BÜSING MÜFFELMANN & THEYE
BREMEN
FRANKFURT AM MAIN
BERLIN
MÜNCHEN

BÜSING MÜFFELMANN & THEYE MAXIMILIANSTRASSE 38, 80539 MÜNCHEN

**Dr. Christian Weitzel**
Rechtsanwalt

SEKRETARIAT Daniela Stoll
TELEFON 089 / 287007-0
TELEFAX 089 / 287007-29
E-MAIL weitzel@bmt.eu

STAND: 20.2.2018

# Web Analytics und Like-Buttons als DS-GVO-Auftragsverarbeitung

## Inhaltsverzeichnis

Seite



## 1. Auftragsverarbeitung – war früher alles besser?

Unter dem alten Bundesdatenschutzgesetz war Auftragsdatenverarbeitung (so hieß sie unter dem alten BDSG) „privilegiert": Im EWR brauchte sie keine gesonderte Rechtsgrundlage.

Eineinhalb Jahre nach Erlass der DS-GVO blieb unklar, ob diese Privilegierung nun entfallen sollte – oder ob Auftragsverarbeitung (so lautet der kürzere Gesetzesbegriff ab jetzt) wie eine eigene Verarbeitung zu behandeln ist. Die Meinungen in Kommentaren, Aufsätzen und Aufsichtsbehörden gingen in die eine oder andere Richtung. Seit dem 16.1.2018 kann man nun von einer herrschenden Meinung ausgehen: Die Datenschutzbehörden von Bund und Ländern haben in der Datenschutzkonferenz eine einheitliche Meinung gefasst und veröffentlicht im „Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO".

Dort heißt es: Der „aufgrund eines Auftrages tätige Dienstleister (…) führt daher die Verarbeitung für den Auftraggeber nicht als Dritter i.S.d. Art. 4 Nr. 10 DS-GVO durch. (…) Die Verarbeitung durch den Auftragsverarbeiter wird deshalb grundsätzlich dem Verantwortlichen zugerechnet."

Genau gesehen geht die Privilegierung durch die DS-GVO also weiter als das alte BDSG. Unter § 3 des alten BDSG war nämlich nur die Auftragsdatenverarbeitung im EWR privilegiert. Ab dem 25. Mai 2018 braucht es für keine Auftragsverarbeitung mehr eine gesonderte Rechtsgrundlage. Damit keine Missverständnisse aufkommen: Einen Vertrag zur Auftragsverarbeitung braucht es gleichwohl. Und die Übermittlung an Auftragsverarbeiter in EU-Drittländer unterliegt strengen Anforderungen. Ohne Beachtung dieser Vorgaben ist sie unzulässig.

Bei der Vorbereitung auf die DS-GVO fragen sich Unternehmen, Behörden und Vereine daher immer wieder: Ist dies oder jenes wirklich Auftragsverarbeitung? Und müssen wir entsprechende Verträge entwerfen und abschließen?

## 2. Web Tracking und Web Analytics unter dem alten BDSG

Fast jede Homepage nutzt heute Analysemethoden, um die Nutzung einzelner Seiten prüfen und verbessern zu können. Dazu dienen Statistik-Tools („Web Analytics") oder noch genauere Tools, die jede Bewegung des Web-Surfers genau verfolgen („Web Tracking").

Web Tracking ist für Werbetreibende bedeutsam. Wer sechsstellige Summen pro Jahr für Search Engine Marketing, Facebook Ads, Retargeting und gezielte Mailings investiert, will alle Details zur „Customer Journey" wissen, z.B: Auf welcher Seite mit welchen Inhalten hat der Nutzer einen Display-Klick vorgenommen, über welche Adword- und SEO-Klicks ist er dann zu welcher Preissuchmaschine und schließlich zum Online-Shop gelangt? Die dazu erforderlichen Tracking-Codes in Websites einzubinden, bereitet hohen Aufwand. Große Websites (wie z.B. Stern online) nutzen bis zu dreißig verschiedene Tracking-Codes auf einer einzelnen Seite!

Unzählige Anbieter überschwemmen dazu den Markt. Ob große kommerzielle Anbieter wie Adobe Analytics oder der Marktpionier Webtrends, kleinere wie Webtrekk mit Q3, Open Source-Tools wie Piwik, oder e-Commerce-Suiten wie Open Web Analytics: Alle diese Tools bereiten schon heute und erst recht ab dem 25. Mai 2018 mehr oder weniger Probleme, sie gesetzkonform zu konfigurieren und implementieren.

Wer sich Geld und Mühe spart, nutzt meist Google Analytics. Das Tool ist kostenlos verfügbar und schnell in die Homepage eingebunden. Deshalb verfügt es über einen Marktanteil von derzeit über 80 %. Nur läuft es stets über Server von Google in den USA, an die Daten übermittelt werden.

Schon unter Geltung des alten BDSG war deshalb klar: Google Analytics ist Auftragsverarbeitung und benötigt einen Vertrag zur Auftragsdatenverarbeitung nach § 11 BDSG (alt). Das und eine abgestimmte Vorlage hatten die Aufsichtsbehörde mit Google so vereinbart. Der sehr komplexe und einseitige Vertrag ist hier abrufbar: http://static.googleusercontent.com/media/www.google.com/de//analytics/terms/de.pdf.

Nach dem alten BDSG brauchte es noch einen schriftlichen Vertrag. Nur haben Betreiber vor Life-Schaltung ihrer Homepage diesen Vertrag fast nie von Google gegenzeichnen lassen.

## 3. Neuerungen unter der DS-GVO

Nach Art. 28 Abs. 9 DS-GVO kann ein Auftragsverarbeitungsvertrag auch in elektronischer Form geschlossen werden. Ab dem 25. Mai 2018 braucht es daher keine Papierform mehr. So weit, so gut!

Neu ist ferner, dass die Auftragsverarbeitung auch in EU-Drittländern keine gesonderte Rechtsgrundlage mehr braucht, sondern nur noch zusätzliche Garantien. Das gilt allerdings nur für die Auftragsverarbeitung an sich – eine *Übermittlung* in EU-Drittländer unterliegt hingegen strengen Anforderungen (dazu näher unter Ziffer 6).

## 4. Google Analytics: Auftragsverarbeitung und noch mehr

Für die gesetzlichen Anforderungen des Datenschutzes kommt es auch noch darauf an, ob die Web-Analyse nur für Zwecke des Website-Betreibers erfolgt – oder ob der Anbieter des Analytics-Tool noch Daten für eigene Zwecke erhält. So ist es z.B. bei Google Universal: Google nutzt die übermittelten Daten für eigene Zwecke.

Dann hilft die „Privilegierung" der Auftragsdatenverarbeitung nichts mehr, es handelt sich nämlich um Datenübermittlung an Dritte, die personenbezogene Daten zu eigenen Zwecken verarbeiten.

Das wiederum bedarf einer ausdrücklichen Einwilligung (dazu näher unter Ziffer 7).

## 5. Verhalten von Google

Google macht sich das Leben leicht. So untersagen die Nutzungsbedingungen für Google Analytics die Erfassung personenbezogener Daten. Auf die Weise erfüllt Google zwar die Anforderungen des Datenschutzrechts und suggeriert, es brauche keine Einwilligung. Andererseits ignoriert Google ganz bewusst, dass die meisten Nutzer ihrer Tools dieses Verbot gar nicht einhalten.

Denn Google verlagert Aufwände und Kontrolle auf den Website-Betreiber. Dem ist oft gar nicht klar, wie schnell und wie viele personenbezogene Daten er unbemerkt an Google übermittelt. Ohne Kenntnis von Website-Programmierung entgehen ihm ganz schnell personenbezogene Daten (und seien es nur dynamische IP-Nummern, siehe BGH-Urteil vom 16.5.2017, VI ZR 135/13) in Form von:

- URL-Parametern für Formulare, Logins oder Bestätigungs-eMails
- UTM-Parametern für Kampagnen-Berichten
- Benutzerdefinierten Dimensionen und Ereignisse
- Nicht gehashten User IDs
- Unmaskierten IP-Nummern

Kurzum: Kaum eine Website mit Google Analytics ist so programmiert, dass sie ohne eine Vereinbarung zur Auftragsverarbeitung auskommt.

Auf der anderen Seite macht es Google schwer zu verstehen, wer welche Daten wohin übertragen bekommt. Selbst die aktuelle „Google Privacy Policy" (abrufbar im Web unter https://www.google.com/intl/en/policies/privacy/) bleibt auffällig unklar über die Verwendung gesammelter Daten („Zwecke" im Sprachgebrauch der DS-GVO), die Zusammenführung von Daten und die Weiterleitung an ungenannte „Partner" und „Affiliates". Die Transparenzanforderungen der DS-GVO erfüllt diese Policy definitiv nicht.

## 6. DS-GVO-Anforderungen auch für Web Analytics?

„Echt jetzt?" – fragen kleine Vereine und Firmen. Wir sollen für Google Analytics Auftragsverarbeitungs-Verträge abschließen? Ganz klar: Ja. Das war schon Rechtslage vor 2016, als die DS-GVO erlassen wurde.

Es sei denn, der Website-Betreiber weist nach, dass nicht die geringsten personenbezogenen Daten an fremde Server übermittelt werden!

## 7. Was heißt das nun konkret – was muss ich tun?

Es kommt noch schlimmer: Jetzt braucht es für die Auftragsverarbeitung eine Einwilligung durch jeden Nutzer der Website – und zwar schon, bevor das Web Analytics Tool mit seiner Arbeit einsetzt. Das erfordert eine entsprechende Programmierung der Website. Und der Betreiber muss sich um die Einholung, Nachweis der Freiwilligkeit und Dokumentation der Einwilligungen kümmern. Zudem muss er mit dem jederzeit möglichen Widerruf der Einwilligung umgehen und jene Nutzer dann vom Web Tracking ausnehmen!

Es ist gar nicht so einfach, eine wirksame Einwilligung für Web Analytics einzuholen:

- Die Einwilligung muss freiwillig (Art. 7 Abs. 4 DS-GVO) und nach ausreichender Information in einfacher, verständlicher Sprache erfolgen (Art. 7 Abs. 2 in Verbindung mit Art. 13 DS-GVO).
- Der Nutzer muss sie unmissverständlich erklären. Da reicht kein verstecktes Ankreuzfeld, das womöglich schon ausgefüllt ist („opt-out"!
- Für jede Art der Datenverarbeitung braucht es eine gesonderte Zustimmung. Wer personalisierte Inhalte nutzt, Web Analytics, den Einsatz von first-party-cookies und auch noch third-party-cookies, braucht also vier getrennte Einwilligungen!
- Minderjährige bis 16 Jahre dürfen nur mit Zustimmung eines Erziehungsberechtigten einwilligen (Art. 8 Abs. 1 DS-GVO). Davon muss sich der Website-Betreiber mit angemessenen Anstrengungen überzeugen (Art. 8 Abs. 2 DS-GVO), außer es hat – was auch zulässig ist – der Erziehungsberechtigte für sein Kind eingewilligt.
- Vor Abgabe der Einwilligung müssen Sie den Nutzer über sein Recht zum Widerruf informieren (Art. 7 Abs. 3 DS-GVO).

Dann muss noch eine einfache Möglichkeit zum Widerruf einzelner oder aller Einwilligungen eingerichtet sein (Art. 7 Abs. 3 DS-GVO). Ein Link auf der Homepage oder – noch besser – ein einfach einzubindendes Widget wäre dazu geeignet. Noch stellt allerdings kaum ein Anbieter von Analyse-Tools solche Mittel in DS-GVO-konformer Ausprägung zur Verfügung.

Nun weiter zur Speicherung und Nachweisführung zu allen Einwilligungen, die es nach Art. 7 Abs. 1 DS-GVO braucht. Wenn die Einwilligungen – der Bequemlichkeit halber – beim Anbieter des Tools gespeichert sind, muss der Website-Betreiber für ständigen Zugriff und ausreichend lange Speicherung sorgen. Sonst kann er seinen Nachweispflichten gegenüber Aufsichtsbehörden und – im Rechtsstreit – gegenüber Betroffenen nicht nachkommen.

Letzter Punkt: Privacy bei Design und Privacy by Default, so lauten wichtige Grundsätze des neuen Datenschutzrechts. Personenbezogene Daten dürfen nur in geringstmöglichem Umfang gesammelt, gespeichert und verarbeitet werden. Eine uferlose Speicherung und Analyse aller Nutzer ist mit diesen Grundsätzen nicht vereinbar. Die eingesetzte Web-Analyse sollte da so weit wie möglich anonym erfolgen – dazu gehört schon die Entfernung der IP-Nummer der Surfer!

Zu diesem Zweck bieten einige Hersteller geeignete Tag Management Systeme an. Diese ermöglichen genaue Voreinstellungen, welche Daten sie genau sammeln.

**Kurzum:**
Web Tracking ist noch möglich. Aber die zum Beispiel von Google praktizierte Datensammlung, deren Ausmaß vor allem bei Google Universal Analytics kaum steuerbar und einsehbar ist, dürfte ab dem 25. Mai 2018 nicht mehr zulässig sein. Ob und wie Google jenes Produkt bis dahin dem EU-Recht anpasst, bleibt spannend!

## 8. Das leidige Thema Ausland

Meist ist es so, dass die Anbieter von Analytics-Tools auf Cloud-basierter Software as a Service-Basis Daten in EU-Drittländer übertragen, häufig in die USA.

Grundsätzlich bedarf die Übertragung personenbezogener Daten in EU-Drittländer einen von fünf Erlaubnistatbeständen: (1) Angemessenheitsbeschluss der EU-Kommission (wie z.B. für Kanada), (2) Abschluss von EU-Standarddatenschutzklauseln, (3) Vereinbarung von der Aufsichtsbehörde genehmigter verbindlicher interner Datenschutzvorschriften („Binding Corporate Rules"), (4) genehmigte Verhaltensregeln („Code of Conduct") oder (5) Zertifizierung der Verarbeitungstätigkeit durch Aufsichtsbehörden oder akkreditierte Zertifizierungsstellen. Weitere in der DS-GVO genannte Gründe sind für Web Tracking nicht einschlägig.

Bedenken Sie: Viele Länder – wie etwa die gesamte USA – gelten nach EU-Datenschutzrecht als „unsicheres Drittland". Also bleibt nur die Auswahl unter den restlichen vier Varianten. Allerdings sind einige davon nur sehr zeitaufwändig abzuschließen, bis die Übertragung zulässig ist, und die letzte ist derzeit kaum realistisch. Viel gravierender: Die meisten Anbieter kostenloser Tools bieten keine dieser Möglichkeit.

Dann hilft nur eines: Die Einwilligung aller betroffenen Nutzer in die Übermittlung ihrer personenbezogenen Daten ins Ausland. Die einzuholen wird noch aufwendiger und weniger erfolgsträchtig sein als die – gesondert abzufragende – Auftragsdatenverarbeitung.

## 9. Zehn Praxistipps

Wie kann man dem schwierigen Thema ab dem 25. Mai 2018 noch beikommen? Hier sind wichtige Handlungsempfehlungen in Form einer 10-Punkte-Liste:

1. Nutzen Sie für externe Speicherung oder Web Analytics-"Services" Server, die in der EU aufgestellt sind und keine Daten an Server oder Unternehmen außerhalb der EU übermitteln (also nicht „irgendwo" in der Cloud).

2. Besser noch: Installieren Sie Analyse-Tools nur auf ihren eigenen Webservern. So vermeiden Sie die Gefahren einer Datenübermittlung oder unzureichender Schutzvorkehrungen, Verträge und Einwilligungen für die Auftragsverarbeitung.

3. Wenn Sie einen externen „Service" für Web Tracking nutzen: Stellen Sie sicher, ob und wo der Service personenbezogene Daten verarbeitet. Für den Fall schließen Sie eine Auftragsverarbeitungsvereinbarung. Und regeln Sie genau die Pflichten und Zusammenarbeit mit dem Anbieter, um die Betroffenenrechte nach der DS-GVO erfüllen zu können (Auskunftsanspruch, Berichtigungsanspruch, Löschungsanspruch etc.). Das wird Ihnen kaum einer der kostenlosen Anbieter ermöglichen …

4. Ermitteln Sie genau die von Ihrem Analyse- oder Tracking-Tool aufgezeichneten – und vor allem die an fremde Server übermittelten – Daten.

5. Reduzieren Sie die Menge an personenbezogenen Daten, die Sie für die Web-Analyse sammeln. Verzichten Sie am besten ganz auf Cookies – die braucht es nicht (außer für Google und Facebook, die ganz gezielt Nutzerdaten sammeln und auswerten). Ansonsten braucht es Opt-in Cookies (mit gesonderter Einwilligung!), wenn diese personenbezogene Daten verarbeiten und übermitteln.

6. Löschen oder maskieren Sie die gesammelten IP-Nummern, so dass insoweit kein Personenbezug mehr hergestellt werden kann. Dasselbe gilt für andere Online-Identifier. Bei Google Analytics erfordert das eine gesonderte Parametrisierung.

7. Damit landet Google Universal Analytics auf der Ausschlussliste. Derzeit ist noch nicht absehbar, ob und wie Google dieses Tool DS-GVO-konform ausgestalten will oder wird. Nur Google Classic Analytics lässt sich mit sorgsamer Programmierung, umfangreicher Parametrisierung und Vertrauen in Googles Ehrlichkeit DS-GVO-konform einsetzen. Beim kommerziellen Google Analytics 360 bedarf es sehr genauer Prüfung und Parametrisierung, um DS-GVO-konform zu handeln.

8. Vergessen Sie also den hippen Trend „targeted advertising" und deaktivieren Sie bei Google Analytics die Werbefunktion („Remarketing"), die Berichte zu Impressionen im Google Displaynetzwerk, die Google Analytics-Berichte zur Leistung nach demografischen Merkmalen und Interessen sowie alle Dienste, für die Daten für Anzeigenvorgaben und Kennungen mit Cookies gesammelt werden – oder machen Sie sich die enorme Mühe, hierfür gesonderte Einwilligungen einzuholen und alle datenschutzrechtlichen Anforderungen zu erfüllen. Seien Sie nicht enttäuscht, wenn die Kosten-Nutzen-Analyse dafür ein negatives Ergebnis hat!

9. Lassen Sie sich nicht einwickeln, wenn Werbepartner Ihnen gegenüber ein „berechtigtes Interesse des Verantwortlichen oder eines Dritten" nach Art. 6 Abs. 1 Buchstabe f) DS-GVO ins Feld führen! Denn auch dann müssen Sie Ihre Nutzer transparent und umfassend über die vorgesehenen Werbemaßnahmen informieren. Nur: Wer macht das schon und welcher Werbetreibender legt seine geplanten Maßnahmen offen?

10. Zum Schluss, ganz wichtig: Überlegen Sie, ob und wie Sie die Nutzung Ihrer Homepage auch ohne Einwilligung und Web Analytics ermöglichen. Sonst schließen Sie eine Menge Nutzer aus. Ist es Ihnen das wert?

**Fazit:** Wenn Sie bislang einen einfachen, kostengünstigen Web Analysis- oder Tracking-Service nutzen, werden Sie sich mit großer Sicherheit umstellen müssen. Suchen Sie rasch einen Anbieter, der Ihnen datenschutzkonforme Lösungen, Einstellungen, Speicherung und Nachweisbarkeit bietet! Und sorgen Sie dafür, dass diese Lösung bis Mai 2018 installiert und getestet ist!

## 10. Was ist mit dem Like-Button von Facebook?

Zum Abschluss werden sich einige Leser fragen: Was ist denn dann mit dem Like-Button von Facebook oder vergleichbaren Social Media-Plugins?

Die Antwort ist klar: Es gibt keinen Unterschied zu Web Tracking mit Übermittlung von Daten zu und für Dritte, wenn das Plugin personenbezogene Daten verarbeitet und überträgt. Ohne ausreichende Information, freiwillige Einwilligung und Abschluss einer Auftragsdatenvereinbarung ist der Einsatz nicht zulässig.

**Fazit:**
Solange Facebook keine vollständige und transparente Information über Nutzung und Weiterleitung der erhobenen Daten zur Verfügung stellt, ist der Einsatz von Facebook-Like-Buttons spätestens ab dem 25. Mai 2018 nicht mehr ratsam – allenfalls mit einem komplizierten und wenig akzeptablem „Double Opt-In" sowie einem fachgerechten Auftragsverarbeitungsvertrag mit der Facebook Inc.