

5 häufige Fehler vermeiden

Die Firmenwebsite

**Mit den digitalen Möglichkeiten steigen
die administrativen Aufgaben.**



Inhaltsverzeichnis

Impressum	4
Vorwort	5
Fehler 1:	
Nicht vorhandene Datenschutzerklärung	6
Fehler 2:	
(Un)Sichere Datenübermittlung	8
Fehler 3:	
Vertragsgrundsätze im Datenschutzzumfeld	10
Fehler 4:	
Analytische Websiteauswertung - die fehlende IP-Anonymisierung	12
Fehler 5:	
Analytische Websiteauswertung - mangelhafte Widerspruchsmöglichkeit	14

Impressum:

Herausgeber:
Datenschutz | Einfach | Digital | Gestalten
eine Initiative der
Marc Weber Management GmbH

Autor:
Marc Weber

Bezugsquelle:
Marc Weber Management GmbH
Lackerbauerstraße 23
81241 München
www.dedg.de
dedg@marcweber.de
Telefon 089 66 62 86 0
Fax 089 66 62 86 25

Stand:
Januar 2018

Bildnachweis:
Marc Weber Management GmbH

Vorwort

Unsere Studie über Datenschutzaspekte auf der Firmenwebsite hat zahlreiche Schwachstellen und Lücken aufgedeckt. Dabei lässt sich ein Nachholbedarf unabhängig von der Betriebsgröße oder dem Sitz eines Betriebes erkennen. 5 der häufigsten Stolpersteine haben wir in diesem Dossier zusammengefasst.

Eingangs wird die beobachtete Problematik dargestellt und welche Auswirkungen folgen können. Im Anschluss wird skizziert, wie das Problem behoben werden kann. In der Regel können an dieser Stelle nur einheitlich allgemeine Tipps und Hilfestellungen gegeben werden. Datenschutz ist ein sehr individuelles Thema und abhängig von den realen Inhalten einer Website.

Ihr Marc Weber



1. Nicht vorhandene Datenschutzerklärung

Die Lage

Die eigene Firmenwebsite ist heute mehr denn je das digitale Schaufenster zur Kundengewinnung. Vielfach dient sie als erster und zentraler Anlaufpunkt für Interessenten, die sich über das Angebot und das Unternehmen informieren möchten. Der erste Eindruck ist dabei von entscheidender Bedeutung. Daher ist es wenig verwunderlich, dass Unternehmen viel Zeit, Engagement und ein bedeutendes Budget für die Realisierung einer gelungenen Internetpräsenz investieren. Dabei spielen ins Besondere das Design, der Inhalt (Content) und die Usability eine bedeutende Rolle. Neben diesen scheinbaren Kernelementen geraten die rechtlichen Aspekte vielfach in den Hintergrund.

Die Anbieterkennung (Impressum) ist wohl noch der weitverbreitetste Rechtliche Baustein, der aktuell umgesetzt wird. Bei Themen rund um den Datenschutz zeigen sich dagegen enorme Lücken. Unserer Branchenstudie nach, verfügen lediglich 56% der Seiten über eine Datenschutzerklärung (der Wert bezieht sich auf das Vorhandensein einer Informationsseite, ohne Wertung über Richtigkeit oder Vollständigkeit).

Dies hat zur Folge, dass 44% keine Hinweise oder Erklärungen bereitstellen. Eine fatale Situation, die teuer werden kann. Hinweise zum Datenschutz, etwa welche personenbezogenen Daten von welcher Stelle zu welchem Zweck erhoben und verarbeitet werden, sind durch das Bundesdatenschutzgesetz verpflichtend und können durch die zuständigen Aufsichtsbehörden geahndet werden. Auch kann das Ausbleiben einer wahrheitsgemäßen und vollständigen Datenschutzerklärung als unlauterer Wettbewerb gesehen werden.

Der Ansatz

Werden auf der eigenen Firmenwebsite personenbezogene Daten verarbeitet, muss eine Datenschutzerklärung bereitgestellt werden. Eine derartige Erklärung erfasst jeden einzelnen relevanten Aspekt der Website und ist für jede Internetpräsenz individuell zu erstellen. Allgemeine Mustervorlagen sind daher unpassend und können im Bedarfsfall lediglich die Basisinformationen abbilden. Im Internet verfügbare Generatoren können bei der individuellen Ausgestaltung einer passenden Datenschutzerklärung helfen. Professionelle Tools fragen Punkt für Punkt ab, welche Inhalte oder Applikationen vorhanden sind und erstellen auf dieser Grundlage einen zusammenhängenden Textbaustein, der auf der eigenen Website eingefügt werden kann. Idealerweise ist oder wird die Menüordnung um einen Punkt „Datenschutz“ oder „Datenschutzerklärung“ erweitert. Auch kann der Punkt „Impressum“ auf „Impressum / Datenschutz“ umbenannt werden. Eine vorhandene Datenschutzerklärung ist zudem regelmäßig auf Aktualität hin zu überprüfen. Insbesondere nach der Neuordnung durch die DS-GVO im Mai 2018.



2. (Un)Sichere Datenübermittlung

Die Lage

Neben zahlreichen technischen Feinessen dient die eigene Firmenwebsite auch im Wesentlichen der Kommunikation. Neben der Bereitstellung von Telefonnummern und der E-Mail-Adresse, ermöglichen es viele Websites den Besuchern direkt über ein Kontaktformular oder eine Chatapplikation in Verbindung zu treten. Neben einer allgemeinen Kommunikation, ist es bereits auch üblich, Verträge bereits online abzuschließen oder Waren zu bestellen. Auf diese Weise werden personenbezogene Daten erhoben und übermittelt. Die verantwortliche Stelle, also der Websitebetreiber, ist für eine sichere Übertragung verantwortlich. Aus technischer Sicht lässt sich eine sichere Übertragung nur mittels einer Verschlüsselung des Datenverkehrs erreichen. Die viel zitierten „SSL-Zertifikate“ oder der Nachfolger „TLS-Zertifikat“ sind daher als obligatorisch zu betrachten, wird mit personenbezogene Daten auf der Firmenwebsite umgegangen. Unsere Studie hat gezeigt, dass gerade bei der technischen Sicherheit ein markanter Nachholbedarf vorhanden ist.

Der Ansatz

In jedem Fall lohnt sich die Installation eines SSL- bzw. TLS-Zertifikates. Websitebetreiber, die nicht zur Sicherheit personenbezogener Daten ohnehin zur Einrichtung einer Verschlüsselung angehalten sind, können von der positiven Auswirkung auf Suchmaschinen profitieren, die im Regelfall verschlüsselten Seiten den Vorzug geben. Mit der zunehmenden Thematik rund um Datenschutz und IT-Sicherheit bieten nahezu alle Provider im administrativen Backend eine Möglichkeit, Zertifikate mit wenigen Klicks zu bestellen und einer Domain zuzuordnen. Die Auswahl kann kostenfreie und kostenpflichtige Zertifikate umfassen. Je höher der Schutzstandard, desto besser. Dabei ist empfehlenswert, auf Qualitätsprodukte von namhaften Unternehmen zu setzen. Im Bedarfsfall sollte eine spezialisierte Agentur hinzugezogen werden.

Tipp:

Verschlüsselte Websites sind in aller Regel durch ein https am Anfang der Domainadresse und einem grünen Schloss in der URL-Zeile zu erkennen.



3. Vertragsgrundsätze im Datenschutzumfeld (Auftragsdatenverarbeitung)

Die Lage

Mit Blick auf die digitale Kommunikation, gibt es eine Besonderheit im datenschutzrechtlichen Sinn zu berücksichtigen. Die verantwortliche Stelle, also der Websitebetreiber, ist stets für die personenbezogenen Daten und deren Sicherheit verantwortlich. Eine Weitergabe der personenbezogenen Daten, beispielsweise an externe Dienstleister, ist grundsätzlich nicht vorgesehen, kann jedoch unter bestimmten Voraussetzungen erfolgen. Eine Möglichkeit eröffnet das Bundesdatenschutzgesetz mit einer Auftragsdatenverarbeitung nach § 11 BDSG.

Das Hosting einer Seite fällt auf den ersten Blick nicht unter eine gezielte Weitergabe an personenbezogenen Daten, jedoch gilt dieser Grundsatz auch bei der theoretischen Möglichkeit, die Daten zu sichten. Fallen auf der eigenen Firmenwebsite nun personenbezogene Daten an, die über den Provider laufen oder sind E-Mail-Postfächer hinterlegt, so ist mit dem Hostler ein Vertrag zur Auftragsdatenverarbeitung zu schließen. Entsprechendes gilt auch für externe E-Mail-Provider oder Applikationsanbieter.

Der Ansatz

Fallen beim Hoster personenbezogene Daten von Kunden oder Interessenten der verantwortlichen Stelle an, sei es durch E-Mail-Postfächer oder durch die Datenstruktur der Unternehmenswebsite, ist mit diesem ein Vertrag zur Auftragsdatenverarbeitung schriftlich zu schließen. § 11 Bundesdatenschutzgesetz sieht unter Absatz 2 eine nicht abschließende Liste an Mindestinhalten an eine derartige Vereinbarung vor. Besonderes Augenmerk ist auf die technisch organisatorischen Maßnahmen zu werfen, die der Auftragnehmer detailliert zu verfassen hat. Im Hostingbereich ist es derzeit üblich, dass der Hoster bereits Musterverträge vorbereitet hat, die die wesentlichen Punkte beinhalten. Empfehlenswert ist es, diese Vertragswerke zu lesen und genau auf die Rechte und Pflichten des Auftraggebers sowie des Auftragnehmers zu achten. Wird eine Auftragsdatenverarbeitungsvereinbarung (ADV) benötigt und der Hoster hat kein Muster, weigert sich eine solche Vereinbarung zu unterzeichnen oder reagiert nicht auf diese Anfrage, bleibt nur der Wechsel zu einem anderen Unternehmen.

Tipp:

Das ADV-Management gehört bei manchen Aufsichtsbehörden zum Standardprüfkatalog und Mängel werden häufig mit Bußgeldern belegt.



4. Analytische Websiteauswertung - die fehlende IP-Anonymisierung

Die Lage

Die eigene Firmenwebsite ist ein mächtiges Marketingwerkzeug. Doch erst mit einer genauen Besucheranalyse lassen sich wertvolle Potentiale für Marketingmaßnahmen heben. Heutzutage ist die Besucheranalyse und Auswertung auch kein unlösbares Problem mehr. Zahlreiche Applikationen und verschiedene Software stehen am Markt kostenpflichtig oder auch kostenfrei bereit. Dabei stehen freie Lösungen den gebührenpflichtigen in Umfang und Funktion in nichts nach. Auch die Implementierung der benötigten Codeabschnitte auf der eigenen Website ist leicht umzusetzen. Doch gibt es bei all diesen Möglichkeiten auch Grenzen, die der Datenschutz zieht. Eine Voraussetzung ist die Anonymisierung der IP-Adresse der Websitebesucher. Stets umstritten, zählt die Anonymisierung zu einer Mindestvoraussetzung für einen konformen Betrieb einer Analysesoftware.

Der Ansatz

Ist eine Analysesoftware im Einsatz oder deren Einsatz geplant, ist die vorhandene Anonymisierungsmöglichkeit zu prüfen und ob diese bereits umgesetzt wurde. Je nach Anbieter existieren unterschiedliche Herangehensweisen, um eine aktive Anonymisierung zu erreichen. In aller Regel ist diese nicht voreingestellt und muss durch den Anwender selbst erst aktiviert werden. Bei manchen Lösungen reicht die Auswahl der Option im Backend, bei anderen Angeboten ist der Code um eine entsprechende Anweisung zu erweitern. Tipps und Hilfe stellen die Anbieter bereit.



5. Analytische Websiteauswertung - mangelhafte Widerspruchsmög- lichkeit

Die Lage

Ein weiterer Eckpfeiler zur konformen Nutzung von Analysesoftware ist die Gewährung einer Widerspruchsmöglichkeit des Besuchers in die Aufzeichnung seines Verhaltens. Die Auswertung unserer Studie hat gezeigt, dass dieser Ansatz bei Websites, die über eine vorhandene Analyse aufklären, in aller Regel vorhanden ist. Jedoch ergab die Studie auch, dass gerade im Hinblick auf einen häufig genutzten Anbieter, die vorhandenen Texte und funktionalen Möglichkeiten veraltet sind. Die Widerspruchsmöglichkeit ist jedem Besucher in gleicher Weise zu ermöglichen, unabhängig der eingesetzten Hard- und Software. Hierbei ergibt sich die Problematik, dass veraltete Widerspruchstexte und Techniken kaum oder gar nicht auf mobile Endgeräte ausgerichtet sind. Auf diese Art entsteht eine Benachteiligung einer spezifischen Benutzergruppe und eine datenschutzrechtliche Lücke für den Betreiber.

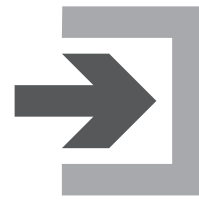
Der Ansatz

Diese Lücke lässt sich durch ein Update der entsprechenden Passage über die Analysesoftware beheben. Aktuelle Texte kann der Softwarehersteller bereitstellen oder lassen sich durch Datenschutzgeneratoren im Internet generieren. Bei der Implementierung ist auf etwaigen Code zu achten, der unter Umständen nicht bei allen Content Management Systemen akzeptiert wird. Weitere technische Einstellungen können die Folge sein. Bei auftretenden Problemen ist es empfehlenswert, eine spezialisierte Agentur hinzuzuziehen. In jedem Fall sollte die Widerspruchsmöglichkeit auf unterschiedlichen Endgeräten auch aktiv getestet werden.

Wichtiger Hinweis zur Nutzung:

Der vorliegende Ratgeber und dessen Inhalt wurden mit größtmöglicher Sorgfalt eruiert und verfasst und basiert auf der hauseigenen durchgeführten Studie „Studie - Datenschutz im Internet, Fahrschulen in Deutschland“. Dieses Werk spiegelt die Auffassung des Autors und den Stand der Untersuchungsobjekte zum Zeitpunkt der Veröffentlichung wider, erhebt jedoch keinen Anspruch auf Vollständigkeit und Richtigkeit. Der Herausgeber sowie der Autor schließen daher die Haftung für etwaige Schäden aus, die sich unmittelbar oder indirekt aus der Nutzung des Werkes und der darin verfassten Informationen ergeben können. Ausgenommen ist hierbei die Haftung für Vorsatz und grobe Fahrlässigkeit.

Der Ratgeber versteht sich als allgemeine Informationsquelle für einen ersten Überblick und eine erste Einschätzung des zugrundeliegenden Themas in Form einer unverbindlichen Anregung. Die Nutzerin / Der Nutzer ist hierbei nicht von einer sorgfältigen eigenverantwortlichen Prüfung entbunden. Vor einer Übernahme des unveränderten Inhalts (auch in Teilauszügen) ist von der Nutzerin / von dem Nutzer daher genau abzuwägen, ob und in welchen Abschnitten eine Anpassung an die konkrete Situation und Rechtsentwicklung erforderlich ist. Der Herausgeber ist nicht für die Nachnutzung der zugrundeliegenden Inhalte verantwortlich.



Datenschutz
Einfach
Digital
Gestalten

**Digital sein bedeutet
Datenschutz zu leben**