Whitepaper Datenschutz

Die DSGVO Website Checkliste – So sorgen Sie auf Ihrer Homepage für Datenschutz

Die Datenschutz-Grundverordnung verändert sich ständig. Gemäß der DSGVO liegt es dabei in der Verantwortung der Website Betreiber, sicherzustellen, dass diese erfüllt wird. Wir übernehmen keine rechtliche Haftung, aber legen einen sehr starken Wert darauf, dass Ihre Webseite DSGVO konform ist. Konkret bedeutet das, dass keine Daten ohne Zustimmung gespeichert oder an Dritte weitergegeben werden. Das gilt auch und vor allem für Tracking-Tools und Applikationen, die in Ihrer Internetseite eingebunden sind. Denn sobald Sie Features von Drittherstellern verwenden, werden oft auch Daten übertragen.

Mit dieser Checkliste sind die wichtigsten Punkte der DSGVO auf der Website abgedeckt:

1 Opt-in Einwilligung für die Website DSGVO Konformität

Früher genügte für die Zustimmung der Datenerfassung ein sogenanntes Opt-out, das den aktiven Widerspruch des Nutzers gegen das Tracking voraussetzte. So wurde der Besucher bereits beim Aufrufen der Seite getrackt und stimmte mit einem Klick auf „Okay“ zu.

Heutzutage wird für eine DSGVO konforme Website hingegen ein Opt-in benötigt. Das bedeutet, dass erst getrackt werden darf, wenn der Nutzer aktiv zustimmt. Da jede Einwilligung vom Besucher bewusst und eindeutig erfolgen muss, empfehlen wir Ihnen ein Opt-in mit einer nicht vor angekreuzten Checkbox.

2 Cookies auf Website einbinden

Bevor wir tiefer in das Thema Cookies eintauchen, möchten wir zunächst die Frage klären, ob und wann ein Cookie-Hinweis verpflichtend ist. Denn es ist ein Irrtum, dass ein Cookie-Banner bei jeder Webseite zwingend erforderlich ist. Er ist nur dann notwendig, wenn auf der Website Features und Elemente eingebunden sind, die den Benutzer bei dem Besuch der Seite tracken und dessen Daten speichern.

Muss ein Datenschutzhinweis integriert werden, gilt es zu beachten, dass die Zustimmung des Nutzers frei gegeben und nicht erzwungen wird.

Die Einwilligungen müssen hierbei detailliert sein. Dies bedeutet, dass Nutzer in der Lage sein müssen, einzelne Cookies zu aktivieren und zu deaktivieren. Sie dürfen nicht gezwungen werden, entweder allen oder keinem der Cookies zuzustimmen.

Hierbei wird grundsätzlich zwischen essentiellen und Marketing-Cookies unterschieden. Essentielle Cookies ermöglichen grundlegende technische Funktionen und sind für die einwandfreie Nutzung der Website erforderlich. Sogenannte Session-Cookies sind zum Beispiel dann erforderlich, damit sich ein Shop die Artikel im Warenkorb oder die Anmeldedaten bei einem Login merken kann. Cookies, die technisch erforderlich sind, bedürfen keiner Einwilligung. Anders sieht dies bei Marketing-Cookies aus, die beispielsweise mithilfe von Google Analytics das Verhalten der Besucher zu Marketing- und Targeting-Zwecken tracken.

Je nach Content-Management-System gibt es unterschiedliche Lösungen, mit denen konforme Datenschutzhinweise konfiguriert und erstellt werden können. Gerne beraten wir Sie zu einer passenden Lösung für Ihre Webseite.

„Der Betreiber einer Webseite hat sicherzustellen, dass keine Daten ohne Zustimmung gespeichert oder an Dritte weitergegeben werden."

3 Datenschutzerklärung Website

Jeder Seitenbetreiber ist dazu verpflichtet, dem Nutzer Informationen zum Datenschutz der Website bereitzustellen. Welche Inhalte in die Datenschutzerklärung gehören, ist individuell vom Umfang und dem Zweck der Datenerhebung abhängig. Grundsätzlich muss eine Datenschutzerklärung aber die gleichen Punkte enthalten wie der Cookie-Hinweis. Wir verwenden zur Erstellung von Datenschutzerklärungen den Generator eines Premiumanbieter für Rechtstexte, der es erlaubt eine Datenschutzbestimmung in mehreren Sprachen zu generieren.

4 Schriften lokal einbinden

Wurde auf einer Webseite Google Fonts standardmäßig eingebunden, werden über Google-Server mitunter personenbezogene Daten wie die IP-Adresse, benutzter Browser oder das verwendete Betriebssystem von Google gespeichert. Eine solche Einbindung der Schriftarten entspricht somit nicht den Richtlinien der Datenschutz-Grundverordnung. Da viele WordPress Themes aus den USA stammen und somit gerne Google Fonts verwenden und direkt einbinden, ist dies ein weitverbreiteter Fehler. Anstatt die Schriften direkt von Google zu laden, können diese auch lokal auf dem eigenen Server abgelegt und eingebunden werden.

5 Kontaktformular auf Website DSGVO sicher einbinden

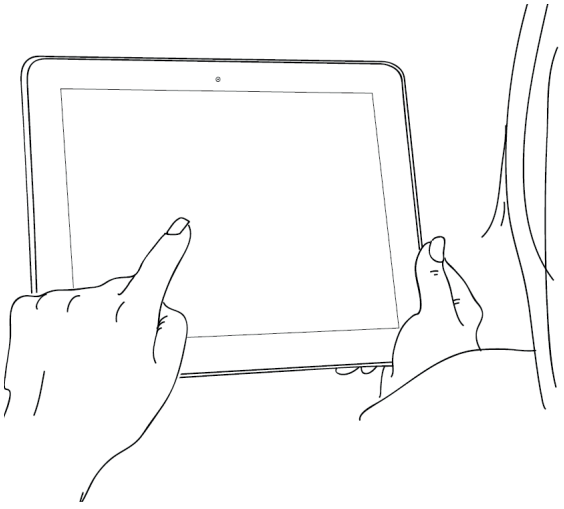
Kontaktformulare bieten Kunden und Interessenten die Möglichkeit einen direkten Kontakt zum Unternehmen aufzunehmen. Bei der Nutzung der Formulare werden in den meisten Fällen personenbezogene Daten aufgenommen. Bevor ein Formular abgeschickt werden kann, ist somit eine gesonderte und aktive Zustimmung der Datenschutzbestimmungen erforderlich. Diese wird durch das Anklicken einer nicht vorausgefüllten Checkbox mit einem entsprechenden Hinweistext und der Verlinkung auf die Datenschutzerklärung erreicht. Eine Erläuterung der Datenverarbeitung muss in der Datenschutzerklärung enthalten sein.

Wenn Sie auf Ihrer Website ein Formular benutzen, müssen Sie zudem sicherstellen, dass der Versand der Daten verschlüsselt wird. Dies wird allerdings oft übergangen und ist somit ein häufiger Fehler auf Webseiten. Wir empfehlen für Kontaktformulare eine Verschlüsselung mittels eines TLS-Protokolls. Gerne unterstützen wir Sie dabei.

Des Weiteren gilt es das Prinzip der Datensparsamkeit zu beachten: So dürfen von dem Nutzer nur Informationen als Pflichtangaben verlangt werden, die notwendig sind, um die Anfrage zu bearbeiten. Was am Ende tatsächlich als erforderlich gilt, hängt von der jeweiligen Situation ab. Für die Anmeldung bei einem Newsletter wird beispielsweise grundsätzlich nur die E-Mail-Adresse benötigt, nicht aber der Vor- und Nachname.

6 Newsletter für eine konforme DSGVO Internetseite

In Deutschland gilt bei Newslettern das Opt-in-Verfahren. Demnach muss ein Endverbraucher explizit und aktiv der Kontaktaufnahme per E-Mail ausdrücklich zustimmen. Um zu gewährleisten, dass auch wirklich der Verbraucher die Einwilligung erteilt hat und der erklärte Opt-in nicht von einem Dritten stammt, ist bei Newslettern das Double-Opt-in Verfahren anzuwenden. Bei diesem Verfahren erhält der Interessent nach Absenden der Newsletter-Anmeldung per Formular eine E-Mail, in der er bestätigen muss, dass der den Newsletter abonnieren möchte. Erst dann wird der Neukunde in die Empfängerliste aufgenommen und der Versand zulässig.



Ein weiterer wichtiger Punkt ist bei der Wahl des Newsletter-Tools zu beachten. Da das Privacy-Shield-Abkommen, also die Vereinbarung für den Datenaustausch zwischen Europa und den USA vom höchsten EU-Gericht gekippt worden ist, sollten keine internationalen Anbieter für den Newsletter verwendet werden. Für den Datenschutz auf Webseiten empfehlen wir die Wahl eines deutschen Anbieters.

„Wenn Sie Features von Drittherstellern auf Ihrer Webseite verwenden, werden oft auch Daten übertragen."

7 Integration von Social Media

Social-Media-Plugins ermöglichen die Integration praktischer Features, wie Teilen-Funktionen, Facebook-Kommentare oder die Einbindung von Instagram Feeds. Da soziale Netzwerke auch außerhalb ihrer eigenen Seiten Nutzerdaten sammeln, werden durch diese Funktionen Daten an Facebook und andere Social Media Anbieter gesendet. Gemäß der DSGVO ist die Nutzung solcher Website-Features nur dann gestattet, wenn der Nutzer der Datenübertragung vor der Verwendung aktiv zustimmt.

Eine gute Alternative zum Teilen von Website Inhalten bietet das Shariff-Plugin, welches keine Daten an Dritte weitergibt.

8 Google Maps auf der Webseite DSGVO konform einbinden

Durch den Kartenabruf beim Website-Besuch werden umfangreiche Datenmengen an den Anbieter des Kartendienstes übermittelt. Deshalb muss der Nutzer bereits vor dem Laden von Google Maps ausdrücklich darüber informiert werden, dass seine persönlichen Daten, wie beispielsweise seine IP-Adresse an Google weitergeleitet werden. In der Datenschutzerklärung der Webseite wird der User über die Übertragung der Daten zu den Portalen aufgeklärt. Eine Online-Karte kann somit erst nach Zustimmung vollständig angezeigt und verwendet werden.

„Vor allem bei Tracking-Tools und Applikationen, die auf der Internetseite eingebunden sind, gilt es auf die DSGVO-Konformität zu achten.“

9 Videoeinbindung ohne Cookies

Werden YouTube- oder Vimeo-Videos auf einer Seite im Standard-Modus eingebunden, werden bereits bei Aufruf einer Seite mit Video-Frame diverse Cookies gesetzt und Daten an den Anbieter der Plattform weitergegeben. Um dies zu umgehen, bietet YouTube selbst die Möglichkeit, Embed-Codes zu generieren, bei dem keine Cookies gesetzt werden. Alternativ können Videos auch lokal über den Server eingebunden werden.

Sobald ein YouTube- oder Vimeo-Video auf der Webseite eingebunden ist, ist es zwingend erforderlich, eine vorherige ausdrückliche Einwilligung des Nutzers einzuholen. Dies erfolgt üblicherweise über einen entsprechenden Cookie-Hinweis.

10 Website Datenschutz und -verschlüsselung durch SSL-Zertifikat

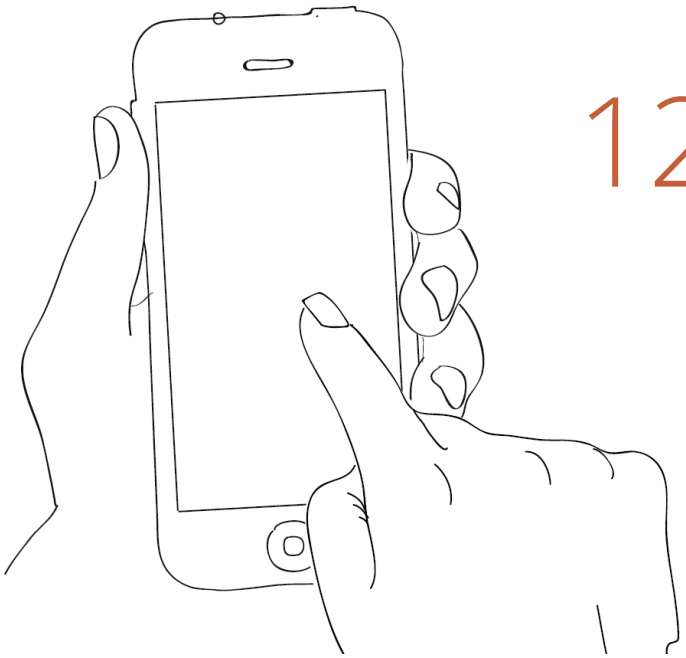
Eine SSL-Verschlüsselung ist nicht nur bei allen Seiten mit Kontaktformularen sowie Webshops rechtlich verpflichtend, sondern empfiehlt sich auch aus SEO-Sicht, da sie eine positive Auswirkung auf das Ranking bei Suchmaschinen hat. Die Datenverschlüsselung Ihrer Webseite ist bei uns standardmäßig dabei.

Mit der SSL-Technologie wird die Datenübertragung von einem Computer zu einem Server Ende-zu-Ende-verschlüsselt. Das Ziel ist zu verhindern, dass unbefugte Dritte Zugriff zu den übermittelten Daten erhalten. Ob eine Seite verschlüsselt ist, lässt sich daran erkennen, dass die Seite über https aufgerufen wird. In vielen Browsern werden verschlüsselte Seiten zusätzlich durch ein kleines Schloss neben der URL oder mit dem Wort „sicher“ gekennzeichnet.

Kann eine Seite auch unter http aufgerufen werden, ist es wichtig, an eine Weiterleitung zu denken und die Seite an https zu referenzieren.

11 Abschluss eines ADV-Vertrags

Einen Auftragsdatenverarbeitungsvertrag, kurz genannt ADV-Vertrag müssen gemäß der DSGVO alle Unternehmen abschließen, die personenbezogene Daten von einem Dienstleister verarbeiten lassen. Dies ist beispielsweise der Fall, wenn Sie über Google Analytics tracken oder einen externen Dienstleister für Ihren Newsletter verwenden. Bei Google Analytics kann der Abschlusses dieses Vertrages direkt online erfolgen.



12 WordPress Website DSGVO sicher machen

Über die Kommentarfunktion speichert WordPress die IP-Adresse des Benutzers. Um auf Ihrer Webseite das Speichern dieser personenbezogenen Daten zu verhindern, deaktivieren wir die Kommentarfunktion standardmäßig. Ein weiteres datenschutzrechtliches Problem stellt die Gravatar-Funktion in WordPress dar, die von einem Drittanbieter bereitgestellt wird. In der WordPress-Standardeinstellung wird bei Verwendung der Gravatar-Bilder die IP-Adresse des Nutzers ins Ausland gesendet. Mit dem Deaktivieren von Gravatar steigern Sie somit den Datenschutz Ihrer Webseite.

ANMUT

Disclaimer

Dieses Whitepaper stellt keine Rechtsberatung dar. Im Rahmen unserer Arbeit haben wir uns zwar intensiv mit den geltenden Datenschutzbestimmungen und der DSGVO für Webseiten beschäftigt, wir sind jedoch weder Jurist noch Datenschutzbeauftragter. Dementsprechend können wir für die Vollständigkeit, Aktualität und Richtigkeit der von uns bereitgestellten Inhalte keine Haftung übernehmen.

Ein Whitepaper der Agentur Anmut

Richtlinien einhalten und Ihre Webseite rundum absichern.

Gerne beraten wir Sie telefonisch unter 07 11 / 219 55 150
oder per E-Mail an info@agentur-anmut.de