Whitepaper Webanalyse und Datenschutz

Webanalyse gibt jedem Webseitenbetreiber wertvolle Hinweise auf das Gesamtkonzept einer Online-Präsenz, informiert über das Nutzerverhalten zur Optimierung der Webseiten und unterstützt mit validen Informationen die Erreichung der unternehmerischen Ziele.

Von Anfang an stand die Webanalyse im Fokus der Datenschützer. Vor allem beim Markteintritt von Google Analytics und anderen Anbietern für Webanalyse herrschte die Sorge, dass zu viele Daten gesammelt und ausgewertet würden. Der Internetkonzern musste sich dem Vorwurf erwehren, seine Webanalyse-Lösung nur zum Datensammeln ins Leben gerufen zu haben. Zusammengeführt mit Daten aus anderen Google-Diensten würden die Informationen über Besucherströme detaillierte Besucherprofile ergeben.

Mit dem „Whitepaper Webanalyse und Datenschutz" bietet die Unit Search im Bundesverband Digitale Wirtschaft (BVDW) e.V. eine umfangreiche Übersicht über die in Deutschland zu berücksichtigenden, datenschutzrechtlichen Anforderungen für die erfolgreiche Webanalyse. Das Whitepaper richtet sich an alle Webseitenbetreiber, die Google Analytics oder andere Webanalyse-Tools einsetzen und diese datenschutzkonform betreiben möchten. Die Unit Search liefert detaillierte Einblicke in die richtige Anwendung des Datenschutzrechts in Puncto Einwilligung, Hinweispflicht, Anonymisierung und Pseudonymisierung sowie Widerspruch und Löschung von Daten. Eine kurze Checkliste für den datenschutzkonformen Einsatz von Google Analytics rundet das Whitepaper ab.

Inhaltsübersicht

1. Anwendbarkeit des Datenschutzrechts
2. Datenschutzrechtliche Einwilligung
3. Hinweispflicht
4. Widerspruch
5. Anonymisierung durch IP-Masking
6. Vertrag über Auftragsdatenverarbeitung
7. Altdaten löschen
8. Pseudonymisierte Nutzungsprofile
9. Datenschutz-Checkliste
10. Zusammenfassung und Autoren

1. Anwendbarkeit des Datenschutzrechts

Grund für die Sorge der Datenschützer war nicht der Umstand, dass Google Analytics die Zuordnung und Speicherung von Nutzungsdaten (verwendeter Browser, zuletzt besuchte Seite etc.) ermöglicht. Die Erhebung von Daten über die Nutzungsaktivitäten begegnet grundsätzlich zunächst keinen rechtlichen Bedenken. Gegenstand der Kritik war und ist die Möglichkeit, das webseitenübergreifende Nutzungsverhalten über die ebenfalls abgespeicherte **IP-Adresse** einem konkreten Nutzer zuzuordnen. Neben der IP-Adresse erhält Google immer die **Identifikationsnummer** des „First Party Cookie", welches auf dem Rechner des jeweiligen Nutzers hinterlegt ist. Mithilfe dieser Cookies sowie der IP-Adresse ist es möglich, das Surfverhalten eines Nutzers über alle Webseiten nachzuvollziehen, welche mit Google Analytics arbeiten.

Datenschützer sowie einige deutsche Gerichte (vgl. LG Berlin v. 06.09.2007, Az.: 23 S 3/07; AG Mitte v. 17.03.2007, Az. 5 C 314/06) sind der Ansicht, dass es sich bei dynamischen IP-Adressen um personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes (BDSG) bzw. des Telemediengesetzes (TMG) handele. Der Europäische Gerichtshof (EuGH) hatte in einem aktuellen Urteil die Personenbezogenheit der dynamischen IP-Adresse bejaht (vgl. EuGH v. 24.11.2011, Az. C-7/10).

Diese Ansichten lassen sich indes nur vertreten, soweit man es ausreichen ließe, dass der Personenbezug nicht im Verhältnis Betroffener-Anbieter sondern von irgendjemandem hergestellt werden kann **(sog. absolute Personenbezogenheit)**. In dem konkreten Einzelfall des EuGH ging es um einen Access-Provider, dem die Zuordnung einer dynamischen IP-Adresse naturgemäß leichter fallen dürfte als anderen Diensten.

Diesen Auffassungen folgend, ist bei der Verwendung von Google Analytics daher das Datenschutzrecht immer zu beachten. Da es sich bei Google um einen Diensteanbieter im Sinne des § 2 Nr. 1 TMG handelt, wären hier vorrangig die Regelungen des TMG einschlägig.

Diese weitgehende Auslegung des Begriff der personenbezogenen Daten wird nicht von jedermann (auch nicht von Gerichten) geteilt (vgl. LG München v. 30.9.2008, Az. 133 C 5677/08). Personenbezug soll in Bezug auf ein konkretes Datum vielmehr immer erst dann vorliegen, wenn die konkret verarbeitende Stelle mit vertretbarem Aufwand eine Identifikation der natürlichen Person hinter der IP-Adresse

vornehmen könnte, sei es durch eigenes oder durch frei verfügbares Wissen **(sog. relativer Personenbezug)**. Eine endgültige Klärung dieser wichtigen Rechtsfrage steht jedoch noch aus.

Aufgrund der bei großen Webanalysten über die verschiedenen Dienste gesammelten Daten dürfte man nach beiden Ansichten aber nicht vollständig ausschließen können, dass ein Bezug zu einer bestimmbaren Person über die Nutzungsauswertungen nicht doch mit nur unerheblichem Aufwand gelänge. Wegen der leicht zu realisierenden Auswertung sämtlicher Daten durch ein und dasselbe Unternehmen kann ein Personenbezug möglicherweise tatsächlich relativ leicht hergestellt werden.

Die Datenschützer lassen sich von der Diskussion um diese Frage jedenfalls nicht beirren. Entsprechend hat der Düsseldorfer Kreis – der Zusammenschluss der Datenschützer der Länder und des Bundes – im Jahre 2009 eine Liste von zu berücksichtigenden Vorgaben[1] erstellt. Diese Liste gilt umfassend für alle Webanalyse-Dienste – nicht nur für Google Analytics.

Um als Nutzer von Webanalyse-Diensten also **unnötige Risiken zu vermeiden**, die sich um die Frage der Anwendbarkeit des Datenschutzrechts ranken empfiehlt die Unit Search im BVDW, die folgenden **datenschutzrechtlichen Hinweise zu beachten.**

2. Datenschutzrechtliche Einwilligung

Personenbezogene Daten wie Name, Adresse und Geburtsdatum dürfen für das Tracking per Webanalyse **grundsätzlich nur mit ausdrücklicher Einwilligung des Besuchers** verwendet werden. Soweit ein Webseitenbetreiber also Google Analytics verwendet, müsste er grundsätzlich zunächst vorab die Einwilligung des betroffenen Nutzers einholen, dass die Erhebung, Speicherung und Verarbeitung der personenbezogenen Daten erlaubt.

Die Voraussetzungen für eine wirksame Einwilligung nennen § 4a BDSG bzw. § 13 Abs.2 TMG. Insbesondere muss die Einwilligung muss vom Betroffenen „bewusst" und „eindeutig" erklärt werden. Eine solche Einwilligungserklärung kann daher nicht als eine unter vielen Erklärungen in die AGB aufgenommen werden. Vielmehr ist dem Nutzer separat die Möglichkeit zu geben, die Einwilligung (etwa durch Pop-up bei Aufruf der Webseite)

[1] Beschluss vom 26./27. November 2009

ausdrücklich zu erklären. Zuvor ist der Nutzer über Art und Umfang der Datenerhebung zu **unterrichten** (§ 13 Abs.1 S.3 TMG).

Im Falle der online abgegebenen Erklärung ist es zudem am Webseitenbetreiber sicherzustellen, dass die Einwilligung **protokolliert**, der Inhalt der Erklärung für den Nutzer **jederzeit abrufbar** bereit gehalten und der Nutzer über sein jederzeitiges **Widerrufsrecht** unterrichtet wird (§ 13 Abs. 2 TMG). Am besten werden die notwendigen Informationen in unmittelbarer Nähe zur anzuklickenden Checkbox bereitgehalten.

3. Hinweispflicht

Der Besucher muss zudem darüber **informiert** werden, dass seine Daten mit einem Webanalyse-System erfasst werden, wofür dies geschieht und wie mit seinen Daten im Anschluss umgegangen wird (§ 13 Abs.1 S. 3 TMG).

Die meisten Webanalyse-Dienste bieten dazu fertige Formtexte in ihren AGBs an, die am besten auf einer eigenen Datenschutzseite (Datenschutzerklärung) auf dem Webauftritt untergebracht werden. So auch Google, die weiterhin die Einbindung des AGB Textes als Voraussetzung zur Nutzung von Analytics erwarten. Diese und alle weiteren, datenschutzrechtlich notwendigen Informationen sollten sich in einer eigenen **Datenschutzerklärung** wieder finden, welche über eine Verlinkung von jeder Webseite aus abrufbar sein sollte.

4. Widerspruch

Dem Besucher der Webseite muss entsprechend der Information auch die tatsächliche Möglichkeit gegeben werden, **Widerspruch** gegen das Tracking **mit Wirkung für die Zukunft** erheben zu können. Um den Widerspruch wirksam umzusetzen, dürfen im Anschluss keine Daten dieses Besuchers mehr analysiert werden. Es gibt allerdings keine konkrete Vorgabe, wie diese Umsetzung auszusehen hat.

Google bietet hierfür ein Browser-Plug-in an, mit dem das Tracking von Google Analytics generell unterbunden werden kann. Aus Sicht der Landesbeauftragten für den Datenschutz ist die Widerspruchsmöglichkeit damit ausreichend gegeben. In der

aktuellen Vorlage für die Datenschutzerklärung der Webseite ist der Hinweis auf dieses Plug-in bereits integriert.
Andere Webanalyse-Anbieter realisieren den Widerspruch zentral auf ihrer Seite per **Opt-Out** Cookie. Der Toolanbieter bietet eine Seite mit Hinweistext, auf die von der jeweiligen Webseite verlinkt wird. Alternativ stellt er einen Inlineframe (iframe) zur Verfügung, den der Webseitenbetreiber auf seiner Datenschutzerklärung einbindet. In beiden Varianten kann sich der Besucher per Button einen Cookie setzen, der bei zukünftigen Counteraufrufen übertragen wird und auf den Servern der Anbieter die Speicherung unterbindet. Löscht der Nutzer seine Cookies oder surft er in einer privaten Browsersession, wird beim nächsten Besuch wieder gezählt.

Bei der parallelen Verwendung mehrerer Trackingtools auf einer Webseite gibt es bislang keine einfache standardisierte Möglichkeit, allen Trackings insgesamt zu widersprechen. Die neuen Versionen des Internet Explorers und des Firefox bieten die Möglichkeit, per Einstellung einem Tracking[2] zu widersprechen. Ist diese Einstellung gesetzt, sendet der Browser bei jeder Anfrage an eine Webseite eine Information über den gesetzten Widerspruch mit.

Es obliegt allerdings der jeweiligen Webseite bzw. dem Trackingtool, diese Einstellung zu berücksichtigen und die Erfassung zu unterlassen. Solange die Browseroption kein Standard und rechtlich verbindlich ist, kann sie eine explizite Widerspruchsmöglichkeit nicht ersetzen. Mittelfristig werden Webanalyse-Anbieter diese Features sicherlich berücksichtigen. Der Hinweis – auf welche Widerspruchsmöglichkeit auch immer – ist Pflicht.

5. Anonymisierung durch IP-Masking

Die Einholung einer Vorabeinwilligung der betroffenen Nutzer dürfte in vielen Fällen jedoch unpraktisch und kaum realisierbar sein. Die Nutzung von Webanalyse-Diensten wie Google Analytics ist **ohne datenschutzrechtliche Einwilligung** des Betroffenen für die Erhebung von Nutzerdaten dann allerdings nur möglich, soweit keine personenbezogenen Daten beim Tracking erhoben werden. Am einfachsten gelänge dies, würde die IP-Adresse von vornherein nicht mit erhoben werden. Dann ließen sich alle verbleibenden Daten ohne Bedenken auch ohne Einwilligung des Betroffenen nutzen.

[2] http://dnt.mozilla.org/

Wird die IP-Adresse – wie bei Google Analytics – allerdings doch mit erhoben, und hat man – wie in diesem Fall – keine Möglichkeit dies selbst abzustellen, kommt eine Nutzung nur in Frage, soweit die **IP-Adresse** bereits bei der Erhebung unkenntlich gemacht, d.h. **anonymisiert,** wird. Dazu muss sie vor dem Speichern derart verändert werden, dass eine Zuordnung zu einer Person – über den Anschluss und Provider – nicht mehr möglich ist.

Google hat für diese Kürzung die Funktion „anonymizeIp"[3] eingeführt, die in den Trackingcode eingebaut werden muss. Bei jedem Aufruf des Trackingcodes muss diese Funktion übergeben werden. Andere Anbieter nehmen die Kürzung automatisch vor oder bieten eine Option im Webanalyse-Programm.

Konkret bedeutet dies die Kürzung der IP-Adresse um die letzte Stelle, also 8 von 32 Bit. Die meisten Webanalyse-Tools wie Google Analytics benutzen die IP-Adresse inzwischen nur noch für die **Geo-Lokalisierung** der Besucher. Die Berechnung von Visits und Erkennung von wiederkehrenden Besuchern geschieht mit Cookies. Somit ergibt sich durch die Kürzung kein Nachteil bei den generellen Kennzahlen. Aus welchem Bundesland oder welcher Stadt der Besucher kommt, wird gleichzeitig ungenauer. Allerdings sind diese Positionsdaten selten verlässlich und die meisten Webseitenbetreiber haben keinen wirklichen Nutzen aus dieser Detailtiefe. Aus welchem Land der Besucher kommt, können die Tools weiterhin erkennen.

Die „anonymizeIp"-Funktion liefert dem Tool die Information, die Adresse vor der weiteren Verwendung zu kürzen. Die eigentliche Kürzung der IP-Adresse erfolgt immer erst auf den Servern des Anbieters, weil die IP als grundlegender Bestandteil bei jeder Datenübertragung im Internet erforderlich ist.

Auf einer Webseite lässt sich daher nicht überprüfen, ob die IP am anderen Ende wirklich gekürzt wird, was einige Kritiker gegen diese Lösung von Google anführen. In den Verhandlungen mit dem Hamburger Datenschutzbeauftragen hat Google zugesichert, die Kürzung der IP-Adressen auf Servern innerhalb Europas vorzunehmen. Damit können diese im Anschluss auch im Ausland (z.B. USA) weiterverarbeitet werden.

In Deutschland wird die Anonymisierung der IP von den Datenschützern zwingend erwartet, also der Einbau des zusätzlichen JavaScript Codes. Die Option lässt sich nicht in den Reportoptionen per Mausklick konfigurieren, sondern muss dem JavaScript Code explizit hinzugefügt werden. Soweit Sie dies

[3] http://code.google.com/intl/deDE/apis/analytics/docs/gaJS/gaJSApi_gat.html

noch nicht umgesetzt haben, sollten Sie handeln, um den Einsatz Ihres Analysetools ohne Einwilligung des Betroffenen datenschutzrechtskonform zu gestalten.

6. Vertrag über Auftragsdatenverarbeitung

Wegen der teilweise erst nach Erhebung der IP-Adresse vorgenommenen Anonymisierung ist das IP-Masking allein nach Meinung von Datenschützern unzureichend, um die Nutzung von Tracking-Diensten wie Google Analytics datenschutzrechtskonform zu ermöglichen. Es soll zusätzlich ein schriftlicher Auftragsvertrag zwischen Webseitenbetreiber und Analyseanbieter geschlossen werden.

Im September 2011 hat Google in Abstimmung mit dem Hamburger Datenschutzbeauftragen einen solchen Vertrag[4] vorgelegt, den der Webseitenbetreiber z.B. mit Google abschließen muss. Darin sind die notwendigen rechtlichen Grundlagen, Pflichten und Vorgänge zur datenschutzkonformen Nutzung des Analysedienstes festgelegt. Der Vertrag wird vom Webseitenbetreiber ausgedruckt und unterschrieben an Google Deutschland in Hamburg geschickt, von dort erhält er ein unterschriebenes Exemplar zurück.

Nach Meinung der Datenschützer handelt es sich bei der Weiterverarbeitung der auf der Webseite erhobenen IP-Adresse durch Google um eine Auftragsdatenverarbeitung gemäß § 11 BDSG, da der Webseitenbetreiber die Daten (inkl. Maskierter IP-Adresse) an Google zum Zwecke der Auswertung überträgt.

Die Rechtsansicht ist nicht unumstritten. Dagegen ließe sich anführen, dass bei einer Anonymisierung der IP-Adresse das Datenschutzrecht nicht mehr anwendbar ist. Demgemäß kann eine Auftragsverarbeitung von personenbezogenen Daten, welche ohne zur Vertragserfüllung nur mit ausdrücklicher Einwilligung des Betroffenen erhoben werden dürfen, nicht mehr vorliegen. Zudem dürfte in einer Übertragung auf die Google-Server in die USA – und damit außerhalb der EU – dann wohl trotzdem eine einwilligungspflichtige Übertragung im Sinne des § 3 Abs. 8 S. 3 BDSG vorliegen. Trotz dieser Bedenken erscheint es derzeit jedoch grundsätzlich empfehlenswert, das von den Datenschützern für erforderlich gehaltene Procedere einzuhalten. Zusätzlich zum Abschluss des Vertrages wird weiterhin gefordert, dass die Betroffenen vom Webseitenbetreiber über die Erhebung

[4] http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.de/de/de/intl/de/analytics/tos.pdf

von Daten durch Google Analytics unterrichtet werden (**Hinweispflicht**) und von ihrem Recht auf Widerspruch mit Wirkung für die Zukunft hingewiesen werden (**Widerspruch**). Die oben dazu beschriebenen Anforderungen gelten also nach wie vor.

7. Altdaten löschen

Das Tracking der Besucherdaten auf ihrer Webseite gilt überdies erst dann als rechtlich zulässig, wenn alle beschriebenen Punkte erfüllt sind. Besucherdaten, die etwa vor der Einbindung von „anonymizeIp" gesammelt wurden, müssen daher gelöscht werden. Bei Google Analytics bedeutet dies konkret, ein neues Profil für die Zählung einzurichten und das Alt-Konto zu löschen.

8. Pseudonymisierte Nutzungsprofile

Für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung von Telemedien ist die Verarbeitung der übrigen Nutzungsdaten darüber hinaus nur dann ohne Einwilligung des Betroffenen gestattet, soweit für jedes Nutzungsprofil ein eigenes Pseudonym angelegt ist, welches nur der verarbeitenden Stelle einen Rückschluss auf den Betroffenen erlaubt.

Das TMG enthält die entsprechende gesetzliche Erlaubnis in § 15 Abs. 3. Nutzungsdaten auf einer Webseite dürfen also grundsätzlich erfasst werden. Dies betrifft zum Beispiel die Information, was sich Besucher A und was sich Besucher B angeschaut haben. Diese Nutzungsdaten müssen für die Weiterverarbeitung jedoch mit Pseudonymen (z.B. eindeutige, nicht nachvollziehbare IDs) versehen werden und dürfen später nicht mit personenbezogenen Daten des Betroffenen zusammengeführt werden, etwa der IP-Adresse oder den Adressdaten aus einem Shop.

Konkret bedeutet dies, dass in einem Shop durchaus getrackt darf, was sich ein Besucher anschaut und auch was er kauft. Wenn man nun durch die Bestellung weiß, dass dieser Besucher in der realen Welt Herr Müller aus Frankfurt ist, darf man zunächst nicht auswerten, was Herr Müller sonst noch so im Shop angeschaut hat. Für eine solche Verbindung wäre die Einwilligung des Besuchers erforderlich.

Wenn ein Besucher auf der Webseite seine E-Mail-Adresse für einen Newsletter angibt, benötigt man keine Einwilligung, die Adresse zu speichern.

Zum Schutz vor unerwünschten Einträgen oder Verwechslungen sollte die Adresse jedoch durch ein Double-Opt-in-Verfahren verifiziert werden. Hier wird ein Newsletter erst versandt, nachdem der Besteller einen entsprechenden Link in der Bestätigungsmail angeklickt hat. Damit ist die angegebene E-Mail-Adresse jedenfalls halbwegs sicher verifiziert. Dieses Verfahren bietet einen geeigneten Nachweisschutz im Falle von Abmahnungen wegen angeblich unerwünscht zugesandten Mailings (Spam) und wird auch von den Gerichten als ausreichend anerkannt.

Im Trackingtool kann problemlos der Umstand erfasst werden, dass sich ein bestimmter Besucher im Newsletter angemeldet hat. Wenn aber die überlassene E-Mail-Adresse mit seinen übrigen Nutzungsdaten kombiniert werden soll (Zweckänderung), erfordert das eine Einwilligung.

Als Faustregel gilt also, dass personenbezogene Daten wie Name und Anschrift (auch die E-Mail-Adresse, soweit sie entsprechende Informationen enthält) ohne Einwilligung zwar beispielsweise zum Zwecke der Vertragserfüllung (gesetzliche Erlaubnis) nicht aber in einem Webanalyse-System erhoben werden dürfen.

Soweit die erhobenen Daten für andere Zwecke verwendet werden sollen, muss stets die Einwilligung des Besuchers vorab eingeholt werden.

Beim Einsatz eines Webanalyse-Tools, welches auch die IP-Adresse (auch in anonymisierter Form) erhebt, muss derzeit zwar noch keine Vorabeinwilligung eingeholt, jedoch müssen trotzdem alle genannten datenschutzrechtlichen Vorgaben eingehalten werden.

9. Webanalyse-Checkliste

1. Haben Sie auf Ihrer Webseite eine Datenschutzerklärung eingebunden, in welcher der Nutzer über Art und Umfang der Erhebung seiner Daten aufgeklärt wird?

2. Ist sichergestellt, dass die Datenschutzerklärung jederzeit abrufbar ist?

3. Wird in dieser Erklärung auf die Verwendung von Webanalyse-Diensten (z.B. Google Analytics) hingewiesen?

4. Wird auf die Widerspruchsmöglichkeit (Plug-in) hingewiesen?

5. Haben Sie einen schriftlichen Vertrag zur Auftragsdatenverarbeitung mit dem Webanalyse-Dienst abgeschlossen?

6. Beinhaltet der Vertrag alle wesentlichen Regelungen im Sinne des § 11 Abs. 2 BDGS?

7. Ist bei der Verwendung von Google Analytics der Trackingcode um die Funktion „anonymizeIp" ergänzt?

8. Haben Sie personenbezogene Daten, die vor der Umsetzung dieser Anforderungen erhoben wurden, gelöscht?

9. Haben Sie sichergestellt, dass bei der Verwendung von pseudonymen Nutzungsdaten keine Zusammenführung mit eventuell vorhandenen personenbezogenen Daten erfolgen kann (Trennung)?

10. Haben Sie, für den Fall der erforderlichen Einholung einer Einwilligung sichergestellt, dass diese protokolliert wird und für den Nutzer jederzeit abrufbar ist?

10. Zusammenfassung

Die wichtigsten Anforderungen der Datenschützer lassen sich mit nahezu jedem Webanalyse-Tool umsetzen. Je nach Webanalyse-System erfordert die Umsetzung allerdings Anpassungen von Trackingcodes oder Tool-Konfiguration.

Mit der Umsetzung dieser Anforderungen ist laut dem Datenschutzbeauftragten Hamburg (stellvertretend für alle deutschen Datenschutzbeauftragten) der beanstandungsfreie Betrieb[5] von Google Analytics möglich.

Die Autoren

Christian Vollmert, Leiter der Unit Search im Bundesverband Digitale Wirtschaft (BVDW) e.V., Gründer und Geschäftsführer der Agentur luna-park GmbH, Köln

Markus Vollmert, Prokurist und Gesellschafter der Agentur luna-park GmbH, Köln (www.luna-park.de), die Kunden im Bereich Webanalyse und speziell Google Analytics berät.

RA Michael Neuber, Justiziar im Bundesverband Digitale Wirtschaft (BVDW) e.V.

[5] http://www.datenschutz-hamburg.de/news/detail/article/beanstandungsfreier-betrieb-von-google-analytics-ab-sofort-moeglich.html