

# Datenschutz

Ratgeber zum  
Umgang mit Web Analyse-Daten



## Hintergrund: Warum ist Datenschutz so wichtig?

- 1. Rechtliche Konsequenzen:** Website-Betreiber, die das Thema Datenschutz außer Acht lassen, laufen Gefahr, abgemahnt zu werden oder gar ein hohes Bußgeld zahlen zu müssen. Abmahnungen können richtig teuer werden und sogar die Existenz bedrohen. Das Landgericht Hamburg hat beispielsweise in einer einstweiligen Verfügung vom 10.03.2016 (Az. 312 O 127/16) den Einsatz von Google Analytics untersagt, wenn die Betreiber der Webseite die Nutzer nicht zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten unterrichten. Für den Fall der Zuwiderhandlung drohte das Gericht ein Ordnungsgeld bis zu 250.000 Euro und ersatzweise Ordnungshaft bis zu sechs Monaten an. Die ab dem 25. Mai 2018 zur Anwendung kommende Europäische Datenschutz-Grundverordnung (EU-DS-GVO) sieht bei Verstößen gegen den Datenschutz sogar Strafen in Höhe von bis zu 20 Mio. Euro oder 4 % des gesamten weltweit erzielten Jahresumsatzes des vergangenen Geschäftsjahres vor.
- 2. Vertrauen:** Kunden verlieren das Vertrauen in Ihr Unternehmen, wenn sie das Gefühl haben, dass Sie fahrlässig oder unrechtmäßig mit ihren Daten umgehen. Nutzer schrecken vor der Vision eines „gläsernen Besuchers“ zurück und sind durch diverse Datenpannen und -missbrauchsskandale sensibilisiert. Wer hingegen aus der Pflicht eine Tugend macht und demonstriert, dass er besonders verantwortungsvoll mit den Daten umgeht und die Privatsphäre der Besucher schützt, kann seine Vertrauenswürdigkeit verstärken und sich positiv von Marktbegleitern abheben.
- 3. Datenabfluss und -hoheit:** Website- bzw. Kundendaten sind das wertvollste Gut für den Erfolg Ihres Online-Business. Geben Sie dieses niemals aus der Hand. Stellen Sie sicher, dass keine unerwünschte Datenweitergabe oder -nutzung erfolgt und Sie die vollständige Hoheit über Ihre Daten erhalten. Schlimmstenfalls bleibt es Ihnen nicht nur verwehrt, weitergehende Analysen mit den Daten durchzuführen oder diese für eine gezieltere Ansprache zu verwenden, sondern Ihre Daten werden für die Aussteuerung von Werbung Ihrer Wettbewerber nutzbar gemacht. Gerade US-Anbieter erlauben gerne mal in den Standard-Einstellungen, dass sie Ihre Daten zur „Verbesserung“ ihrer Produkte und Dienste nutzen dürfen. Was das konkret bedeutet und wo die Grenze ist, bleibt offen.

## Die Rechtsgrundlage in Deutschland und Europa

Für Deutschland sind das Bundesdatenschutzgesetz (BDSG) und das Telemediengesetz (TMG) die vorrangige Rechtsnorm. Weiterhin sollten Website-Betreiber mit den Beschlüssen des Düsseldorfer Kreises vom November 2009 vertraut sein.

In Europa gilt ab dem 25. Mai 2018 die Datenschutz-Grundverordnung. Diese soll von der ePrivacy Verordnung flankiert werden, die die elektronische Kommunikation mit den Verbrauchern regelt. Mit der Europäischen Datenschutz-Grundverordnung werden sich die bestehenden Spielregeln in Deutschland jedoch nicht grundlegend ändern, baut sie doch auf bewährte Grundsätze auf.

Die folgenden Tipps helfen Ihnen dabei, die größten Stolperfallen zu vermeiden:

### Tipp 1 – Datenschutzerklärung

Informieren Sie Ihre Website-Besucher in einem extra Menüpunkt über Zweck und Umfang der Datenerhebung und -speicherung sowie über die Erstellung von Nutzerprofilen. Eine solche Datenschutzerklärung ist in Deutschland Pflicht.

**Bei Einsatz von etracker:** Einen geprüften Mustertext finden Sie unter Account Info > Einstellungen > Account > Widerrufsmöglichkeit über 1st-Party Cookie und Tracking Opt-in.

## Tipp 2 – Widerspruchsmöglichkeit

In der Datenschutzerklärung sollte auf die Möglichkeit zum Widerspruch der Datenerfassung (Opt-out) hingewiesen werden. Als Website-Betreiber haben Sie nach dem Einspruch die Pflicht, den aktiven Ausschluss eines Besuchers aus der Datenerfassung sicherzustellen und/oder die entsprechenden Daten zu löschen.

Anders als in Deutschland, verlangen einige EU-Länder die ausdrückliche Einwilligung des Website-Besuchers noch vor Beginn des Trackings (Tracking Opt-in) oder Einsatzes von Cookies (Cookie Opt-in). Um diese Anforderung umzusetzen, wird ein Tracking-System benötigt, welches flexibel Opt-out sowie differenziertes Cookie- und Tracking-Opt-in unterstützt. Denn wenn von Rechts wegen auch das Einverständnis zum Setzen von Cookies verlangt wird, muss ja nicht auf das Erfassen von Besuchsdaten verzichtet werden.

**Bei Einsatz von etracker:** Der Mustertext unter Account Info > Einstellungen > Account > Widerrufsmöglichkeit über 1st-Party Cookie und Tracking Opt-in enthält bereits einen entsprechenden Widerrufsbutton. Einfach Ihre Domain eintragen, in Ihre HTML-Seite übernehmen, fertig. Wollen Sie anstelle des bereitgestellten Widerrufsbuttons eine eigene Funktion oder eigenes Design integrieren, so steht Ihnen die Widerrufsfunktion auch als Link und JavaScript-Funktion zur Verfügung.

## Tipp 3 – Achtung personenbezogene Daten

Web Analyse-Daten dürfen standardmäßig nur anonymisiert oder pseudonymisiert erfasst werden. Diese Anforderung ist erfüllt, wenn sich hinter einem Datensatz fünf oder mehr Personen verbergen können beziehungsweise ein Personenbezug nur mit unverhältnismäßig großem Aufwand hergestellt werden kann. IP-Adressen dürfen ohne Einwilligung weder vollständig verarbeitet noch gespeichert werden. Vielmehr müssen sie so früh wie möglich bei der Annahme gekürzt werden.

Auch wenn der Ruf nach zentraler Datenhaltung und dem Ende von Daten-Silos laut wird, dürfen Web Analyse-Daten nicht ohne Einwilligung mit personenbezogenen Daten zusammengeführt werden. Genauso muss bei UX- beziehungsweise CX-Analyse darauf geachtet werden, dass bei Session Replays Formulareingaben und persönliche Daten von der Aufzeichnung ausgeschlossen werden.

**Bei Einsatz von etracker:** Die IP-Kürzung erfolgt standardmäßig. In der UX-Analyse werden Formulareingaben automatisiert durch Sternchen ersetzt und Seitenelemente mit persönlichen Angaben können von der Aufzeichnung ausgenommen werden.

## Tipp 4 – Auftragsdatenvereinbarung

Da für die Sammlung von Daten meist Tools von Drittanbietern genutzt und die Daten entsprechend auf fremden Servern gespeichert werden, schließen Sie mit dem Anbieter eine Auftragsdatenvereinbarung (ADV) entsprechend der Anforderungen nach §11 des BDSG ab. Dieser Vertrag bedarf immer der Schriftform.

Wichtig zu wissen: Als Auftraggeber bleibt die Verantwortung für die datenschutzkonforme Verarbeitung immer bei Ihnen. Im Falle eines Verstoßes gegen den Datenschutz werden Sie haftbar gemacht.

**Bei Einsatz von etracker:** Sie können eine Auftragsdatenvereinbarung mit etracker schließen, indem Sie die Vereinbarung unter Account Info > Einstellungen > Account > Datenschutzoptionen herunterladen, ausdrucken, datieren, unterzeichnen und ein Exemplar an die etracker GmbH per Brief oder Fax zurücksenden. Sie erhalten die von der etracker GmbH unterschriebene Fassung per Fax zurück.

## Tipp 5 – Öffentlicher Bereich

Für öffentliche Stellen gelten gesonderte und strengere Anforderungen als für den nicht-öffentlichen Bereich. Hierzu zählt je nach Bundesland, dass einem Auskunftersuchen des Landesdatenschutzbeauftragten angemessen entsprochen werden muss und Dienstleister sich verpflichten, sich der Kontrolle des Landesdatenschutzbeauftragten zu unterwerfen. Nach Auskunft der Hessischen Aufsichtsbehörde will Google diese Anforderungen nicht erfüllen.

**Bei Einsatz von etracker:** Eine Vereinbarung zur beanstandungsfreien Nutzung von etracker im öffentlichen Bereich kann mit entsprechender Verpflichtungserklärung durch etracker abgeschlossen werden.

## Tipp 6 – Rechtliches Risiko Google Analytics

Die USA gilt nach europäischem Datenschutzrecht als unsicheres Drittland. Daten Ihrer Kunden und Nutzer dürfen ohne explizite Einwilligung beziehungsweise ohne Sicherstellung eines angemessenen Datenschutzniveaus nicht dorthin übermittelt werden. Letzteres sollte das Safe-Harbor-Abkommen gewährleisten, bis der Europäische Gerichtshof es im Oktober 2015 für unwirksam erklärte. Auch der im Juli 2016 von der Europäischen Kommission angenommene Nachfolger, der EU-US Privacy Shield, stand von Anfang an in der Kritik und bringt keine absolute Rechtssicherheit. Wenn die US-Regierung ihre Zusagen nicht einhält oder die ausgehandelten Voraussetzungen ändert, droht die Kündigung des Abkommens.

Ob eine datenschutzkonforme Nutzung des Dienstes Google Analytics dauerhaft beanstandungsfrei möglich sein wird, ist daher sehr ungewiss. Im Übrigen gelten die Hinweise zum beanstandungsfreien Betrieb von Google Analytics lediglich in Bezug auf die Standardimplementierung von Google Analytics, auch wenn dies nur wenig deutlich wird.

Bei Nutzung der Google Analytics-Werbefunktionen ist eine Einwilligung des Nutzers erforderlich. Zu den Werbefunktionen gehören Remarketing mit Google Analytics, Berichte zu Impressionen im Google Displaynetzwerk, Berichte zur Leistung nach demografischen Merkmalen und Interessen sowie integrierte Dienste, für die in Google Analytics Daten mithilfe von Cookies für Anzeigenvorgaben und Kennungen gesammelt werden.

**Bei Einsatz von etracker:** Die Datenspeicherung findet garantiert und ausschließlich in Deutschland statt. Dadurch entstehen aktuell und zukünftig keine Rechtsunsicherheiten aufgrund von Datenübermittlung in Drittländer außerhalb der EU.