DR.-ING. KLAUS MEFFERT
IT LOGIC GMBH®

DIE HÄUFIGSTEN DATENSCHUTZFEHLER AUF WEBSEITEN

DIE DATENSCHUTZGRUNDVERORDNUNG IN DER PRAXIS

INHALTSVERZEICHNIS

Einleitung

Wir haben über 30000 Webseiten darauf hin geprüft, ob sie Verstöße gegen das Telemediengesetz (TMG) oder das Datenschutzgesetz (DSGVO bzw. zuvor auch BDSG) enthalten. Von diesen Webseiten wurden **über 200 intensiver analysiert**. Das Ergebnis daraus ist in dieser Studie dargestellt.

Alle Arten von Webseiten:
Die analysierten Webseiten wurden willkürlich ausgewählt.

Es handelt sich um Webseiten aus allen möglichen Branchen und von Unternehmen jeder Größe.

Geprüft wurden nur Webseiten, die Inhalte in deutscher Sprache anbieten und die offensichtlich für den deutschen Markt bestimmt sein.

Fast immer handelt es sich bei den Betreibern der Webseiten um in Deutschland ansässige Unternehmen, Gewerbebetriebe oder Organisationen.

Am häufigsten wurden Webseiten von deutschen Unternehmen mit mehr als zehn Mitarbeitern geprüft, gefolgt von solchen mit weniger Mitarbeitern.

Relativ selten waren Organisationen oder Seiten von Privatpersonen Teil der Prüfung.

Vorschau der Ergebnisse

In einer kompakten Übersicht sind die wichtigsten Erkenntnisse der Studie zusammengefasst:

Eine Webseite besteht im Durchschnitt aus weit über 100 Seiten

WordPress und Google Analytics werden sehr oft verwendet

Von allen geprüften Webseiten enthielten über 95% gravierende Datenschutzfehler

Häufigstes Problem sind unvollständige Datenschutzerklärungen

Oft wurden populäre Tools rechtswidrig eingebunden, u.a. YouTube-Videos, Social Media Plugins und Analyseprodukte

Sie finden detaillierte Ausführungen in den folgenden Abschnitten.

Prüfung

Die Prüfung wurde durchgeführt von der IT Logic GmbH, deren Haupttätigkeitsfeld die **IT-Beratung und Software-Entwicklung** ist.

Autor für die IT Logic GmbH ist deren Geschäftsführer, **Dr. Klaus Meffert** (Diplom-Informatiker).

Juristische Expertise wurde von der Anwaltskanzlei Roland Rodenberg eingeholt, die auf IT-Recht spezialisiert ist.

Die Prüfung wurde manuell durchgeführt und unterstützt von einer eigens entwickelten Software, die alle Seiten einer Internetpräsenz durchläuft, sowie Auffälligkeiten automatisch identifizieren und vorklassifizieren kann. Nur mit Hilfe dieser Software war eine wirtschaftliche, sichere und repräsentative Prüfung überhaupt möglich.

Grundlage der Prüfung

Rechtliche Grundlage ist das deutsche Recht, das für alle Webseiten gilt, die für den deutschen Markt bestimmt sind.

Die Datenschutzrichtlinie der Europäischen Union (DSGVO) gilt für alle Mitgliedsstaaten der EU und somit auch für Deutschland.

Ebenso gilt die DSGVO für alle Unternehmen, die sich an den Europäischen Markt wenden (Marktortprinzip).

Urteile aus den vergangenen drei Jahren wurden berücksichtigt, so u.a. die Entscheidung des Bundesgerichtshofs (BGH), **dass selbst dynamische IP-Adressen als personenbezogene Daten gelten**, aber auch Entscheidungen von deutschen Gerichten zu Google Analytics und zur wettbewerblichen Betrachtung von Datenschutzverstößen.

Seit 2019 können **selbst Privatpersonen** eine Unterlassungserklärung von Webseitenbetreibern fordern, die Produkte wie Google Analytics ohne IP-Adressenanonymisierung einsetzen.

Die **Einbindung von Ressourcen von Drittservern** ist ohne entsprechende Datenschutzerklärung bzw. Nutzereinwilligung nicht zulässig oder zumindest rechtlich kritisch zu bewerten, da dabei zwangsläufig die IP-Adresse des Nutzers zum Dritten übertragen wird.

Solche Ressourcen sind etwa **Schriftarten, Scripte oder Bilder**. Wir haben diese Art von Fällen allerdings nicht weiter untersucht, weil die Rechtslage hier noch nicht vollständig gefestigt ist.

Prüfzeitraum

Die Prüfung fand zwischen dem dritten Quartal 2017 und dem dritten Quartal 2019 statt.

Geprüfte Sachverhalte

Unsere Prüfung konzentrierte sich auf folgende Sachverhalte:

- Erreichbarkeit der Datenschutzerklärung
- Existenz allgemeiner Klauseln in der Datenschutzerklärung
- Datenschutzkonforme Verwendung von Analyseprodukten
- Datenschutzkonforme Verwendung von Social Media Komponenten
- Datenschutzkonforme Verwendung von Mediendateien wie Videos
- Vorliegen von Datenschutzerklärungen zu verwendeten Komponenten
- Ausreichende Verbraucherinformation zum Datenschutz außerhalb der Datenschutzerklärung
- Erreichbarkeit des Impressums
- Pflichtangaben im Impressum

Die Prüfungen zum Impressum sind deshalb aufgenommen, weil das Impressum wichtiger Bestandteil der Webseite ist und oft in einem Atemzug mit dem Stichwort Datenschutz genannt wird. Das Impressum ist, soviel sei der Ordnung halber erwähnt, kein datenschutzrechtlich relevanter Bestandteil einer Webseite, sondern dem Telemediengesetz (TMG) untergeordnet.

Die Prüfungsergebnisse wurden im Zweifel zugunsten der geprüften Webseite festgelegt. War die Datenschutzerklärung (nur) über das Impressum erreichbar, wurde dies nicht als Verstoß gewertet, obwohl es nach aktueller Auffassung nicht zulässig ist.

Abgrenzung

Nicht geprüft wurden mit Newslettern spezifisch zusammenhängende Sachverhalte, wie etwa das Vorhandensein des Double Opt-in Verfahrens oder ein vorhandenes Impressum in Newslettern. Bei Newslettern wurde lediglich geprüft, ob die notwendigen Angaben dort vorhanden waren, wo der Newsletter bestellt werden konnte.

Kleinere Verstöße, wie eine vorhandene, aber unvollständige Erklärung zu einem Analyseprodukt, wurden nicht aufgenommen. Wir haben davon abgesehen, spezielle Seiten wie Login-Seiten oder RSS-Feed-Seiten, in die Betrachtung aufzunehmen.
Nach unserer Auffassung, die einer strengen Auslegung der Datenschutzvorschriften folgt, gehören diese Seiten mit einem Link auf Datenschutzhinweise und auf das Impressum versehen.

Eine strenge Auslegung ist unserer Auffassung und der Verfolgung der Rechtsprechung nach zwar angebracht, würde die Statistik aber einseitig verfälschen, weil derartige Probleme noch nicht als solche in die Rechtsprechung eingegangen sind. Abgesehen davon, hat der Anbieter von WordPress sich entschieden, die Datenschutzerklärung sogar automatisch auf Login-Seiten zu integrieren, wenn der Webseitenbetreiber sein System richtig konfiguriert hat.

E-Commerce Funktionen, wie sie charakteristisch für Online Shops sind, waren nicht Gegenstand unserer Untersuchung. Urheberrechtsverletzungen wurden nicht geprüft, u.a. auch, weil dies über einen Black Box Test gar nicht oder nur mit sehr hohem Aufwand möglich ist. Verlinkte externe Inhalte wurden nicht geprüft.

Ergebnis der Analyse

Von den zahlreichen generell geprüften Webseiten (einige im Auftrag von Kunden, einige zum Test unserer Datenschutz-Software) wurden 207 Webseiten detaillierter analysiert. Die weniger intensive Beurteilung der restlichen Webseiten bestätigt das Ergebnis der detaillierten Analyse der Teilmenge.

Die folgende Statistik stellt konsolidiert die häufigsten der gefundenen Verstöße dar.
Die Namen der Webseiten und der Betreiber werden zum Schutz der Betroffenen nicht genannt.

Für alle Angaben übernehmen wir trotz sorgfältiger Prüfung keine Gewähr.

Häufigste gefundene Verstöße

Im Rahmen dieser Studie wurden mehrere Verstöße geprüft, die nachfolgend ausgelistet sind. Pro Webseite sind mehrere Verstöße möglich. Die Prozentzahl gibt an, auf wie vielen der untersuchten Websites der jeweilige Verstoß vorhanden war.

- Datenschutzerklärung allgemein unvollständig: 91%
- Datenschutzerklärung fehlt für Einzelkomponente: 60,9%
- Rechtswidriges Kontaktformular: 50,4%
- Rechtswidrige Einbindung von YouTube Videos: 37,6%
- Unberechtigter Einsatz von Social Media Widgets: 19,2%
- Fehlendes Cookie-Popup: 12,4%
- Impressum oder Datenschutzerklärung nicht erreichbar: 10,7%
- Impressum unvollständig: 4,2%
- Google Analytics ohne IP-Adressenanonymisierung: 27,7%

Die Prozentzahl für den zuletzt genannten Verstoß bezieht sich nur auf Seiten, die Google Analytics einsetzten. Diese Zahl ging seit Mitte 2018 zurück, war aber bis vor Inkrafttreten der Datenschutzrichtlinie der EU (DSGVO) dafür deutlich höher.

Anzahl problematischer Websites

Von allen geprüften Webseiten enthielten über 95% gravierende Datenschutzfehler, die nach unserer Einschätzung eine Sanktion (Bußgeld, Abmahnung, Unterlassungserklärung) rechtfertigen würden.

Selbst Webseiten von Unternehmen, die Security-Produkte oder Dienstleistungen mit Bezug auf Datensicherheit anbieten, waren oft voll von Unzulänglichkeiten.

Webseiten von Banken waren überdurchschnittlich oft ohne gravierende Mängel. Dies liegt sicher auch mit daran, weil Banken sparsam mit Dritt-Technologien auf ihren Webseiten umgehen und weil die Banken eines Verbundes oft dasselbe Webseitensystem verwenden.

Problembewusstsein

Vielen Unternehmen ist nicht bewusst, dass sie eine hochgradig rechtswidrige Webseite verantworten, die zahlreiche Datenschutzfehler enthält.
Eine Befragung einiger dieser Unternehmen zeigte folgende insbesondere Ursachen für diesen Missstand:

- Die Online Agentur/der Webmaster des Unternehmens wird als kompetent angesehen, ungeachtet der Tatsache, dass diese es offensichtlich nicht war/ist
- Ein Anwalt, der eine Webseite in Rechtsfragen betreut, wird als kompetent angesehen - oder er hat ein Problem damit, indirekt zuzugeben, dass er der Komplexität der Materie nicht vollständig gewachsen ist
- Man bemüht sich schon so sehr darum, alles korrekt zu machen, irgendwann muss mal Schluss sein
- Für die Behebung von rechtlichen Problemen auf der Webseite wird kein Budget bereitgestellt

Weitere Statistiken

Die Angaben sind gerundet, bei Prozentwerten können in Summe so andere Werte als 100% entstehen.

Umfang der Webseiten

Der Umfang einer Webseite ergibt sich hier aus der Anzahl der Seiten (Pages). Eine Seite ist etwa die Startseite, das Impressum oder die Seite mit der Datenschutzerklärung. Eine Webseite mit genau einer Seite ist ein sog. One-Pager.

Aus Gründen der Effizienz wurden max. 1000 Seiten pro Webseite untersucht. Es ist nicht auszuschließen, dass wegen dieser Limitierung eine im Einzelfall unvollständige Erfassung verwendeter Komponenten vorliegt.

Durchschnittlich enthielt eine Website ca. 300 Seiten.

Der Umfang der untersuchten Webseiten in Seiten samt Anzahl der Webseiten pro Größenkategorie:

- 700 und mehr Seiten: 10,2%
- 400 bis 699 Seiten: 22,0%
- 200 bis 399 Seiten: 19,1%
- 100 bis 199 Seiten: 13,0%
- 50 bis 99 Seiten: 15,4%
- 20 bis 49 Seiten: 11,3%
- 2 bis 19 Seiten: 7,4%
- One-Pager: 1,7%

Verwendete Analyse-Tools

Die analysierten Webseiten verwendeten folgende Analytics Bibliotheken in der angegebenen Häufigkeit (Angaben gerundet, Mehrfachnennung pro Website möglich):

- Google Analytics: 62,8%
- Matomo (Piwik): 12,8%
- INFOnline: 8,7%
- Optimizely: 4,7%
- WordPress Status: 4,6%
- eTracker (kostenpflichtig): 3,5%
- NewRelic: 2,3%
- Kein Tracker: 14,5%

Wenn Google Analytics durch den Google Tag Manager nachgeladen wurde, konnten wir dies erkennen und in die Statistik aufnehmen.

Weitere verwendete Tools dieser Art sind vorhanden, aber nicht aufgeführt, weil deren Nutzungsgrad entsprechend gering ist oder eine automatische Erkennung nicht durchgeführt wurde. Vollständig lokal laufende Lösungen wie eigene Analyse-Tools, konnten nicht aufgeführt werden, weil sie an sich nicht erkennbar sind.

Webseiten-Systeme

Hierzu zählen Content Management Systeme (CMS), aber auch Homepage-Baukästen oder reines HTML. Die von den analysierten Seiten verwendeten Systeme sind:

- WordPress: 24,7%
- Typo3: 21,3%
- Jimdo: 3,1%
- HTML/Unbekannt, mit Cookies: 8,6%
- HTML/Unbekannt, ohne Cookies: 2,9%
- (Noch) Nicht ermittelt: 31,9%

Das populärste CMS, WordPress, wurde auch in unserer Statistik als Nummer eins bestätigt.

Fazit

Wie unsere umfangreiche Untersuchung zeigt, gibt es so gut wie keine Webseite in Deutschland bzw. für den deutschen Markt, die konform mit den einschlägigen Datenschutzbestimmungen ist.
Der **Hauptgrund** ist nach unserer Beobachtung die Tatsache, dass IP-Adressen als personenbezogene Daten gelten. Dies ist vielen zum jetzigen Zeitpunkt immer noch nicht bewusst. Selbst Anwälte wissen darüber oft nicht bescheid. Diese Unwissenheit lässt sich auch anhand des folgenden Satzes nachweisen, der in zahlreichen Datenschutzerklärungen zu finden ist: *Sie können diese Webseite in der Regel besuchen, ohne uns personenbezogene Daten zu hinterlassen.*

Viele Verantwortliche meinen, ihr Webmaster, die Webagentur oder ein für die Rechtstexte auf der Webseite zuständiger Anwalt hätte ausreichend Kompetenz. Dies ist eindeutig nicht der Fall.
Auch **Datenschutzbeauftragte**, die durch die DSGVO einen Boom erleben, haben im Allgemeinen nicht die nötige Kompetenz, um Webseiten Datenschutzrechtlich abzusichern.

Seit 2016, dem Jahr mit einigen richtungsweisenden Entscheidungen zum Datenschutz, reicht es bei weitem nicht mehr aus, den sogenannten Disclaimer im Impressum anzugeben. Man muss mittlerweile für jede Webseite, egal wie wenig Inhalt sie enthält, eine recht umfangreiche Datenschutzerklärung bereitstellen.

Die Konfiguration von Komponenten wie Google Analytics oder YouTube Videos vergrößert das Problem. Hier prallen zwei Welten aufeinander: **Technik und Rechtswissenschaft**.

Es reicht nicht aus, nur Rechtstexte einzubauen und davon auszugehen, dass diese automatisch eingehalten werden.

Dementsprechend sind Textgeneratoren nicht geeignet, eine rechtlich halbwegs einwandfreie Datenschutzerklärung zu erhalten.
Die Bestandsaufnahme von auf einer Webseite verwendeten Komponenten ist mühsam bis unmöglich. Zumindest, wenn diese manuell vorgenommen wird.

Ohne eine solche Inventarisierung ist aber eine korrekte Datenschutzerklärung nicht möglich.

Wegen der DSGVO und ihren weitreichenden Konsequenzen kann nur empfohlen werden, vom Datentransfer hin zu Unternehmen, die nicht Mitglied der EU sind, nach Möglichkeit Abstand zu nehmen.

Nicht umsonst wurde der Einsatz des **Facebook Like Buttons** in seiner von Facebook angebotenen Form in Deutschland gänzlich untersagt.

Dementsprechend empfehlen wir, Google Analytics – das bis dato populärste Analyseprodukt – gar nicht mehr einzusetzen, sondern lokal auf dem eigenen Server laufende Alternativen wie Matomo (Piwik) zu setzen. Dann spart man sich auch die Mühe, eine komplexe Auftragsdatenverarbeitung mit der Firma Google (Sitz Irland) per Briefpost abzuschließen, ganz zu schweigen von dem Wegfall des Opt-Out Cookies samt zugehörigem JavaScript-Code.

Schlussbemerkungen

Datenschutz auf Webseiten ist ein hochkomplexes Thema. Eine Absicherung gegen rechtliche Risiken macht nicht nur Sinn, sondern ist auch rein logisch eingängig.
Das Risiko, mit einem Bußgeld belegt zu werden oder eine Abmahnung zu erhalten, ist recht gering, steigt aber. Datenschutzbehörden haben die Schonfrist für beendet erklärt.

Weiterhin darf mittlerweile jeder, also nicht nur Konkurrenten, sondern auch Privatpersonen, gegen Webseitenbetreiber vorgehen, die Nutzerdaten veruntreuen. Diese Veruntreung findet meist unbewusst statt, ist aber schnell vorhanden. Es reicht bereits der falsche Einsatz eines Tools oder die Verwendung eines verbotenen Social Media Plugins oder ein YouTube-Video, welches ohne erweiterte Datenschutzeinstellungen eingebunden wurde.

Verantwortlich für dieses Dokument

IT Logic GmbH
Ihr Partner für IT & Datenschutz
An der Struth 25
65510 Idstein
Deutschland

Geschäftsführer: Dr.-Ing. Klaus Meffert
USt.-ID: DE301065898
Amtsgericht Wiesbaden, HRB 28310
Mail: kontakt@it-logic.de

Autor: Dr.-Ing. Klaus Meffert,
Adresse und Kontakt wie oben

Wir freuen uns über Ihre Rückmeldungen, gerne per Mail an
redaktion@it-logic.de

Besuchen Sie unsere XING-Gruppe, um Wissenswertes zum Datenschutz auf Internetseiten zu erfahren:
https://www.xing.com/communities/groups/datenschutz-auf-webseiten-b20f-1113643/