Diese benutzen Online-Kennungen für die Überwachung von Einzelpersonen. Es könne insbesondere nicht ausgeschlossen werden, dass die US-Behörden bereits mehrere Informationen über eine Person gesammelt hatten, welche es ihnen nun ermöglichen, eine Person genau zu identifizieren.

Da die Daten erst in einem zweiten Schritt anonymisiert werden, befänden sie sich kurzzeitig voll einsehbar auf den Servern von Google und könnten von den Behörden herausverlangt werden. Auch aus den Transparenzberichten von Google sei ersichtlich, dass solche Datenanfragen der US-Nachrichtendienste an Google stattfinden.

Richtig sei zwar der Einwand, dass lediglich die Endgeräte hinter den Daten identifiziert werden können, jedoch gelten die Daten als personenbezogene Daten derjenigen Person, die das Endgerät am wahrscheinlichsten verwendet habe. Dies sei hier der Beschwerdeführer. Die gegenteilige Ansicht würde zu einem zu engen Anwendungsbereich führen, da man sich nie sicher sein könne, welche Person gerade das Endgerät verwendet habe.

Die durch das Tool gewonnen Informationen seien somit als „personenbezogene Daten“ des Beschwerdeführers zu bewerten. Diese wurden durch die Erstbeschwerdegegnerin als Verantwortliche gem. Art. 4 Z 7 DSGVO verarbeitet.

DSGVO ist anwendbar

Die Anwendbarkeit der DSGVO bejahte die Datenschutzbehörde unproblematisch im gegebenen Fall. Die Erstbeschwerdegegnerin habe ihren Sitz in Österreich und unterliege damit der DSGVO, sie legte die personenbezogenen Daten durch Implementierung des Tools offen und Google habe seinen Sitz in einem Drittland, der USA.

Für die Rechtmäßigkeit der Datenübermittlung an ein Drittland fordere Art. 44 DSGVO, dass diese unter Gewährleistung eines angemessenen Schutzniveaus erfolge. Hierfür sieht Kapitel V der DSGVO grundsätzlich drei Möglichkeiten vor.

Wie bereits erwähnt erklärte der EuGH den **EU-US-Angemessenheitsbeschluss** des Art. 45 DSGVO für ungültig, sodass diese Möglichkeit für die Gewährleistung des Schutzniveaus ausscheide.

Als weitere Möglichkeit sehe Art. 46 DSGVO vor, dass eine Datenübermittlung vorbehaltlich geeigneter Garantien zur Sicherstellung des Schutzniveaus erfolgen dürfe.

Der EuGH benenne als geeignetes Instrument hierfür die Vereinbarung von **Standardvertragsklauseln**. Problematisch ist jedoch, dass diese auf vertraglicher Basis vereinbart werden und Behörden damit nicht an sie gebunden seien. Die vorliegend vereinbarten Standardvertragsklauseln zwischen dem Erstbeschwerdegegner und Google würden somit keinerlei Einfluss auf die Überwachung von Google durch die US-Nachrichtendienste haben und deshalb kein angemessenes Schutzniveau bieten.

Um dieses Schutzniveau zu gewährleisten, müssten zusätzliche Maßnahmen vertraglicher, organisatorischer oder technischer Natur getroffen werden, die in der Lage seien, die von dem Datenexporteur bei Prüfung der Lage festgestellten Rechtsschutzlücken zu schließen.

Im gegebenen Fall lasse sich jedoch nicht erkennen, dass effektive Maßnahmen getroffen wurden, um den Zugriff der US-Behörden zu verhindern oder einzuschränken. Selbst eine Verschlüsselung der Daten führe nicht zu diesem Ziel, da sich der Zugriff der Behörden auch auf kryptographische Schlüssel erstrecke. Auch könnten die personenbezogenen Daten nicht als Pseudonym betrachtet werden, da eine Individualisierung stets möglich sei, solange die Daten nicht gelöscht oder verschleiert seien. Ebenso wenig führe die Anonymisierung wie bereits oben erläutert zu dem gewünschten Erfolg.

Als letzte Möglichkeit sehe Art. 49 DSGVO eine Ausnahmeregelung vor. Hierfür ergeben sich jedoch im gegeben Fall auch keine Anhaltspunkte. Auch eine **Einwilligung** in die Übermittlung läge **nicht** vor.

Risikobasierter Ansatz

Letztlich wurde von Google vorgebracht, dass bei Datenübermittlungen an die USA das jeweilige Risiko der Übermittlung zu berücksichtigen sei. Dieser „risikobasierte Ansatz“ ergebe sich jedoch der Datenschutzbehörde zur Folge nicht aus Art. 44 DSGVO.

Vielmehr müsse bei jeder Datenübermittlung das erforderliche Schutzniveau überprüft und sichergestellt werden, unabhängig davon, ob ein tatsächlicher Zugriff der US-Behörden erfolgen würde, wie sensibel die Daten sind, ob ein gewisses „Mindestrisiko“ bestehe oder wirtschaftliche Interessen entgegenstehen. Selbst unsensible Daten könnten in Kombination mit anderen Daten einen großen

Mehrwert bieten.

Ist Google selbst verantwortlich?

Zu klären blieb schließlich noch, ob auch Google gegen die Pflichten aus Art. 44 DSGVO verstoßen hatte. Eine Verletzung der Norm könne jedoch nur dann vorliegen, wenn ein für die Verarbeitung Verantwortliche oder Auftragsverantwortlicher personenbezogene Daten offenlege. Dies treffe auf Google als Datenimporteur von vornherein nicht zu, da es die Daten lediglich empfangen habe und es damit einen anderen Grad an Verantwortung treffe.

Fazit

Nach den bereits zuvor getroffenen Entscheidungen sowohl der österreichischen als auch der französischen Datenschutzbehörde, die sich beide mit dem Tool „Google Analytics“ auseinandersetzten, entschied die österreichische Datenschutzbehörde nun erneut, dass die Verwendung des Tools kein angemessenes Schutzniveau bei der Übermittlung von personenbezogenen Daten biete und deshalb verboten sei.

Die Datenschutzbehörde ging darauf ein, dass eine Datenübermittlung an ein Drittland nur unter Gewährleistung eines angemessenen Schutzniveaus erfolgen dürfe. Hierbei hob sie insbesondere hervor, dass geeignete Garantien zur Sicherstellung des angemessenen Schutzniveaus getroffen werden müssen, insbesondere vertragliche Vereinbarungen alleine nicht ausreichen würden, wenn der Zugriff von Behörden verhindert werden solle. Sei dies nicht möglich, dürfe eine Übermittlung nicht stattfinden. Auch die IP-Anonymisierung, wie sei bei Google stattfinde, stelle keine effektive Maßnahme dar, die Daten zu schützen.

Es bleibt somit abzuwarten, ob andere Länder der Entscheidung der österreichischen Datenschutzbehörde folgen, um einen umfangreicheren Schutz der personenbezogenen Daten zu bieten.

Bleiben Sie rechtlich stets auf dem Laufenden und schaffen so dauerhafte Rechtssicherheit! Die Schutzpakete der IT-Recht Kanzlei sichern Sie dauerhaft ab.

Autor:
RA Jan Lennart Müller
Rechtsanwalt