RAIDBOXES

DSGVO-Guide für Agenturen, Freelancer & Webseitenbetreiber

ZEITSPAREND ZUR DSGVO-KONFORMITÄT

Inhaltsverzeichnis

DSGVO-Guide für Agenturen, Freelancer & Webseitenbetreiber

ZEITSPAREND ZUR DSGVO-KONFORMITÄT

Virginia Ostfeld, Leefke Krönke, Johannes Benz & Torben S. Meier « RAIDBOXES

In diesem kostenlosen E-Book möchten wir sowohl Agenturen und Freelancer als auch Webseiten- und WooCommerce Shopbetreiber mit den wichtigsten Inhalten der EU Datenschutz-Grundverordnung (EU-DSGVO) vertraut machen. Außerdem schauen wir uns konkrete Anwendungsfälle wie Tracking, E-Mail-Marketing und WordPress-Plugins an.
In diesem Guide findest du konkrete To-Dos und eine Checkliste, die dich dabei unterstützen, dein Unternehmen und deine WordPress-Seite rechtzeitig DSGVO-konform zu machen.

1. Was ist die DSGVO und was muss ich beachten?

Die europäische Datenschutz-Grundverordnung (engl. General Data Protection Regulation oder GDPR) wird am 25. Mai 2018 in allen Mitgliedsstaaten der Europäischen Union wirksam. Sie wurde im April 2016 vom EU-Parlament bestätigt und ist bereits am 25. Mai 2016 in Kraft getreten. Damit endet in wenigen Wochen die zweijährige Übergangsfrist. Das bedeutet, dass ab dem 25. Mai 2018 bei Nichteinhaltung der Vorgaben hohe Bußgelder verhängt werden können.

Die DSGVO ist keine Richtlinie der Europäischen Union, sondern eine Verordnung. Das bedeutet, dass sie unmittelbar gilt und die Mitgliedstaaten nur in geringem Maße davon abweichen dürfen. Diese Abweichungen werden durch die sogenannten ‚Öffnungsklauseln' geregelt, die in einigen Bereichen der Verordnung nationale Regelungen erlauben. Die für Deutschland einschlägigen Regelungen finden sich dabei vor allem im Bundesdatenschutzgesetz-Neu (kurz BDSG).

Das Ziel der DSGVO ist es, durch eine Harmonisierung des Datenschutzes personenbezogene Daten in allen EU-Mitgliedsstaaten gleichermaßen zu schützen. Außerdem soll durch die DSGVO der freie Verkehr personenbezogener Daten in der EU geregelt werden. Dieser Aspekt zeigt, dass die DSGVO auch wirtschaftliche Interessen berücksichtigt. Des Weiteren berücksichtigt die DSGVO neue Technologien und stärkt die Rechte von Internetnutzern.

Was sind personenbezogene Daten?

Als personenbezogene Daten gelten ‚alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen' (Art. 4 Nr. 1 DSGVO).

Dazu gehören zum Beispiel:

- Name
- Anschrift
- E-Mail-Adresse
- Telefonnummer
- Geburtstag
- Kontodaten
- Standortdaten
- IP-Adresse
- Nutzungsverhalten

In diesem Zusammenhang solltest du wissen, dass auch pseudonymisierte Daten personenbezogen sind. Als nicht personenbezogen gelten Daten nur, wenn sie gänzlich anonymisiert, also nicht zurückführbar auf eine natürliche Person, verarbeitet werden.

Viele der technischen Maßnahmen begründen sich auf die Verwendung von IP-Adressen. Das IP-Adressen und Cookies ganz klar zu personenbezogenen Daten gehören ist die wesentliche Klarstellung seitens der DSGVO.

Welche Handlungen zählen als Datenverarbeitung?

Als Verarbeitung gelten laut DSGVO Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder die Verknüpfung, Einschränkung, Löschen oder Vernichtung von personenbezogenen Daten.

Demnach verarbeitest du als WordPress-Nutzer bspw. Daten, wenn …

- … du die WordPress-Kommentarfunktion nutzt. (Dabei werden Name, E-Mail-Adresse, Zeitstempel und IP-Adresse in der Datenbank gespeichert)
- … sich Nutzer oder Kunden auf deiner Seite registrieren können
- … du Kontaktformulare verwendest
- … du Analyse- oder Tracking-Tools nutzt
- … du Plugins nutzt, die Daten verarbeiten

Wen betrifft die DSGVO?

Die Datenschutz-Grundverordnung betrifft jeden, der personenbezogene Daten verarbeitet. Da Online-Kennungen wie IP und Cookies laut DSGVO als personenbezogene Daten gelten, ist im Prinzip jeder Webseitenbetreiber davon betroffen, der Daten von EU-Bürgern verarbeitet.

Bei der DSGVO gilt das Marktortprinzip. Das bedeutet, dass die DSGVO auch für dich gilt, wenn dein Unternehmen zwar nicht in der EU ansässig ist, aber deine Kunden oder Webseitenbesucher EU-Bürger sind.

Welche Strafen drohen?

Wenn du den Anforderungen der DSGVO nicht nachkommst, musst du mit einem Bußgeld von bis zu 10 Mio. Euro oder von bis zu 2 Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres rechnen, je nachdem, welcher Wert der höhere ist.

In einigen besonders gravierenden Missbrauchsfällen liegt der Bußgeldrahmen sogar bei bis zu 20 Mio. Euro und bis zu 4 Prozent des Jahresumsatzes, je nachdem, was höher ist.

Wodurch können Verstöße bekannt werden?

- Durch aktive Inspektionen, die die Aufsichtsbehörde durchführen wird
- Durch Kunden, Mitarbeiter oder Mitbewerber, die Verstöße bei der Aufsichtsbehörde melden
- Durch Selbstanzeige nach einem Verstoß
- Durch Journalisten oder Blogger, die Verstöße öffentlich aufdecken

Die Wahrscheinlichkeit, dass die aktiven Überprüfungen der Aufsichtsbehörde genau bei dir stattfinden, ist vermutlich sehr gering. Dennoch solltest du dir bewusst sein, dass ein Verstoß gegen die DSGVO auch von anderen Personen bei den Behörden gemeldet werden kann. Bei der Bemessung des Strafmaßes wird dabei auch die Art und Weise, wie der Verstoß bekannt wurde, sowie der Umfang der Zusammenarbeit mit der Aufsichtsbehörde berücksichtigt.

2. Die acht Grundprinzipien der DSGVO

Bevor wir auf konkrete Anwendungsfälle für Webdesigner, Marketer und Webseitenbetreiber eingehen, hier erst einmal die grundlegenden Prinzipien der DSGVO:

Rechtmäßigkeit

Im Prinzip bedeutet dieser Punkt, dass du personenbezogene Daten nur verarbeiten darfst, wenn die Verarbeitung der Daten gemäß DSGVO rechtmäßig ist (siehe Verbot mit Erlaubnisvorbehalt).

Transparenz

Betroffene müssen die Verarbeitung ihrer personenbezogenen Daten nachvollziehen können. Deshalb ist eine verständliche Datenschutzerklärung so wichtig. Die DSGVO verschärft außerdem die Informationspflichten, worauf wir später noch eingehen.

Verbot mit Erlaubnisvorbehalt

Die DSGVO definiert sechs Bedingungen, von denen mindestens eine für eine rechtmäßige Verarbeitung personenbezogener Daten erfüllt sein muss:

1. Zweckgebundene Einwilligung
2. Vorvertragliche Maßnahmen oder Erfüllung eines Vertrages
3. Rechtliche Verpflichtung zur Verarbeitung
4. Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen
5. Verarbeitung im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt
6. Ein berechtigtes Interesse, welches eine Datenverarbeitung rechtfertigt. Hier ist allerdings Vorsicht geboten bis die ersten Gerichtsentscheidungen vorliegen

Interessenabwägung

Ein berechtigtes Interesse (legal oder wirtschaftlich) allein reicht allerdings nicht aus, um die Verarbeitung personenbezogener Daten zu rechtfertigen, denn es muss zusätzlich eine Notwendigkeit für die Verarbeitung bestehen. Außerdem dürfen, wenn du dich bei der Datenverarbeitung auf berechtigtes Interesse stützt, die Interessen der Betroffenen nicht überwiegen.

Praxisbeispiel Interessenabwägung

Wenn du beispielsweise als Webseitenbetreiber Tracking ohne Einwilligung betreibst und es mit wirtschaftlichem Interesse begründet, wird das Interesse des Betroffenen, anonym zu bleiben, höchstwahrscheinlich höher gewichtet. Damit ist die Datenverarbeitung nicht rechtmäßig.

Wenn du dich bei der Datenverarbeitung auf ein berechtigtes Interesse stützt, solltest du also immer eine Widerspruchsmöglichkeit (z.B. ein Opt-Out) bereitstellen. Sobald ein Betroffener das Opt-Out in Anspruch nimmt, darfst du die Daten nicht mehr verarbeiten. Wie genau du mit den Daten umgehst, muss in deiner Datenschutzerklärung stehen.

Zweckbindung

Du darfst die erhobenen Daten nur für den Zweck verwenden, für den du sie erhoben hast und für den du die Einwilligung des Betroffenen eingeholt hast. Den Zweck der Verarbeitung darfst du nur nachträglich ändern, wenn er ‚mit dem ursprünglichen Zweck vereinbar ist'.

Datenminimierung

Du darfst nur die personenbezogenen Daten verarbeiten, die du tatsächlich benötigst. Ein Erheben von Daten darüber hinaus ist nicht erlaubt ...

Integrität und Vertraulichkeit

Du musst die personenbezogenen Daten, die du verarbeitest, durch technische und organisatorische Maßnahmen (TOM) vor unbefugter Verarbeitung, Zerstörung, Veränderung oder Verlust schützen.

Privacy by Design

Mit Privacy by Design ist die Verpflichtung gemeint, den Datenschutz schon bei der Konzeption neuer Produkte oder Techniken (z.B. Hard- oder Software) zu berücksichtigen. Dadurch soll die unrechtmäßige Datenverarbeitung möglichst früh verhindert werden.

Privacy by Default

Dieser Grundsatz verpflichtet dazu, dass bei Geräten oder Online-Plattformen bereits die Voreinstellungen die höchste Datenschutzstufe gewährleisten. Das bedeutet beispielsweise, dass diese Geräte und Dienste so vorkonfiguriert sein müssen, dass nur die für den Verwendungszweck unbedingt notwendigen Daten erhoben werden.

3. Deine Pflichten als Webseitenbetreiber

Einholen der Einwilligung zur Datenverarbeitung:

- Die Einwilligung muss freiwillig erfolgt sein
- Die Einwilligung muss aktiv gegeben werden. Ein Opt-In-Feld darf also nicht vorausgefüllt sein
- Der Betroffene muss ein Wahlrecht haben. Er muss also deinen Service auch nutzen können, wenn er nicht einwilligt
- Bevor du die Einwilligung einholst, musst du den Betroffenen über den Zweck der Datenverarbeitung informieren
- Du musst die Einwilligung nachweisen können
- Du musst den Betroffenen auf sein Widerrufsrecht hinweisen

Wichtig ist hier, dass du das Grundprinzip der Zweckbindung beachtest. Das bedeutet, dass du die Daten nur für den Zweck verwenden darfst, für den du die Einwilligung nachweisen kannst. Für einen anderen Datenverarbeitungsvorgang benötigst du demnach eine weitere Einwilligung. Wie kleinteilig die einzelnen Einwilligungen von Gerichten bewertet werden (z.B. ob der Versand des Newsletters und die Personalisierung des Newsletters zwei getrennte Zwecke sind), wird sich in den ersten Urteilen zeigen.

Rechenschaftspflicht

Du musst auf Anfrage der Datenschutzaufsichtsbehörde vorweisen können, dass du die Vorgaben der DSGVO einhältst. Bedeutet also, dass du innerhalb einer festgesetzten Frist (z.B. 72 Stunden) der anfragenden Behörde Dokumente über z.B. deine Verarbeitungstätigkeiten, die erteilten Einwilligungen, usw. vorlegen musst.

Informationspflicht bei Datenpanne

Wenn eine Datenpanne stattgefunden hat, musst du den Betroffenen und die Datenschutzaufsichtsbehörde innerhalb von 72 Stunden darüber informieren.

4. Die Rechte deiner Kunden und Webseitenbesucher

Recht auf Richtigkeit der Daten

Personenbezogene Daten müssen korrekt und auf dem neuesten Stand sein. Als Verarbeiter der Daten musst du entsprechende Maßnahmen treffen, um veraltete Daten zu löschen oder zu berichtigen.

Recht auf Löschung der Daten – Recht auf Vergessenwerden

Die betroffenen Personen können ihre Erlaubnis zur Datenverarbeitung jederzeit zurückziehen. Wenn das geschieht, musst du die betroffenen Daten sofort löschen.

Recht auf Übertragbarkeit der Daten

Betroffene können dich darum bitten, die Daten, die sie dir zur Verfügung gestellt haben (z.B. bei der Anmeldung), an einen Dritten zu übertragen. Dadurch soll ein Anbieterwechsel erleichtert werden.

Auskunftsrecht

Betroffene haben das Recht zu erfahren:

- Welche personenbezogenen Daten du speicherst und für welchen Zweck
- Wie du diese Daten verarbeitest
- Wo und wie lange du sie speicherst
- Ob du personenbezogene Daten an Dritte weitergibst

Sobald du nach einer solchen Auskunft gefragt wirst, hast du 72 Stunden Zeit, um zu reagieren. Du solltest dich daher nach Möglichkeit bereits jetzt darüber informieren, wie du möglichst schnell deine Datenbank durchsuchen kannst. Ebenfalls gilt es beim Auskunftsrecht zu beachten, dass du dir sicher sein musst, dass derjenige, der die Auskunft anfordert, auch Berechtigter ist. Es muss also eine Verifizierung stattfinden.

Widerspruchsrecht

Jeder Nutzer hat das Recht, jederzeit seine Einwilligung zur Datenverarbeitung zu widerrufen.

5. Die wichtigsten To-Dos

Leider sind mit der DSGVO einige To-Dos verbunden, die sich nicht vermeiden lassen. Wir haben hier die wichtigsten To-Dos und Ressourcen zusammengestellt, damit du sie möglichst schnell und strukturiert abarbeiten kannst. Wie oben im Disclaimer dargestellt, können wir keine Haftung für Richtigkeit und Vollständigkeit übernehmen. Allerdings bringt dich unsere Liste auf ein akzeptables oder gutes Niveau und macht dich deutlich weniger angreifbar. Allein das Umsetzen der hier genannten Punkte zeigt, dass du Datenschutz ernst nimmst, was sich bei jeder Prüfung positiv auswirkt.

Priorisierung von To-Dos

Da es sich um eine ganze Reihe von Maßnahmen handelt, die teils sehr umfangreich sind, ist es unabdingbar eine Priorisierung vorzunehmen. In der Darstellung der To-Dos haben wir die Maßnahmen innerhalb der Kategorien absteigend nach Wichtigkeit sortiert. Das Wichtigste zuerst. Diese Sortierung spiegelt eher unsere subjektive Sicht wieder, soll aber bei der Implementierung helfen.

Grundsätzlich solltest du dir bei der Priorisierung und Implementierung folgende Fragen stellen (auch nach Wichtigkeit sortiert):

- Wo habe ich personenbezogene Daten und sind diese gut geschützt?
- Wenn ich personenbezogene Daten verarbeite geschieht dies mit Einwilligung des Betroffenen und bin ich transparent bezogen auf den Einsatzzweck?
- Wo habe ich nach außen hin offensichtliche Defizite, an denen sich Betroffene stören könnten, z.B. eine fehlende Datenschutzerklärung?
- In welchem Ausmaß werden personenbezogene Daten verarbeitet und wie stark könnte sich ein Betroffener dadurch in seinen Rechten verletzt fühlen?
- Kann ich auf Anfrage eine Dokumentation vorlegen, wie ich Daten verarbeite?

Dabei gilt zu beachten, dass alles was von außen direkt und ohne weiteres überprüfbar ist, wahrscheinlich als erstes ins Visier genommen wird. Achte daher auf jeden Fall darauf, eine datenschutzkonforme Datenschutzerklärung und ein vollständiges Impressum zu haben.

6. To-Dos außerhalb deiner Webseite

Gib deinen Daten ein Mindestmaß an Schutz

Bei aller Dokumentationspflicht sollte man eines nicht vergessen: Es geht darum den Datenschutz voranzubringen und Nutzern die Datenhoheit zurück zu geben. Am Ende bringt es nichts, wenn zwar eine umfangreiche Dokumentation vorhanden ist, aber Daten fahrlässig verloren gehen.

Der wichtigste Punkt, den wir bei RAIDBOXES übrigens auch immer wieder betonen, sind sichere Passwörter. Dies gilt für jegliche Applikation, die mit Kundendaten arbeitet. Der aktuell häufigste Grund für Malware bei uns, sind sehr einfache Passwörter! Diese sind dann so einfach, dass Programme sie automatisiert erraten können.

Aus diesem Grund haben wir sichere Passwörter als Pflicht beim Anlegen einer WordPress-Webseite eingeführt. Ein Passwort sollte aus mindestens 7 Zeichen bestehen, Sonderzeichen, Zahlen und Groß- und Kleinbuchstaben enthalten.

Da auch wir uns hunderte Passwörter nicht merken können, nutzen wir einen Passwort-Manager, konkret 1Password. Die Passwort-Manager sind dann in das Betriebssystem eingebettet und fügen die sicheren Passwörter je nach Situation auch automatisch ein. Weitere Maßnahmen sind eine verschlüsselte Festplatte, die Trennung zwischen privaten und geschäftlichen Daten und eine Antivirensoftware.

Veröffentliche eine (angepasste) Datenschutzerklärung

Wenn deine Webseite nicht rein privater Natur ist (z.B. nur Bilder von Freunden und Verwandten beinhaltet), brauchst du eine Datenschutzerklärung, die leicht verständlich sein muss. Sobald du personenbezogene Daten verarbeitest (z.B. IP-Adressen), muss deine Webseite eine DSGVO-konforme Datenschutzerklärung aufweisen. Dabei ist es egal, ob du die Seite kommerziell nutzt oder nicht.

Ein empfehlenswertes Muster für eine DSGVO-konforme Datenschutzerklärung findest du beispielsweise auf dem Internetauftritt des ITM Münster.

Tipp!

Es gibt Online-Tools, mit denen du eine Datenschutzerklärung erstellen kannst, wie z.B. von e-recht24.de oder rechtsanwalt-metzler.de. Die Macher der Tools übernehmen natürlich keine Haftung, darum solltest du die generierte Datenschutzerklärung unbedingt selbst überprüfen bzw. diese, wenn du ganz sichergehen möchtest, von einem Datenschutz-Experten oder einem Anwalt prüfen lassen.

Schließe Auftragsdatenverarbeitungsverträge (ADV) mit Drittanbietern

Ein sogenannter Auftragsdatenverarbeitungsvertrag (ADV) ist grundsätzlich nötig, wenn Drittanbieter Daten deiner Kunden oder Webseitenbesucher im Auftrag verarbeiten. Mit diesen Drittanbietern (z.B. Newsletter-Anbieter, Webhoster, Besucher-Tracking wie Google Analytics etc.) musst du einen ADV abschließen.

Unter Auftragsdatenverarbeitung fällt die Erhebung, die Verarbeitung oder die Nutzung von personenbezogenen Daten durch einen Auftragnehmer nach den Weisungen des Auftraggebers. Im ADV-Vertrag wird die Datenverarbeitung zwischen dem Auftragnehmer und dem Auftraggeber vertraglich geregelt.

Google stellt beispielsweise online einen ADV-Vertrag für die Nutzung von Google Analytics bereit. Diesen Vertrag musst du ausdrucken, beide Exemplare unterschreiben und diese dann an die Vertragsadresse in Irland schicken. Google wird die Verträge ebenfalls unterschreiben und dir dann eine Version wieder zurücksenden. Die bittere Wahrheit ist leider, dass hier mit jedem Anbieter ein ADV geschlossen werden muss, der deine personenbezogenen Daten im Auftrag verarbeitet.

Sorge für ausreichende Dokumentation

Mit wenigen Ausnahmen muss jeder, der personenbezogene Daten verarbeitet, ein Verzeichnis der Verarbeitungstätigkeiten (inkl. einer Beschreibung der technischen und organisatorischen Maßnahmen (TOMs) vorlegen können. Auf folgender Seite kannst du bspw. ein kostenloses Muster herunterladen.

7. To-Dos auf deiner WordPress-Webseite

Ist WordPress überhaupt DSGVO-konform?

Seit kurzem gibt es im WP-Core ein GDPR-Compliance-Team, welches die DSGVO-Konformität von WordPress vorantreibt. Das GDPR-Team hat sich unter anderem zum Ziel gesetzt, verständliche Datenschutzrichtlinien für Webseitenbetreiber, Guidelines für Plugin-Entwickler und Dokumentation über die Anforderungen der DSGVO zur Verfügung zu stellen. Außerdem arbeitet das Team an DSGVO-Tools, die bis Anfang Mai in den Word-Press-Core integriert werden sollen.

WordPress als Ganzes betrachten

Ein wichtiges WordPress-Kernfeature, nämlich die Kommentarfunktion, ist beispielsweise aktuell noch nicht DSGVO-konform. Konkrete Maßnahmen findest du unter dem Punkt ‚Kontaktformulare' weiter unten.

Außerdem solltest du als Webseitenbetreiber alle deine WordPress-Plugins auf DSGVO-Konformität überprüfen. Die meisten Plugin-Anbieter haben bereits Informationen bereitgestellt, die dir helfen, die entsprechenden Einstellungen vorzunehmen.

DSGVO-Plugins als Hilfestellung

Es gibt sogar bereits Plugins, wie beispielsweise WP DSGVO Tools (3,000+ aktive Installationen), die dir bei der Umsetzung der DSGVO-Konformität deiner WordPress-Seite helfen.

Mit WP DSGVO Tools kannst du durch Integrationen außerdem die Datenverarbeitung weiterer Plugins wie bspw. Contact Form 7, Gravity Forms, WooCommerce, MailChimp oder den Events Manager verwalten. Die Macher der Plugins übernehmen dabei natürlich keine Haftung, denn du als Webseitenbetreiber musst dafür sorgen, dass der Datenschutz gewährleistet ist.

Was müssen Shopbetreiber mit WooCommerce beachten?

Wie bei allen Drittanbietern geht es bei WooCommerce zunächst darum, zu überprüfen, ob und welche personenbezogenen Daten durch das Plugin verarbeitet werden. WooCommerce hat sich bereits zur DSGVO geäußert und betont dabei, dass es keine Musterlösung für alle gibt:

> *‚Each WooCommerce site uses a different set of plugins, has a different flow for shipping, etc., so there isn't a one-size-fits-all approach'.*

In dem WooCommerce-Beitrag wird außerdem betont, dass es die Pflicht des Webseitenbetreibers ist, seine Besucher über die Verwendung des Plugin und die Verwendung der Daten aufzuklären. Dafür ist eine DSGVO-konforme Datenschutzerklärung das A und O.

8. DSGVO-bedenkliche WordPress-Plugins auf deiner Webseite entfernen und mit DSGVO-konformen Alternativen ersetzen

Selbst Plugins, die vom kommerziellen WordPress-Unternehmen Automattic selbst zur Verfügung gestellt werden, benötigen eine gültige Verbindung zu wordpress.com und damit auch eine direkte Verbindung nicht nur deiner Daten, sondern auch der IPs deiner Webseitenbesucher.

Sie sind das perfekte Beispiel dafür, bei welcher Art von Plugins du vor dem 25.05.2018 reagieren solltest, um sie mit einer EU-DSGVO-konformen Alternative zu ersetzen bis die Unternehmen ggf. eine rechtskonforme Version ihrer Plugins veröffentlichen. Rechtskonform werden sie dann, wenn sie keinerlei personenbezogene Daten, wie z.B. IP-Adressen weitergeben.

Exemplarisch stehen hierfür folgende Automattic Plugins:

- Jetpack (Statistik-Plugin)
- Gravatar (Community-Plugin)
- Akismet (Anti-Spam Plugin)
- VaultPress (Backup Plugin)
- WP Super Cache (Caching Plugin)

Um deinen Webseitenbetrieb aber weiter gewährleisten zu können, kannst du auf folgende Alternativen zurückgreifen, die keinerlei persönliche Daten deiner Besucher weitergeben.

Anonyme Besucher-Statistiken erheben

Auch wir möchten natürlich gerne wissen, was auf unserer Webseite besonders gut funktioniert und gern gelesen oder geteilt wird und wie lange Besucher verweilen oder wie hoch die Absprungrate ist. Mit der EU-DSGVO wird die Gesetzeslage noch ein wenig verschärft. Du musst, wie bereits unter der aktuellen deutschen Datenschutzgrundverordnung, jeden Besucher deiner Webseite vollständig anonymisieren. Jedoch dürfen darüber hinaus auch keine persönlichen Daten an andere Dienste übertragen werden. Aus diesem Grund empfehlen wir Statify, damit alle anonymisierten personenbezogenen Daten auf deiner Webseite verbleiben und an keine weiteren Dienste weitergegeben werden.

Statify anstelle von Jetpack

Laut Angaben der Entwickler von Statify verarbeitet, versendet und speichert das Plugin keinerlei personenbezogene Daten, wie Cookies oder IP-Adressen außerhalb deiner Webseite.

WordPress-Backup-Plugins mit alternativen Lösungen ersetzen

Integrierte WordPress-Backups anstelle von VaultPress

Um dem Übertragen von personenbezogenen Daten auf beispielsweise amerikanische Server entgegenzuwirken und als positiven Nebeneffekt weitere Performance-Kapazitäten deiner Webseite freizumachen, empfehlen wir auf spezielle WordPress-Backup Plugins zukünftig zu verzichten. Eine bessere Alternative ist das nutzen von automatischen WordPress-Backups über deinen WordPress-Hoster wie z.B. bei RAIDBOXES.

9. Rechtswidrige Verbindungen von Social Plugins, wie der Facebook Like Button, Like Box oder Twitter Widgets, unterbinden

Shariff Wrapper anstelle von z.B. AddToAny Share Buttons

Share-Dienste verwenden häufig bereits Daten, sobald sich deine Besucher auf der Webseite mit aktivem Social Plugin befinden. Auch wenn ein Nutzer noch gar nichts geteilt hat, werden die Daten bereits weitergegeben. Dies ist noch weitestgehend unbekannt, im Sinne der DSGVO allerdings kritisch.

Bei der Recherche nach rechtskonformen Lösungen sind wir nur auf ein einziges kostenloses Social Plugin gestoßen, das die Weitergabe von Daten noch vor dem Klick auf einen Share-Button verhindert. Wir empfehlen daher zum jetzigen Zeitpunkt integrierte Twitter Widgets oder Facebook Like Buttons oder der Like Box zu löschen und für Share-Buttons in Beiträgen auf das Social Plugin von Shariff Wrapper zu setzen.

Antispam-Schutz auf die eigene Webseite beschränken

Antispam Bee anstelle von Akismet

Antispam Bee lässt sich DSGVO-konform nutzen, wenn du folgende Einstellung des Plugins beachtest: Die Einstellung ‚Öffentliche Spamdatenbank berücksichtigen' sowie die Funktion ‚Kommentare nur in einer bestimmten Sprache zulassen' müssen von dir in den Einstellungen des Plugins deaktiviert sein, sonst werden weiter die IP-Adressen deiner Besucher an den Dienst Stop Forum Spam übermittelt und der Kommentartext zur Spracherkennung an Google Translate geschickt.

CDN-Anbieter überprüfen und ggf. ersetzen

Serverseitiges Caching anstelle von ausländischem CDN

Bei einem CDN-Anbieter wird die Seite auf fremden Servern zwischengespeichert. Durch das Zwischenspeichern kann die Webseite dann schneller ausgeliefert werden. Gerade bei Eingabe von Formulardaten kann dies zu Problemen hinsichtlich Datenschutz führen.

Sollten deine Besucher aus der DACH-Region kommen, erfüllt ein Cache die gleiche Funktion, wie ein CDN. Die Webseite wird genau so schnell, wenn nicht sogar schneller ausgeliefert. Bei RAIDBOXES ist Caching serverseitig integriert und es wird nur auf deutschen Servern mit ISO 21007-Zertifizierung abgespeichert.

Daher hast du folgende Möglichkeiten um das schnelle Laden DSGVO konform zu gestalten:

- Du nutzt Caching-Plugins oder wechselst zu einem deutschen Anbieter mit serverseitigen Caching
- Du überprüfst ob dein ausländischer CDN-Anbieter das Privacy-Shield Abkommen unterstützt und schließt einen ADV mit dem Anbieter
- Du nutzt einen europäischen CDN-Anbieter, wie KeyCDN. Auch hier musst du einen ADV schließen

Double-Opt-In-Verfahren für Kommentare

Hier soll vorab gesagt sein, dass die Benachrichtigung von weiteren Kommentaren zum eigenen Kommentar bereits voraussetzt, dass Daten weitergegeben werden. Um dennoch der Grauzone keine Möglichkeit der falschen Interpretation zu geben, nutze das kostenlose Plugin Subscribe to Double-Opt-In Comments, um vorab vom Besucher bestätigen zu lassen, dass er wirklich Benachrichtigung über Folgekommentare erhalten möchte.

Rechtskonforme Avatare für Blog & Kommentare verwenden

WP User Avatar anstelle von Gravatar

Um Gravatar allerdings vollständig in WordPress zu deaktivieren, musst du noch folgende Einstellungen im WordPress Admin-Bereich unter dem Menüpunkt ‚*Einstellungen*' tätigen.

Im Untermenü unter Diskussionen: Hier musst du ganz nach unten scrollen, bis du den Bereich Avatare erreicht hast. Anschließend deaktivierst du das Auswahlfeld: ‚*Avataranzeige – Zeige Avatare*'. Klicke auf Speichern um die Einstellungen zu übernehmen und lösche den Cache deiner Seite. Nun sollte deine Webseite nicht mehr mit Wordpress.com kommunizieren.

Cookie Banner einbauen

Der Fall ‚Cookie-Benachrichtigungen der Nutzer' ist kein Fall, den die DSGVO erstmals regelt. Er wurde bereits vor einiger Zeit mit der Cookie Richtlinie der EU eingeführt. Die DSGVO nimmt Cookies jedoch noch einmal speziell ins Visier, da hiermit personenbezogene Daten verarbeitet werden können.
In jedem Fall solltest du dir daher die Einwilligung des Nutzers einholen.

Das geschieht meist über ein Cookie-Banner. Ein Freemium-Plugin, das diese Funktionalität bietet ist beispielsweise WP DSGVO Tools. Damit bist du zunächst auf der sicheren Seite. Eine wesentliche Änderung kommt dann voraussichtlich erst mit der ePrivacy-Verordnung (ePV) Ende 2019.

10. Formular-Plugins wie z.B. Contact Form 7 & Gravity Forms anpassen

E-Mail Marketing-Prozess anpassen

In deinen Newsletter-Formularen sollte nur die E-Mail-Adresse ein Pflichtfeld sein, alle anderen Daten wie z.B. Vor- und Nachname sollten nur optional abgefragt werden.

Wenn du es bisher noch nicht getan hast, dann nutze ab sofort immer das Double-Opt-In-Verfahren. Beim Double-Opt-In muss der E-Mail-Empfänger nach der ersten Anmeldung ein zweites Mal explizit auf einen Link in einer Bestätigungsmail klicken, um in den Verteiler mit aufgenommen zu werden.

So ist sichergestellt, dass niemand sich in deinem Namen für einen Newsletter anmeldet und die tatsächliche Anmeldung auch von dir gewünscht ist. Die Bestätigungsmail darf keine Werbung oder sonstige Inhalte enthalten.

Acceptance Box bei Kontaktformularen ergänzen

Laut der Datenschutz-Grundverordnung setzt das Versenden eines Formulars die Einwilligung des Versenders voraus. Als Daten gelten nicht nur die IP-Adresse, sondern auch die E-Mail-Adresse und der Inhalt an sich.

Ein Opt-In für die Bestätigung der gewollten Datenspeicherung lässt sich per zusätzlicher Acceptance Checkbox bei Contact Form 7 und bei Gravity Forms mit dem Freemium-Plugin WP DSGVO Tools umsetzen.

Mittel- bis langfristig sind wir davon überzeugt, dass alle bekannten Plugin-Entwickler die nötigen Bestimmungen umsetzen werden, um der DSGVO gerecht zu werden. Bis dahin kann das WP DSGVO Tools wirklich gute Dienste leisten.

11. Technische Maßnahmen außerhalb deiner WordPress-Plugins

SSL-Verschlüsselung implementieren

SSL-Verschlüsselung ist zwar keine Pflicht in der DSGVO, aber ohne eine SSL-Verbindung ist eine sichere Datenübertragung rund um deine Webseite nicht möglich. Mehr über SSL erfährst du auch in unserem ausgiebigen Let's Encrypt SSL-Kompendium.

Du möchtest das SSL-Zertifikat nicht selbst einrichten? Dann nutze z.B. Let's Encrypt SSL-Zertifikate. Kostenlos per 1-Klick-Installation, um ein SSL-Zertifikat für deine WordPress-Webseite schnell und einfach zu aktivieren.

Google Analytics Opt-Out schaffen

In diesem Zusammenhang ist noch einmal darauf hinzuweisen, dass bereits das aktuell gültige Bundesdatenschutzgesetz (BDSG) die vollständige Anonymisierung von Besucherdaten bereits seit Jahren vorschreibt. Um dies zu gewährleisten ist spätestens jetzt das sehr oft benutzte Google Analytics um folgende Code-Zeile zu erweitern:

ga(‚set', ‚anonymizeIp', true);

Sollte dein Javascript Snippet vorab so ausgesehen haben:

```
<script>
(function(i,s,o,g,r,a,m){i[‚GoogleAnalytic-
sObject']=r;i[r]=i[r]||function(){
(i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Da-
te();a=s.createElement(o),
m=s.getElementsByTagName(o)[0];a.async=1;a.
src=g;m.parentNode.insertBefore(a,m)
})(window,document,'script','https://www.goog-
le-analytics.com/analytics.js','ga');
ga(‚create', ‚UA-XXXXXXXX-X', ‚auto');
ga(‚require', ‚displayfeatures');
ga(‚require', ‚linkid', ‚linkid.js');
ga(‚send', ‚pageview');
</script>
```

sieht der Code nach dem Hinzufügen folgendermaßen aus:

```
<script>
(function(i,s,o,g,r,a,m){i[,GoogleAnalytic-
sObject']=r;i[r]=i[r]||function(){
(i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Da-
te();a=s.createElement(o),
m=s.getElementsByTagName(o)[0];a.async=1;a.
src=g;m.parentNode.insertBefore(a,m)
})(window,document,'script','https://www.goog-
le-analytics.com/analytics.js','ga');
ga(,create', ,UA-XXXXXXXX-X', ,auto');
ga(,require', ,displayfeatures');
ga(,require', ,linkid', ,linkid.js');
ga(,set', ,anonymizeIp', true);
ga(,send', ,pageview');
</script>
```

Des Weiteren musst du in deinen Datenschutzbestimmungen eine Möglichkeit schaffen, dass Besucher deiner Webseite sich vollständig aus der Google-Analyse ausschließen lassen können. Ein kostenloses Opt-Out Plugin für Google Analytics findest du mit dem Namen Google Analytics Opt-Out im WordPress-Plugin-Verzeichnis. Es installiert einen Cookie, welches analytics.js davon abhält die Daten zu sammeln.

IP-Adressen in Blog-Kommentaren anonymisieren

WordPress speichert standardmäßig die IP-Adressen der Kommentarschreiber. Dieses Erfassen der IP-Adresse ist nach der neuen EU-DSGVO aber nicht datenschutzkonform.

Du kannst mithilfe eines kleinen PHP-Codes in deiner functions.php das zukünftige Speichern der IP-Adressen verhindern. Wir empfehlen dafür eine Child-Theme zu nutzen, um den Code auch nach der nächsten Aktualisierung deines Themes noch integriert zu haben. Der einzufügende Code lautet:

```
function wpb_remove_commentsip( $comment_author_ip ) {
return ,'; }
add_filter( ,pre_comment_user_ip', ,wpb_remove_commentsip' );
```

Abschließend musst du noch bestehende IP-Adressen rückwirkend in der Datenbank deiner Webseite einmalig manuell löschen. Eine gute Anleitung, wie du dies erledigen kannst, findest du hier.

Google Fonts lokal hosten

Viele WordPress-Seiten machen von Googles kostenlosen Schriftarten (Google Fonts) Gebrauch. Sobald eine Webseite mit Google Fonts aufgerufen wird, werden diese Schriften über den Google Server geladen. Da bei diesem Aufruf Daten an Google übertragen werden, sorgen sich einige Seitenbetreiber um die DSGVO-Konformität von Google Schriften.

Was auf den ersten Blick sehr penibel wirkt, ist bei genauerem Hinsehen doch verständlich. Genau wie oben bei den Facebook-Plugins, ermöglichen die Google Fonts Besucher über eine riesige Anzahl an Webseiten zu tracken und Daten zu senden, obwohl der User dem nie zugestimmt hat.
Google selbst verweist nur auf die allgemeinen Terms of Service ohne sich konkret zu äußern.

Um eine Datenverarbeitung durch Google zu umgehen, kannst du Google Fonts auf deinem eigenen Webserver einbinden. Verständliche Schritt-für-Schritt Anleitungen, wie du diese Maßnahme umsetzt, gibt es zum Beispiel bei WP Ninjas von Jonas Tietgen.

12. Welche Maßnahmen hat RAIDBOXES schon umgesetzt?

Bereits vor der DSGVO haben wir als WordPress-Dienstleister den Datenschutz sehr ernst genommen, weshalb wir einige Vorgaben der DSGVO direkt abhaken konnten. Generell ist Deutschland ein Land mit einem sehr hohem Datenschutzniveau, weshalb du dich bezüglich der Maßnahmen, die du jetzt zusätzlich umsetzten musst, nicht verrückt machen solltest. Besonders wenn du Freelancer bist und keine Mitarbeiter hast, sollten die Maßnahmen relativ schnell umsetzbar sein.

Aktuell arbeiten wir auf Hochtouren daran bis zum 25. Mai komplett DSGVO-konform zu sein. Folgende Maßnahmen haben wir bisher erfolgreich umgesetzt:

- Wir haben alle zu erledigenden Aufgaben und die Verantwortlichen dokumentiert und dafür einen Ablaufplan geschrieben
- Zwei unserer Mitarbeiter haben sich als Datenschutzbeauftragte zertifizieren lassen und das ganze Team bezüglich der DSGVO geschult
- Jeder unserer Mitarbeiter hat eine gesonderte Datenschutzerklärung unterschrieben
- Wir haben Auftragsdatenverarbeitungsverträge (ADV) mit allen Drittanbietern, die wir nutzen, geschlossen
- Wir haben einen ADV erstellt zum Abschluss mit unseren Kunden
- Wir haben unsere technischen und organisatorischen Maßnahmen

dokumentiert, welche Teil unseres ADV sind

- Wir haben eine komplett neue Datenschutzerklärung verfasst. In dieser wirst du sehr ausführlich darüber unterrichtet, wo und wann welche Daten verarbeitet werden
- Unser Bürotüren sind mit Sicherheitsschlössern ausgestattet
- Alle Laptops sind verschlüsselt, mit starken Passwörtern versehen und mit Virenschutz gesichert
- Wir haben auf unserer Webseite alle oben beschriebenen Maßnahmen umgesetzt
- Wir haben starke Passwörter als Pflicht für das Anlegen einer WordPress-Webseite eingeführt
- Wir pflegen ein Verzeichnis über Verarbeitungstätigkeiten
- Wir erstellen einen Double-Opt-In Sign-Up für neue Tester
- Zusätzlich streben wir eine Zertifizierung gemäß ISO 27001 an
- Wir sind Mitglied bei der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.
- Unsere ernannte Datenschutzbeauftragte nimmt in regelmäßigen Abständen an Schulungen teil und strebt derzeit eine Zusatzausbildung im IT-Recht an
- Wir entwickeln ein Sicherheits-Prämienprogramm
- Bei Auskunftsersuchen, wird ein Verifizierungscode verschickt

DSGVO-Checkliste

- [ ] Prüfe alle deine Prozesse, in denen du personenbezogene Daten verarbeitest und sorge für ausreichend Datenschutz (Verarbeitung heißt: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder die Verknüpfung, Einschränkung, Löschen oder Vernichtung).

- [ ] Mit wenigen Ausnahmen muss jeder, der personenbezogene Daten verarbeitet, ein Verzeichnis der Verarbeitungstätigkeiten inkl. einer Beschreibung der technischen und organisatorischen Maßnahmen (TOMs) vorlegen können. Auf folgender Seite kannst du bspw. ein kostenloses Muster herunterladen.

- [ ] Prüfe, ob du einen Datenschutzbeauftragten benötigst (Faustregel: ab 10 Mitarbeitern). Falls ihr keinen benötigt, sollte aber dennoch ein Ansprechpartner für die Datenschutzaufsichtsbehörde ernannt werden.

- [ ] Schließe mit Drittanbietern (z.B. Marketing- oder Tracking-Tools), die in deinem Auftrag personenbezogene Daten verarbeiten, Verträge zur Auftragsdatenverarbeitung (ADV) ab. Dies ist laut DSGVO auch auf elektronischem Weg zulässig.

- [ ] Passe deine Datenschutzerklärung auf die Vorgaben der DSGVO an. Am wichtigsten dabei ist, dass du immer mit angibst, zu welchem Zweck Daten verarbeitet werden und du darüber aufklärst, wie der Datenverarbeitung widersprochen werden kann. Die Datenschutzerklärung sollte dabei für jeden lesbar und verständlich sein.

- Stelle sicher, dass du im Fall einer Überprüfung durch die Behörden oder durch eine Anfrage eines Betroffenen deiner Nachweispflicht nachkommen kannst. (Datenschutzkonzept, Verzeichnis der Verarbeitungstätigkeiten, ADVs, Einwilligungen, etc.).

- Wenn du Betreiber einer WordPress-Seite bist, überprüfe, ob du Plugins verwendest, die personenbezogene Daten verarbeiten und ob diese DSGVO-konform sind. Viele bekannte Plugins haben bereits Informationen hinsichtlich der DSGVO veröffentlicht.

- Prüfe, ob dein Impressum vollständig ist!

RAIDBOXES ist Mitglied bei der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.