Google Analytics und die Datenschutz-aufsichtsbehörden – eine Verortung

Die ersten Entscheide von Aufsichtsbehörden bezüglich der Nutzung von Google Analytics haben Anfang Jahr für Gesprächsstoff unter Datenschutzexperten und zu Verunsicherung unter Webseitenbetreibern geführt. Die beiden Entscheide haben die französische (CNIL) und die österreichische Datenschutzaufsichtsbehörde (dsb) gefällt. In den nächsten Monaten dürften weitere Entscheide zu Google Analytics und Facebook Connect folgen. Es handelt sich um die ersten zwei Beurteilungen von 101 Beschwerden, welche der Verein NYOB bei diversen nationalen Aufsichtsbehörden in der EU eingereicht hat. Ob es sich die restlichen Behörden einfach machen und die Argumente der ersten Entscheide unreflektiert übernehmen, wird sich zeigen.

Von Yves Goginat

Anwendbarkeit für Schweizer Webseitenbetreiber

In der Schweiz hat sich der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) noch nicht zu den aktuellen Entwicklungen geäussert. Schweizer Webseitenbetreiber sind daher nur indirekt von den Entscheiden betroffen. Sie wären nur dann direkt betroffen, wenn eine Verhaltensbeobachtung nach Art. 3 Abs. 2 lit. b DSGVO stattfindet. Ob dies bei Webseitenanalysen der Fall ist, darüber lässt sich streiten. Der Tatbestand ist nur gegeben, wenn die Daten von Personen aus der EU mit der Absicht erhoben werden, diese weiterzuverwenden.

Schweizer Webseitenbetreiber scheinen zurzeit auch nicht im Fokus des NYOB zu sein, und die europäischen Behörden sind im Moment mit den 101 Beschwerden des NYOB ausreichend beschäftigt. Dies soll keinesfalls ein Freifahrtschein für Schweizer Webseitenbetreiber sein, die aktuellen Entwicklungen zu ignorieren. Als Webseitenbetreiber soll man aber seit den beiden Entscheiden auch nicht gleich in Panik verfallen.

Sofern nicht bereits geschehen, sollte als Erstes geprüft werden, ob die Webseite spezifisch auf Personen aus der EU ausgerichtet ist und somit die DSGVO zur Anwendung gelangt.

Politisch gefärbter Entscheid

Die von NYOB im Nachgang zum Schrems-II-Urteil eingereichten Beschwerden zielen nicht nur gegen Google und Facebook, sondern gegen den Datentransfer in Drittländer im Allgemeinen und hierbei insbesondere gegen den Transfer in die USA. Es scheint, dass mit den Beschwerden vor allem der politische Druck erhöht werden soll. NYOB kämpft mit seinen Beschwerden weiterhin gegen einen Datentransfer. NYOB und einige Aufsichtsbehörden scheinen die Meinung zu vertreten, dass ein Datentransfer unter den neuen Standardvertragsklauseln (SCC) inkl. zusätzlicher Massnahmen in den meisten Fällen weiterhin zu einer Verletzung der Grundrechte von betroffenen Personen führe und daher ein Datentransfer unzulässig sei. Die Entscheide sollen die Webseitenbetreiber, aber auch andere Verantwortliche dazu bewegen, auf europäische Anbieter umzuschwenken. Falls diese Entscheide einer richterlichen Beurteilung standhalten sollten

und dies in Zukunft die Messlatte für einen Datentransfer in ein Drittland darstellt, dann führt dies wohl effektiv dazu, dass sich viele für einen europäischen Anbieter entscheiden müssen. Ein Datentransfer wäre dann mit einem wirtschaftlich sinnvollen Aufwand kaum noch möglich. Wenn es ein globaler Internetkonzern nicht mehr hinbekommt, wie soll es dann ein KMU schaffen?

Ende März 2022 haben die Europäische Kommission und die Vereinigten Staaten bekannt gegeben, dass sie sich grundsätzlich auf einen neuen transatlantischen Datenschutzrahmen geeinigt haben, der die vom EuGH im Schrems-II-Urteil geäusserten Bedenken ausräumen soll. Wie dieser Privacy Shield 2.0 im Detail genau aussehen soll, ist noch nicht bekannt. In den scharfen Entscheiden der Aufsichtsbehörden schwingt daher wohl auch ein politisches Statement mit, entsprechende Forderungen an die USA zu stellen.

Je nach Ausgang der Verhandlungen könnten die genannten Entscheide also bald wieder obsolet sein, zumindest bis der NYOB den Privacy Shield 2.0 wieder vor das EuGH bringt und das Spiel allenfalls wieder von vorne losgeht.

Kritische Würdigung der aktuellen Entscheide

Analysedaten als Personendaten

Bis anhin hat sich Google auf den Standpunkt gestellt, dass bei einer korrekten Konfiguration durch den Webseitenbetreiber bei Google Analytics keine Personendaten im Sinne der DSGVO bearbeitet werden. Im Gegensatz dazu vertritt die deutsche Datenschutzkonferenz in ihren Hinweisen zum Einsatz von Google Analytics schon länger die Ansicht, dass es sich in jedem Fall um Personendaten handelt. Im österreichischen Fall wurde die **Anonymisierungsfunktion** offensichtlich nicht korrekt implementiert, weshalb sich dieser Fall nur bedingt als Beispiel eignet. Selbst wenn die Anonymisierungsfunktion (Kürzung der IP-Adresse) korrekt implementiert wurde, bleibt umstritten, ob es sich um Personendaten handelt.

Um einen wiederholten Besuch oder den Besuch anderer Webseiten zu verfolgen, vergibt Google zusätzlich eine Kennnummer. Gestützt auf das **Breyer-Urteil (Rs. C-582/14)** des EuGH und mit Verweis auf Erwägung 26 der DSGVO kommen nun sowohl die CNIL also auch die österreichische dsb zum Schluss, dass zumindest Google die Webseitenbesucher mithilfe der zusätzlich gesammelten Nutzungsdaten mit einem verhältnismässigen Aufwand (re-)identifizieren kann. Eine Identifizierung sei zudem durch Google möglich, wenn die betroffene Person ihrerseits über ein Google-Konto verfüge und gewisse Einstellungen aktiviert habe.

Dies darf man durchaus kritisch hinterfragen, da es jeder registrierte Nutzer grundsätzlich selbst in der Hand hat, mit entsprechenden Einstellungen eine Verknüpfung der Website-Nutzungsdaten mit anderen Daten aus seiner Nutzung von Google-Diensten zu verhindern. Das Breyer-Urteil liesse durchaus eine differenziertere Betrachtung zu. CNIL und dsb hätten gemäss dem Breyer-Urteil prüfen müssen, ob eine (Re-)Identifizierung von Nutzern durch Google oder andere Inhaber oder Empfänger der Kennnummer oder IP-Adressen vernünftigerweise wahrscheinlich ist. Eine rein theoretische Möglichkeit der Identifizierung reicht gemäss dem Breyer-Urteil gerade nicht aus. Es wird bezweifelt, dass eine Re-Identifizierung von Nutzern in der Praxis mit einem verhältnismässigen Aufwand überhaupt möglich ist.

Wie bereits andere Aufsichtsbehörden davor, haben die CNIL und dsb die Möglichkeit einer (Re-)Identifizierung angenommen und gingen in der Folge davon aus, dass die Analysedaten im Ergebnis Personendaten darstellen. Eine vertiefte Analyse blieb aber aus.

Aus Schweizer Sicht

In der Schweizer Rechtsprechung findet sich mit dem Logistep-Entscheid **(BGE 136 II 508)** ebenfalls ein Entscheid zur Beurteilung von IP-Adressen. Wie der EuGH geht auch das Bundesgericht nicht pauschal davon aus, dass es sich bei IP-Adressen immer um Personendaten handelt. So führte es aus, *dass für die Bestimmbarkeit nicht jede theoretische Möglichkeit der Identifizierung genügt. Ist der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor. Die Frage ist abhängig vom konkreten Fall zu beantworten, wobei insbesondere auch die Möglichkeiten der Technik mitzuberücksichtigen sind, so zum Beispiel die im Internet verfügbaren Suchwerkzeuge. Von Bedeutung ist indessen nicht nur, welcher Aufwand objektiv erforderlich ist, um eine bestimmte Information einer Person zuordnen zu können, sondern auch, welches Interesse der Datenbearbeiter oder ein Dritter an der Identifizierung hat.*[1] Dies führt zum Schluss, dass korrekt anonymisierte Nutzerdaten – wenn also eine (Re-)Identifizierung unwahrscheinlich ist – keine Personendaten im Sinne des Schweizer Datenschutzgesetzes (DSG) sind.

Soweit ersichtlich, hat sich der EDÖB seit Längerem nicht mehr mit dieser Thematik auseinandergesetzt. Er hat sich zuletzt in seinem Tätigkeitsbericht 2012/2013 dazu geäussert.[2] Er scheint zwar IP-Adressen grundsätzlich als Personendaten zu betrachten, er hält darin aber auch fest: *«Wenn hingegen mittels spezieller Vorkehrungen sichergestellt werden kann, dass bei der Analyse keine personenbezogenen Daten erhoben werden, findet das DSG keine Anwendung.»* Dies deute zumindest daraufhin hin, dass anonymisierte Nutzerdaten nicht zwingend Personendaten darstellen.

1 BGE 136 II 508, E.3.2

2 Tätigkeitsbericht 2012/2013 des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, Abschnitt 1.3.6.

Im Übrigen ist noch zu erwähnen, dass, selbst wenn es sich um Personendaten handelt, in der Schweiz sowohl unter dem Datenschutzgesetz sowie nach Art. 45c FMG keine Einwilligung notwendig wäre. Sofern die Informationspflichten erfüllt werden, ist der Einsatz von Google Analytics grundsätzlich zulässig.

Kommt man zum Schluss, dass es sich unter dem Schweizer Datenschutzgesetz (DSG) ebenfalls um Personendaten handelt, würde gemäss dem DSG ein Datentransfer in ein Drittland stattfinden. Es wäre demnach ebenfalls eine entsprechende Einzelfallprüfung vorzunehmen.

Internationaler Datentransfer

CNIL und dsb konzentrierten sich nicht auf allfällige Verletzungen des Transparenzprinzips oder anderer Bearbeitungsgrundsätze. Stattdessen liegt der Fokus der Aufsichtsbehörden auf den Datentransfers in die USA. Die rechtskonforme Nutzung von Google Analytics scheitert daher nicht an der Nutzung, sondern am Datentransfer innerhalb des Google-Konzerns.

Gemäss dem Schrems-II-Urteil reichen die SCC alleine nicht mehr in jedem Fall aus, um einen rechtskonformen Datentransfer zu gewährleisten. Obwohl es sich bei den transferierten Analysedaten um eher wenig heikle Daten handelt, kamen beide Aufsichtsbehörden zum Ergebnis, dass die vertraglichen, organisatorischen und technischen Massnahmen von Google nicht ausreichen und daher der Datentransfer in die USA einen Rechtsverstoss darstellt.

Google Analytics ist zweifellos ein sehr stark verbreitetes Analysetool, und im Verhältnis zur starken Verbreitung von Google Analytics sind gemäss **Google Transparenzbericht** bislang nur sehr wenige Behördenanfragen erfolgt. Der Transparenzbericht bezieht sich zudem auf alle Google-Dienstleistungen.

Ungenügende Risikobeurteilung

Beide aktuellen Entscheide scheinen derzeit die Bekanntgabe von Personendaten in die USA nur zuzulassen, wenn ein Behördenzugriff komplett ausgeschlossen werden kann. Laut der dsb kann nicht ausgeschlossen werden, dass Nachrichtendienste bereits im Vorfeld Informationen gesammelt haben, mit deren Hilfe sie die nun für die Zwecke von Google Analytics übertragenen Nutzungsdaten auf eine bestimmte Person rückführen können. Obwohl man bereits sehr viel Fantasie aufbringen muss, um in diesem Kontext ein Interesse der Geheimdienste an den entsprechenden Nutzungsdaten zu ersinnen, und nota bene der Aufwand und Ertrag von Geheimdiensten diesbezüglich wohl kaum in einem vernünftigen Verhältnis steht, wenn überhaupt eine Identifizierung und Profiling technisch möglich ist, kann selbstverständlich ein Zugriff und damit eine Grundverletzung auch in diesem Fall nicht ganz und gar ausgeschlossen werden. Eine «sehr» theoretische Gefahr scheint für die Aufsichtsbehörden somit ausreichend zu sein, um einen Datentransfer generell auszuschliessen.

Eine solche Herangehensweise und Interpretation widerspricht klar dem Schrems-II-Urteil. Dieses hält nämlich fest, dass jeweils eine Einzelfallprüfung vorzunehmen sei und anhand der konkreten Datenverarbeitung angemessene zusätzliche Massnahmen zu treffen seien, um ein adäquates Datenschutzniveau herzustellen. Neben einer vertieften Auseinandersetzung mit den getroffenen Zusatzmassnahmen ist insbesondere eine Risikobeurteilung vorzunehmen. Es gab zwar eine oberflächliche Beurteilung, und beide Behörden kamen sehr schnell zum Schluss, dass solche Datensätze bezüglich Webseitenbesuche wohl für die Behörden interessant sein könnten und daher der Aufwand einer Identifizierung für einen US-Geheimdienst generell (und nicht in einem konkreten Fall!) nicht unverhältnismässig sei. Die Frage ist aber durchaus erlaubt, ob diese Daten tatsächlich in jedem Fall und generell so wertvoll sind, dass sich der Aufwand einer Identifizierung bestimmter Webseitennutzer für US-Geheimdienste überhaupt lohnt. Für einen US-Geheimdienst gibt es wohl relevantere Datenquellen, die mit einem wesentlich geringeren Aufwand verknüpft sind.

In Anbetracht der Erwägung 20 des SCC-Beschlusses (Durchführungsbeschluss [EU] 2021/914), welche verlangt, dass dokumentierte praktische Erfahrungen zu berücksichtigen sind, stellt sich sodann die Frage, weshalb die Aufsichtsbehörden die effektiven Auswirkungen nicht genauer geprüft haben. Der **Google Transparenzbericht** führt diverse FISA-Anfragen auf, bei wie vielen davon effektiv Google-Analytics-Daten betroffen waren, haben die Behörden bis anhin weder nachgefragt noch gewertet. Google ist zwar als Anbieterin elektronischer Kommunikationsdienste im Sinne von 50 U.S. Code § 1881(b)(4) zu qualifizieren, weshalb sie der Überwachung durch US-Nachrichtendienste gemäss 50 U.S. Code § 1881a («FISA 702») unterliegt. Ob Google Analytics jemals Thema einer Anfrage war, wurde jedoch nicht geprüft. Im Nachhinein machte der Global Affairs & Chief Legal Officer von Google **öffentlich,** dass es in den letzten 15 Jahren keine einzige Anfrage von Geheimdiensten bezüglich Google Analytics gab! Die Behörde hat somit ganz offensichtlich die praktischen Erfahrungen vollständig ausgeblendet und alleine aus dem Fakt, dass es Anfragen bezüglich Google-Dienstleistungen gab, und dem theoretischen Interesse von Geheimdiensten an solchen Daten, auf Zugriffe geschlossen. Im Ergebnis eine sehr praxisferne Beurteilung aus dem Elfenbeinturm heraus.

Dies steht auch im Widerspruch zu den neuen SCC, die eine fallbezogene und differenzierte Betrachtungsweise erfordern. Gemäss den neuen SCC muss bei der Beurteilung des angemessenen

Schutzniveaus bei Transfers in unsichere Drittstaaten jeweils dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und dem Zweck der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffenen Personen gebührend Rechnung getragen werden. Es muss daher auch bei Zusatzmassnahmen das Verhältnismässigkeitsprinzip gewahrt bleiben und eine entsprechende Risikobeurteilung stattfinden. In eine gleiche Richtung gehen die EDSA-Empfehlungen zum internationalen Datentransfer, welche ebenfalls einen risikobasierten Ansatz postulieren.

Die Aufsichtsbehörden scheinen jedoch bei jedem Datentransfer Massnahmen zu verlangen, die einen Zugriff hundertprozentig ausschliessen. Dies widerspricht dem regulatorisch vorgesehenen risikobasierten Ansatz komplett. Es ist unverständlich, weshalb die getroffenen technischen und organisatorischen Massnahmen für ein eher theoretisches Risiko und wenig sensible Personendaten nicht ausreichend sein sollen.

Schliesslich zeichnen die Entscheide von CNIL und dsb ganz allgemein ein gar düsteres Bild. Zum einen handelt es sich bei Google Analytics um ein Produkt, das keine umfangreichen Personendaten (sofern es sich bei den analysierten Nutzungsdaten überhaupt um Personendaten handelt) bearbeitet. Zum anderen wird der Dienst von einem der grössten Internetkonzerne betrieben. Dieser scheint es mit all seinen Ressourcen nicht zu schaffen, Zusatzmassnahmen zu implementieren, die den Aufsichtsbehörden genehm wären. Wenn dies nun effektiv die zukünftige Hürde darstellen soll, dann stellt das die Möglichkeit eines internationalen Datentransfers allgemein infrage.

Da sich der EDÖB noch nicht zum Thema geäussert hat, bleibt eine Beurteilung für die Schweiz schwierig. Es ist unklar, ob er sich an den bereits erfolgten Entscheiden orientieren würde oder selbst eine vertiefte Beurteilung vornehmen würde. Es ist auf das Zweite zu hoffen.

Zusammenfassung und Ausblick

Zusammengefasst schliessen die Aufsichtsbehörden von einer theoretischen Möglichkeit der Identifizierung von Nutzern anhand der Analysedaten darauf, dass Webseitenbetreiber bei der Verwendung von Google Analytics stets Personendaten bearbeiten. Zudem unterliessen es die Aufsichtsbehörden, das Risiko eines Behördenzugriffs in den USA im Einzelfall zu prüfen. Im Lichte dieser Überlegungen ist es fraglich, ob die Entscheide der CNIL und der dsb einer richterlichen Überprüfung standhalten werden.

Die beschriebenen Behördenentscheide zeigen zwar eine Tendenz der Aufsichtsbehörden, für Datentransfers in ein Drittland eine sehr hohe Hürde zu setzen. Im Moment fehlt aber noch eine richterliche Beurteilung, welche dies stützen würde. Insbesondere ein EuGH-Entscheid liegt noch in weiter Ferne, und es wird noch einige Jahre dauern, bis die Zulässigkeit von Google Analytics und ähnlichen Tools abschliessend geklärt ist. Bis dahin werden wir vielleicht bereits den Privacy Shield 2.0 sehen, was einen Entscheid obsolet machen könnte.

Im Moment sollte man daher gerade als Schweizer Webseitenbetreibern ruhig Blut bewahren. Wer Google Analytics heute nutzt, sollte sicherstellen, dass alle technischen und vertraglichen Massnahmen ausgeschöpft sind. Es gilt insbesondere zu prüfen,

- ob die Nutzung auf den aktuellen Nutzungsbedingungen basiert und Google Ireland Limited Vertragspartei ist und nicht Google LLC. Bei den neueren Vertragsverhältnissen sollte dies bereits der Fall sein.
- ob Google Analytics technisch korrekt implementiert ist. Insbesondere sollten die Anonymisierungsfunktionen eingeschalten sowie die Datenfreigabeeinstellungen und Google-Signale deaktiviert sein.
- und ob die Nutzer ausreichend informiert werden. In der Schweiz ist die Einwilligung nicht vorgeschrieben. Viele Webseitenbetreiber setzen trotzdem ein Cookies-Management-Tool ein. In einem solchen Tool lässt sich auch Google Analytics als optional konfigurieren.

Wer keinerlei Risiko eingehen will, in den Fokus von Aufsichtsbehörden, Konsumentenschutzorganisationen oder gar von Gerichten zu geraten, kann selbstverständlich auch auf Analytics Tools setzen, die Daten ausschliesslich in Europa bearbeiten oder keine Drittanbieter für die Analyse einsetzen.

AUTOR

Yves Gogniat hat Rechtswissenschaften an der Universität St. Gallen (Master of Arts HSG in Law, 2011) und an der Universität Edinburgh (LL.M. in Information Technology, 2019) studiert. Er ist zur Tätigkeit als Anwalt in der Schweiz zugelassen.

IMPRESSUM

Verlag: WEKA Business Media AG, Hermetschloostrasse 77, CH-8048 Zürich, www.weka.ch
Herausgeber: Reto Fanger
Redaktion: Junes Babay
Layout/Satz: Dimitri Gabriel
Publikation: 10 × jährlich, Abonnement: CHF 98.– pro Jahr, Preise exkl. MWST und Versandkosten.
Als digitale Publikation erhältlich unter: www.weka-library.ch
Bildrechte: www.istockphoto.com
Bestell-Nr.: NL9231