LEGAL REVOLUTIONary
Recht in der digitalen Wirtschaft

Google Analytics rechtssicher einsetzen

Rechtliche Herausforderungen beim Einsatz von Cookies und Handlungsempfehlungen für Webseitenbetreiber

Sebastian Durchholz | Externer Datenschutzbeauftragter | Datenschutz Durchholz

19. Mai 2021
LR 2021, Seiten 116 bis 125 (insgesamt 10 Seiten)

I. Ziel des Aufsatzes

Der Einsatz von Tracking Tools ist für viele Unternehmen derzeit unverzichtbar – trotz der DSGVO und vielen anderen Vorstößen von Datenschützern.[1] Die häufig verwendeten Website Analyse Tools wie Google Analytics stellen eine große Herausforderung für die Datenschutz-Compliance dar. Ziel des Aufsatzes ist es, Webseitenbetreiber für die Gefahren beim Einsatz von US-Tracking-Anbietern zu sensibilisieren und anhand des prominenten Beispiels von Google Analytics aufzuzeigen, wie ein weitestgehend rechtssicherer Einsatz des Tools gelingt. Dabei werden die rechtlichen Probleme erläutert und eine praxisnahe Anleitung für Webseitenbetreiber vorgestellt.

II. Funktionsweise von Google Analytics

Zu Beginn stellt sich die Frage, wie Tracking Tools, und im konkreten Google Analytics, technisch funktionieren. Das Ziel von sog. Web Analyse Tools ist es, Webseitenbetreibern nützliche Information über die Benutzung ihrer Webseite bereitzustellen. Beispielsweise kann die Anzahl der Besucher ermittelt werden, welche Beiträge sie interessieren oder von welcher anderen Seite sie zu dieser Webseite gelangt sind.[2]

Hierzu wird meist ein sog. Tracking-Code verwendet. Sobald ein Nutzer die Webseite aufruft, wird dieser Code vom Browser des Besuchers ausgeführt. Das Skript[3] speichert dann eine Textdatei im Browser, die bestimmte Informationen zum Nutzer und dessen Nutzung enthält. Bei diesen Textdateien handelt es sich um die bekannten „Cookies“. Das

[1] Zur Übersichtlichkeit wird das generische Maskulinum verwendet.
[2] *Koreng/Lachenmann*, DatenschutzR-FormHdB, F. I. 5. Web Analytics.
[3] Ein Skript besteht aus einer kurzen Abfolge von Befehlen, die von einer Webseite ausgeführt wird. Auf Websites wird meistens die Programmiersprache JavaScript verwendet.

Cookie überträgt anschließend die Daten an den Tracking-Anbieter, der dem Webseitenbetreiber im Anschluss eine Auswertung übergibt.

Im Falle von Google Analytics sieht der Tracking-Code wie folgt aus:

```
<script async src="https://www.googletagmanager.com/gtag/js?id= UA-XXXXXXXXX-X "></script>

<script>

window.dataLayer = window.dataLayer || [];

function gtag(){dataLayer.push(arguments);}

gtag('js', new Date());

gtag('config', ' UA-XXXXXXXXX-X ');

</script>
```

Dieser Code erzeugt beim Ausführen ein Cookie und erhebt die folgenden Nutzungsdaten: Cookie-ID, vom Nutzer besuchte Webseiten, Art des Endgeräts (PC, Mobil, Tablet), Browser und Betriebssystem, IP-Adresse und Besucherquelle. Die Daten werden im Anschluss an die Server von Google übertragen und dort automatisiert ausgewertet. Die Auswertungen stehen im Anschluss dem Webseitenbetreiber zur Verfügung.

III. Rechtliche Herausforderungen beim Einsatz von Google Analytics

Durch die neuste Rechtsprechung des EuGHs zu Datenübermittlungen in Drittstaaten und dem BGH-Urteil zum Einsatz von Google Analytics ergeben sich verschiedene rechtliche Herausforderungen. Bereits vor diesen Urteilen gab es von der Datenschutzkonferenz (DSK) massive Kritik am Einsatz von Google Analytics.[4] Im Folgenden wird keine detaillierte datenschutzrechtliche Prüfung vorgenommen, sondern vielmehr auf die wesentlichen juristischen Probleme und mögliche Lösungen eingegangen.

1. Übermittlung in Drittstatten (insb. USA)

Bei der Nutzung von Google Analytics erfolgt ein Datentransfer in die USA. Das Land gilt seit dem „Schrems II"-Urteil des EuGHs als unsicherer Drittstaat. Dementsprechend

[4] Beschluss DSK vom 12.05.2020, *Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich*.

müssen die Vorgaben der Art. 46 ff. DSGVO und insbesondere die Vorgaben des EuGH-Urteils umgesetzt werden, damit eine datenschutzkonforme Übermittlung vorliegt.

a) „Schrems II" Urteil

In seiner „Schrems II" Entscheidung erklärte der EuGH das EU/US Privacy Shield für ungültig.[5] Dieses Abkommen ermöglichte zuvor, dass personenbezogene Daten an zertifizierte Unternehmen in die USA übertragen und von diesen verarbeitet werden durften. Mit diesem Urteil wurde nahezu jeglicher Datenverkehr in die USA vom einen auf den anderen Moment rechtswidrig.

Der EuGH erklärte die Standarddatenschutzklauseln der EU-Kommission für weiterhin gültig.[6] Die Standarddatenschutzklauseln sind deshalb relevant, weil nach Art. 46 Abs. 1 DSGVO der Verantwortliche nur Daten in unsichere Drittstaaten übermitteln darf, wenn er geeignete Garantien vorgesehen hat und die Betroffenen ihre Rechte durchsetzen können. Als solche Garantien gelten gem. Art. 46 Abs. 2 Buchst. c DSGVO die Standarddatenschutzklauseln der EU-Kommission. Allerdings betonte der EuGH, dass bei solchen Datentransfers neben dem Abschluss der Standarddatenschutzklauseln auch zusätzliche geeignete Garantien nötig seien.[7] In allen Fällen müsse zwingend eine Einzelfallprüfung vorgenommen werden.[8]

b) Auftragsverarbeitungsvertrag

Der Europäische Datenschutzausschuss (EDSA) und die DSK halten eine Übermittlung von Daten in die USA und weitere Drittstaaten auf Grundlage von Standarddatenschutzklauseln weiterhin für möglich, wenn der Verantwortliche eine positive Risikoabschätzung des Einzelfalls erstellt, die ggf. mit zusätzlichen Schutzmaßnahmen verbunden ist.[9]

Bei Google Analytics wird neben einem Auftragsverarbeitungsvertrag seit August 2020 zusätzlich ein Vertrag mit einer Standarddatenschutzklausel angeboten. Viele Unternehmen nutzen Google Analytics bereits seit mehreren Jahren. Deshalb kann es sein, dass sie zwar einen Auftragsverarbeitungsvertrag, jedoch keinen Zusatzvertrag mit der Standarddatenschutzklausel abgeschlossen haben. Die Verantwortlichen sollten

[5] EuGH, Urteil vom 16. Juli 2020 – C-311/18 –, NJW 2020, 2613 (2622).
[6] Ebd., S. 2613.
[7] Ebd., S. 2618.
[8] Ebd., S. 2618.
[9] FAQ des EDSA vom 16.7.2020, siehe auch Opinion 24 und 25/2020 zu verbindlichen internen Datenschutzvorschriften (Art. 47 DSGVO); Pressemitteilung der Datenschutzkonferenz vom 28.7.2020; *Jungkind/Raspé/Schramm*, Risikoanalyse und zusätzliche Maßnahmen – Konzerninterner US-Datentransfer nach „Schrems II", NZG 2020, 1056 (1057).

diesen Zusatzvertrag zusätzlich zu dem Auftragsverarbeitungsvertrag abschließen, um eine rechtskonforme Verarbeitung zu ermöglichen. Wo dieser Vertrag genau zu finden ist, wird unten erläutert.[10]

c) Zusätzliche geeignete Garantien

Weiterhin sind zusätzliche geeignete Garantien nötig. Jedoch konkretisiert der EuGH in seinem Urteil nicht, was unter diesen „geeigneten Garantien" zu verstehen ist. Die EDSA beantwortet diese Frage in seinen FAQ vom 23.07.2020 nicht. In der Kommentarliteratur ist nur zu lesen, dass durch einen Vertrag oder durch eine einseitige Verpflichtung ein angemessenes Datenschutzniveau im Drittland hergestellt werden muss.[11] Damit ist der Verantwortliche und ggf. sein Auftragsverarbeiter bei der eine Bewertung der geeigneten Garantien auf sich alleine gestellt. Es scheint vertretbar zu sein, dass der Verantwortliche neben den Standarddatenschutzklauseln andere geeignete technische und organisatorische Maßnahmen gem. Art. 32 DSGVO ergreift, um eine zusätzliche Schutzmaßnahme zu schaffen.[12] Der Verantwortliche sollte seine Abwägung und die getroffenen Maßnahmen stets dokumentieren, da er bei Schadensersatzansprüchen gem. Art. 82 Abs. 3 DSGVO i.V.m. dem Erwägungsgrund 42 die Beweislast trägt.

Die IP-Adresse ist als personenbezogenes Datum einzuordnen. Aus diesem Grund bietet Google Analytics eine IP-Anonymisierung an. Bei dieser Anonymisierung werden die letzten drei Stellen der IP-Adresse gelöscht, bevor die Daten an Google in die USA übertragen werden. Die Anonymisierung stellt eine technische und organisatorische Maßnahme[13] dar und ist damit als zusätzliche Garantie geeignet.

d) Ergebnis

Insgesamt kann mit dem Einsatz von Standarddatenschutzklauseln und der IP-Anonymisierung als zusätzliche Garantie ein angemessenes Datenschutzniveau aus Sicht eines Verantwortlichen vertretbar hergestellt werden. Die sichere Klärung der Rechtsfrage bedarf zuletzt der Klärung durch die Gerichte. Bis dahin muss der Verantwortliche eine eigene Risikoabschätzung im Fall von Google Analytics vornehmen.

---

[10] Siehe Punkt III.2.b.

[11] *Schantz* in *Simitis/Hornung/Spiecker gen. Döhmann*, Datenschutzrecht, 1. Auflage 2019, DSGVO Art. 46 Rn. 5; *Voigt* in *Spindler/Schuster*, Recht der elektronischen Medien, 4. Aufl. 2019, DS-GVO Art. 49 Rn. 19.

[12] *Paal/Kumkar*, Datenübermittlungen nach dem Unwirksamwerden des EU-US-Privacy Shield, MMR 2020, 733 (736).

[13] *Hornung/Wagner*, Anonymisierung als datenschutzrelevante Verarbeitung? ZD 2020, 223 (223).

2. Abgrenzung Auftragsverarbeitung und gemeinsame Verantwortlichkeit

Darüber hinaus stellt sich die Frage, ob Google gemeinsam mit dem Webseitenbetreiber verantwortlich i.S.d. des Art. 26 Abs. 1 DSGVO ist oder lediglich als Auftragsverarbeiter tätig wird. Im Falle der gemeinsamen Verantwortlichkeit ist ein sog. Joint-Controller-Agreement nach Art. 26 Abs. 1, 2 DSGVO erforderlich. Dieser Vertrag legt unter anderem fest, welche unterschiedlichen Zwecke die Parteien mit der Datenverarbeitung verfolgen und wer von ihnen welche Pflichten aus der DSGVO zu erfüllen hat. Dazu gehören unter anderem die Informationspflichten nach Art. 13 und 14 DSGVO sowie die Wahrung von Betroffenenrechten.

Die Auftragsdatenverarbeitung unterscheidet sich von der gemeinsamen Verantwortlichkeit insofern, dass ein Unternehmen allein über die Zwecke und Mittel der Verarbeitung entscheidet und es eine hierarchische Struktur gibt, bei der ein Subunternehmer nur im Auftrag und auf Weisung die Daten verarbeitet.[14]

Die DSK geht bei Google Analytics von einer gemeinsamen Verantwortlichkeit gem. Art. 26 Abs. 1 DSGVO aus.[15] Begründet wird dies damit, dass Google zum Teil ausschließlich die Zwecke und Mittel selbst vorgibt und diese vom Webseitenbetreiber akzeptiert werden.[16] Google stellt in einem zusätzlichen Vertrag, den *Google Measurement Controller-Controller Data Protection Terms* klar, dass sie und der Anwender für bestimmte Verarbeitungen getrennt verantwortlich seien.[17] Schließlich erkläre Google in den Nutzungsbedingungen, dass sie die Daten für eigene Zwecke verwenden würden.[18] Damit ist aus Sicht der DSK keine Auftragsverarbeitung gem. Art. 28 DSGVO mehr vorhanden, es handelt sich vielmehr um eine gemeinsame Verantwortlichkeit.

In der noch nicht rechtskräftigten Entscheidung des LG Rostock, Urteil vom 15.9.2020 – 3 O 762/19, sieht das Gericht eine gemeinsame Verantwortlichkeit beim Einsatz von Google Analytics gegeben.[19] Leider geht das Gericht in seiner Entscheidung nicht auf die genauen vertraglichen Umstände ein, sondern bezieht sich lediglich auf die Entscheidung der DSK.

Der DSK ist insoweit zuzustimmen, dass die Nutzung von Google Analytics in den Standardeinstellungen eine gemeinsame Verantwortlichkeit nach Art. 26 Abs. 1 DSGVO bewirkt. Allerdings verkennt die DSK, dass auch andere Einstellungen möglich sind, die eine Weitergabe der Daten an Google unterbinden und damit eine gemeinsame

[14] BeckOK DatenschutzR/*Spoerr* DS-GVO Art. 28 Rn. 22a.
[15] Beschluss DSK vom 12.05.2020, *Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich*, S. 2 f.
[16] Ebd., S. 2.
[17] Ebd., S. 2 f.
[18] Ebd., S. 3.
[19] LG Rostock, Urteil vom 15. September 2020 – 3 O 762/19 –, juris Rn. 95.

Verantwortlichkeit ausschließen. Die DSK hätte daher auf alternative Einstellungen eingehen müssen, um eine praktikable Einschätzung geben zu können. Insgesamt kann eine Auftragsverarbeitung angenommen werden, wenn die Standardeinstellungen entsprechend geändert werden. Wie die Einstellungen bei neuen oder bestehenden Accounts konkret geändert werden müssen, wird im Folgenden erläutert.

a. Vorgehen bei neuen Accounts

Wenn ein neuer Account bei Google Analytics erstellt wird, enthält die Registrierungsmaske zunächst Optionen für die „Datenfreigabeeinstellungen für das Konto". An dieser Stelle entscheidet sich, ob eine Auftragsverarbeitung nach Art. 28 Abs. 1 DSGVO oder eine gemeinsame Verantwortlichkeit gem. Art. 26 Abs. 1 DSGVO vorliegt.

Es empfiehlt sich, alle vorgeschlagenen Punkte (Google-Produkte und Dienste, Benchmarking, Technischer Support und Account Specialists) abzulehnen. Das gilt besonders beim Punkt „Google-Produkte und Dienste", bei dem Google den Abschluss eines Vertrages nach Art. 26 Abs. 1 DSGVO verlangt.

Ferner wird ein Auftragsverarbeitungsvertrag und der Zusatzvertrag inklusive der Standardvertragsklauseln der EU-Kommission direkt bei der Registrierung mit abgeschlossen. Schließlich muss die Region gewählt (in unserem Fall Deutschland) und dann die Bedingungen akzeptiert werden. Der Vertrag kommt hierbei mit der Google Ireland Ltd. zustande.

b. Vorgehen bei bestehenden Accounts

Oftmals sind bei bestehenden Google Analytics Accounts sämtliche Datenfreigabeeinstellungen aktiviert und der Zusatzvertrag wurde nicht abgeschlossen. Dies kann geändert werden, indem man sich bei Google Analytics einloggt. Danach wird der Punkt „Verwaltung" unten rechts ausgewählt. Anschließend wird im neuen Menü „Kontoeinstellungen" ausgewählt.

In dem neu geöffneten Menü gelangt man zu dem Punkt „Datenfreigabeeinstellungen". Dort stehen die Punkte (Google-Produkte und Dienste, Benchmarking, Technischer Support und Account Specialists) zur Verfügung. Bei bestehenden Google Analytics Accounts sind meistens alle Einstellungen aktiviert. Auch hier empfiehlt es sich, die gesamten Kreuze zu entfernen, um so eine gemeinsame Verantwortlichkeit gem. Art. 26 Abs. 1 DSGVO zu vermeiden.

Anschließend kommt man unten zu dem Punkt „Zusatz zur Datenverarbeitung". Dort kann man sehen, ob bereits ein Vertrag inklusive der Standarddatenschutzklauseln abgeschlossen wurde. In zwei Fällen besteht Handlungsbedarf: Erstens, wenn zwar einem

Zusatzvertrag zugestimmt wurde, dieser allerdings mittlerweile aktualisiert ist. Zweitens wenn bei Ihnen steht, dass noch gar kein Zusatz akzeptiert wurde. In beiden Fällen klicken Sie auf „Aktualisierter Zusatz“ oder „Zusatz anzeigen“ und stimmen diesem zu.

c. Weitere Einstellungen in Google Analytics

Ferner muss die Aufbewahrungsdauer der Daten bei Google Analytics begrenzt werden. Standardmäßig sieht Google Analytics eine Aufbewahrungsdauer von 26 Monaten vor. Um dem Prinzip der Datensparsamkeit aus Art. 25 Abs. 1 DSGVO zu genügen, muss diese Dauer herabgesetzt werden. Google Analytics bietet hierbei die Möglichkeit, die Speicherung auf 14 Monate zu begrenzen.

Um diese Einstellung zu ändern, kann auf „Verwaltung“ geklickt werden. Dort ist mittig unter dem Reiter „Property“ der Menüpunkt „Tracking-Informationen“. Beim Auswählen öffnet sich ein Untermenü mit weiteren Einstellungen und wählt dann den Punkt „Datenaufbewahrung“ aus. Anschließend öffnet sich das Einstellungsfenster „Aufbewahrung von Nutzer- und Ereignisdaten“. Dort kann als Aufbewahrungsdauer 14 Monate ausgewählt sowie der Vorgang gespeichert werden.

3. Rechtsgrundlage für den Einsatz von Tracking Cookies

Neben den datenschutzrechtlichen Vorschriften existieren für Webseiten als Telemedium noch andere Vorschriften. Darunter fällt beispielsweise das Telemediengesetz (TMG), dass die deutsche Umsetzung der Richtlinie 2002/58/EG (ePrivacy-RL) darstellt. Auch dieses muss beim Einsatz von Google Analytics beachtet werden. Deshalb wird im Folgenden das weitreichende „Planet49“-Urteil des BGH vom 28. Mai 2020 (Az. I ZR 7/16) aufgegriffen.

a) „Planet49“-Urteil

Mit dem „Planet49“-Urteil hat das Gericht festgestellt, dass es beim Einsatz von Google Analytics einer Einwilligung des Nutzers bedarf.[20]

Hintergrund ist, dass § 15 Abs. 3 TMG die Möglichkeit vorsieht, dass der Diensteanbieter Nutzungsprofile für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien bei Verwendung von Pseudonymen erstellen darf, sofern der Nutzer dem nicht widerspricht. Das bedeutet, dass der Webseitenbetreiber Tracking-Cookies wie Google Analytics auf seiner Webseite einsetzen darf, ohne dass der Nutzer in das Setzen der Cookies vorher einwilligt. Nach dem Wortlaut der Norm muss der

[20] BGH, Urteil vom 28. Mai 2020 – I ZR 7/16 –, NJW 2020, 2540 (2540).

Betreiber lediglich eine Möglichkeit bieten, dass der Nutzer die Cookies nachträglich wieder löschen kann (sog. „Opt-Out“).

Zwar hätte der deutsche Gesetzgeber bis 2011 den geänderten Art. 5 Abs. 3 ePrivacy-RL (Richtlinie 2002/58/EG) in den § 15 Abs. 3 TMG umsetzen müssen; dies ist jedoch nie geschehen.[21] Im Unterschied zu § 15 Abs. 3 TMG sieht Art. 5 Abs. 3 ePrivacy-RL vor, dass der Nutzer aktiv zustimmen muss, bevor Tracking-Cookies eingesetzt werden (sog. „Opt-In“). Es ist also eine Einwilligung zum Speichern der Cookies auf dem Gerät nötig.

Der BGH nahm nun in dem „Planet49“-Urteil eine „richtlinienkonforme Auslegung“ des § 15 Abs. 3 TMG vor.[22] Das Gericht hat die Norm entgegen ihrem Wortlaut so ausgelegt, dass sie die gleichen Regelungen wie die dazugehörige Richtlinie enthält. Der BGH legte den § 15 Abs. 3 TMG so aus, dass eine Einwilligung (Opt-In) beim Einsatz von Tracking-Cookies nötig ist.[23] Aufgrund der Auslegung des BGH, erntete dieser scharfe Kritik aus der Lehre.[24] Interessant ist auch, dass der BGH die DSGVO und das TMG nebeneinander anwendbar sieht.[25]

b) Auswirkungen auf die Praxis

Für die Praxis bedeutet dies, dass in Zukunft eine Einwilligung zur Nutzung von Tracking-Cookies, insbesondere beim Einsatz von Google Analytics, eingeholt werden muss. Da es eine Vielzahl von Cookie-Bannern auf dem Markt gibt, werden hier nur die wichtigsten Rahmenbedingungen erläutert, die beim Einsatz von Cookie-Bannern wichtig sind.

Die Cookies dürfen nicht auf dem Gerät des Nutzers gespeichert werden, bevor er eingewilligt hat. In der Vergangenheit waren viele Cookie-Banner nur optisch aktiv und es wurden im Hintergrund bereits Cookies unabhängig von der Einwilligung ausgeführt. Es wird empfohlen, dass sich Verantwortliche mit einem Webprogrammierer zusammensetzen und gemeinsam die Cookies überprüfen.

Zudem wird bei Cookie-Bannern zwischen verschiedenen Arten von Cookies unterschieden, da manche keine Einwilligung erfordern. Beispielsweise benötigt ein Cookie für einen Einkaufswagen in einem Webshop keine Einwilligung, weil dafür Art. 6 Buchst. b DSGVO als Rechtsgrundlage in Frage kommt. Diese Rechtsgrundlage gestattet

[21] *Spindler/Schuster/Nink*, 4. Aufl. 2019, TMG § 15 Rn. 3.
[22] BGH, Urteil vom 28. Mai 2020 – I ZR 7/16 –, NJW 2020, 2540 (2545 f.).
[23] *Stender-Vorwachs/Steege*, Anmerkung zu BGH, Urteil vom 28.5.2020 – I ZR 7/16 – Cookie-Einwilligung II,
[24] Ebd.; *Rauer/Bibi*, Anmerkung zu BGH, Urteil vom 28.5.2020 – I ZR 7/16 – Cookie-Einwilligung II, ZUM 2020, 887 (889); *Moos/Strassemeyer*, Der gestalterische Spielraum für Einwilligungserklärungen nach BGH Cookie-Einwilligung II, DSB 2020, 207 (209).
[25] BGH, Urteil vom 28. Mai 2020 – I ZR 7/16 –, NJW 2020, 2540 (2544).

dem Verantwortlichen die Datenverarbeitung, wenn sie zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Diese Cookies sind meistens mit „essentiell" in einem Banner gekennzeichnet. Andere Cookie-Kategorien wie „Statistik" oder „Marketing" sind einwilligungsbedürftig und deshalb extra aufgeführt. Google Analytics fällt in den Bereich „Statistik".

Viele Cookies-Banner erlauben dem Nutzer, die einzelnen Kategorien zu akzeptieren oder zu bearbeiten. Allerdings setzen Webseitenbetreiber oftmals bei den einwilligungsbedürftigen Kategorien bereits ein Kreuz, das der Nutzer nicht selbst angeklickt hat. Dies ist rechtlich einem Opt-Out gleichzusetzen und ist deshalb nicht zulässig. Damit muss der Cookie-Banner so konfiguriert werden, dass der Nutzer aktiv die einzelnen Kategorien ankreuzen muss. Außerdem muss der Nutzer die Möglichkeit erhalten, neben den Kategorien auch die einzelnen Cookies auszuwählen bzw. zu entfernen.

Ferner haben manche Webseitenbetreiber in der Vergangenheit ein Scrollen auf der Webseite einer Einwilligung gleichgesetzt. Allerdings sieht der ESDA in seiner Stellungnahme 05/2020 vor, dass durch das Scrollen keine Einwilligung vorliegt.

Eine Einwilligung in eine Datenverarbeitung bedarf immer der Freiwilligkeit. Dementsprechend darf der Nutzer keine Nachteile haben, wenn er nicht einwilligt. Auch in diesem Fall muss der Webseitenbetreiber dem Nutzer den Zugang der Website ermöglichen. Manche Nachrichtenseiten bieten derzeit die Möglichkeit an, entweder die Cookies zu akzeptieren oder ein kostenpflichtiges Abonnement abzuschließen. Diesbezüglich prüfen derzeit die Datenschutzbehörden, ob bei den Verlagshäusern ein Verstoß gegen die DSGVO vorliegt.

Ferner muss ein einfacher Widerruf der Einwilligung möglich sein. Bei den meisten Cookie-Banner erfolgt dies, indem man dort die einzelnen Cookies oder die Kategorie widerruft. Webseitenbetreiber müssen insofern darauf achten, dass der Cookie-Banner nach der Einwilligung wieder aufgerufen werden kann. Beispielsweise lassen einige Cookie-Banner einen Fingerabdruck unten links erscheinen oder verlinken sich in der Datenschutzerklärung. Allerdings muss nach Ansicht mancher Datenschutzbehörden im Footer der Webseite ein Link zum Cookie-Banner mit dem Text „Cookie-Einstellungen" verlinkt sein, der beim Öffnen des Links erscheint.

Letztlich müssen dem Nutzer umfangreiche Informationen über die eingesetzten Cookies gegeben werden. Dazu zählen unter anderem Zweck der Verarbeitung, Rechtsgrundlage, Datenkategorien, Empfänger, Speicherdauer etc. Diese Informationen können in dem Cookie-Banner integriert werden und müssen zwingend in der Datenschutzerklärung

vorhanden sein. Somit kann der Webseitenbetreiber dem Nutzer die Informationen geben, indem er die die Datenschutzerklärung im Cookie-Banner verlinkt.

IV. Zusammenfassung

Der Einsatz von Google Analytics bringt viele rechtliche Herausforderungen mit sich. Nimmt der Nutzer bestimmte Änderungen an den Kontoeinstellungen vor, kann er allerdings ein vertretbares Datenschutzniveau erreichen.

Das größte Risiko liegt hierbei in der Nutzung von Drittanbietern aus den USA, da personenbezogene Daten in unsichere Drittstaaten übertragen werden. Durch geeignete Maßnahmen und eine stets vollständige Dokumentation der Einzelprüfung kann eine vertretbare Lösung geschaffen werden. Verantwortliche sollten sich allerdings überlegen, ob der Einsatz von europäischen Tracking-Anbietern oder auch Open Source Webanalysediensten wie *Matomo* geeigneter ist.

Google hat angekündigt, ab 2022 komplett auf Tracking Tools zu verzichten und stattdessen sog. „Sandbox-Lösungen" zu etablieren. Diese Maßnahme wird in der Datenschutzliteratur unterschiedlich bewertet. Wie genau Google die Alternative umsetzt, wird sich erst noch zeigen.

Auf europäischer Ebene soll mit der ePrivacy-VO Rechtssicherheit geschaffen werden. Ursprünglich sollte die ePrivacy-VO gemeinsam mit der DSGVO 2018 in Kraft treten, doch der Prozess verzögert sich auf europäischer Ebene und die ePrivacy-VO wird nicht vor 2023 in Kraft treten. In Deutschland befindet sich derzeit das Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) im parlamentarischen Gesetzgebungsprozess, das u.a. die Regelungslücke aus § 15 Abs. 3 TMG schließen soll.