WordPress und der Datenschutz:
Was Blogbetreiber beachten sollten

# DSGVO-proof bloggen

**Ritchie Pettauer**

Auch Blogger, Selbstständige, Vereine und Kleinstunternehmen müssen sich mit den Regeln des neuen, europaweit geltenden Datenschutzgesetzes auseinandersetzen. Betreiber von WordPress-Websites können ihre Seiten mit verhältnismäßig wenig Aufwand DSGVO-konform gestalten.

Am 25. Mai 2018 trat die europäische Datenschutz-Grundverordnung (EU-DSGVO) in Kraft. Sie legt EU-weit einheitliche Regeln im Umgang mit personenbezogenen Daten fest, löst nationale Gesetzgebungen ab und soll innerhalb Europas sowohl den Datenschutz sicherstellen als auch den freien Datenverkehr erleichtern – zumindest in der Theorie. In der Praxis allerdings schüren die erhöhten Datenschutzstandards spätestens seit April eine veritable Panik in der Webbranche. Das liegt primär an den horrend hohen angedrohten Strafen: Bis zu 20 Millionen Euro oder vier Prozent des Jahresumsatzes soll ein „besonders schwerwiegender" Verstoß kosten. Kleinere Unternehmen, Selbstständige und Blogger fürchten sich – zumindest in Deutschland – zudem vor Abmahnungen: Verstöße gegen die DSGVO sind auf Websites besonders leicht zu entdecken.

Die DSGVO erschwert oder verunmöglicht in der Tat viele bislang gängige Webmarketing-Praktiken und fordert von den Betreibern kommerzieller Webseiten eine eingehende Beschäftigung mit möglichen Problemfeldern. Denn sie klassifiziert – zum Missfallen vieler Experten – IP-Adressen als personenbezogene Daten. Die technische Struktur des Web bedingt aber bei jeder Datenübertragung von einem Server zum anderen die Übermittlung dieser IP-Adresse.

Auch wenn man also nicht explizit Nutzerdaten sammelt, unterliegt man als Websitebetreiber den Bestimmungen des neuen Gesetzes. Schon allein der Betrieb einer „ganz normalen" WordPress-Instanz reicht aus, um gleich an mehreren Stellen potenziell gegen Vorgaben der DSGVO zu verstoßen. Denn überall dort, wo Daten von oder zu Drittservern übertragen werden, ist eine vorherige Zustimmung des Nutzers grundsätzlich erforderlich.

Die ideologischen Grundpfeiler der neuen Verordnung lauten „Datenminimierung" und „Transparenz". Für die betroffene Person soll nicht nur klar sein, welche ihrer Daten von wem wann und warum verarbeitet werden, sie soll auch jederzeit Einsicht in gespeicherte Daten nehmen und deren Löschung beantragen können, soweit nicht andere gesetzliche Bestimmungen vorrangig sind, etwa die Aufbewahrungspflicht für Finanzunterlagen.

Zugleich darf der Datenverarbeiter nur die für den jeweiligen Verwendungszweck notwendigen Daten speichern. Und auch dies nicht auf immer und ewig, sondern lediglich für einen „angemesse-

nen Zeitraum“. Das hört sich wie ein Befreiungsschlag gegen zweifelhafte Datenhandelspraktiken an, betrifft aber letztlich jeden Webseitenbetreiber, dessen Provider Serverlogs und Zugriffsstatistiken mit gespeicherten IP-Adressen vorhält. Dafür gibt es schließlich auch gute Gründe.

## Daten speichern aus „berechtigtem Interesse“

Die guten Gründe heißen im Fachjargon der DSGVO „berechtigtes Interesse“: Wann immer der Betreiber einer Webseite Nutzerdaten speichert oder an Drittservices überträgt, muss er ein solches glaubhaft argumentieren. Mangels Präzedenzfällen wird es im Zweifelsfall den zuständigen Behörden obliegen, in Einzelfällen über dieses berechtigte Interesse zu entscheiden. Genau diese Unsicherheit verleitete zahlreiche Blogger dazu, ihre Seiten vor dem 25. Mai präventiv offline zu nehmen.

Die große Abmahnwelle ist zwar bisher ausgeblieben, doch nationale und EU-Politiker sind sich alles andere als einig: Angela Merkel sprach von einer Überforderung speziell für KMU, während die zuständige EU-Kommissarin Věra Jourová keine großen Veränderungen im Vergleich zur Datenschutzrichtlinie von 1995 sehen wollte, aber zugleich eingestand, dass sie keine vollständige Compliance aller Akteure zum Stichtag erwarte (siehe ix.de/ix1809052).

Das österreichische Parlament nahm in der nationalen Umsetzung sogar in letzter Minute ganze Berufsgruppen, unter anderen Künstler und Journalisten, komplett von der DSGVO aus. Wenn sich selbst die Experten in manchen scheinbar völlig trivialen Punkten uneinig sind, dann bleibt dem pragmatischen Webmaster nur eines übrig: die Bestimmungen der DSGVO so gut zu erfüllen, dass eine Abmahnung möglichst unwahrscheinlich wird.

Nährboden für ein lukratives Abmahnwesen à la Impressumspflicht bietet die DSGVO keinen, denn allfällige Strafen sind nicht an die Konkurrenz, sondern an die staatlichen Behörden zu bezahlen. Allenfalls über den Umweg des Wettbewerbsrechts könnten einzelne Bestimmungen der DSGVO die Grundlage für eine entsprechende Schadensersatzklage bieten – die aufgrund der beschriebenen Rechtsunsicherheit aber für den Kläger mit einem beträchtlichen finanziellen Risiko verbunden wäre.

## Für welche Webseiten gilt die DSGVO überhaupt?

Grundsätzlich gilt die DSGVO für alle nicht privaten Webseiten, also für Vereine und NGOs, Blogger und Selbstständige ebenso wie für kleine und mittlere Unternehmen und Großbetriebe, die sich an ein europäisches Publikum richten. Der geografische Standort von Server und Unternehmen spielt keine Rolle.

Ausgenommen sind lediglich private Webseiten. Diese können zwar öffentlich zugänglich sein, dürfen aber keinerlei Werbung enthalten und keine kommerzielle Absicht des Betreibers erkennen lassen. Letzteres jedoch ist ein Kriterium, das nur ein verschwindend kleiner Teil der deutschsprachigen Blogландschaft erfüllt, zumal ein einziges Banner oder ein Testbericht bereits für die Klassifizierung als kommerzielles Onlineangebot ausreicht.

Während die Betreiber selbst gehosteter WordPress-Websites zumindest die technischen Möglichkeiten haben, die Vorgaben der DSGVO entsprechend zu implementieren, stellt sich die Situation bei Hosting-Plattformen wie Blogger.com oder WordPress.com um einiges komplizierter dar: Die Nutzer dieser Gratisangebote sind auf die Umsetzung durch den jeweiligen Plattformbetreiber angewiesen.

## Die Grundanforderungen der DSGVO an jede Webseite

**Datenschutzerklärung:** Die Nutzer eines Onlineangebots sollen transparent und in verständlichen Worten über die zur Anwendung kommenden Datenverarbeitungsverfahren aufgeklärt werden. Die Datenschutzerklärung muss die entsprechenden Rechtsgrundlagen auflisten und den Nutzer über alle relevanten Datenverarbeitungsvorgänge aufklären.

Da die wenigsten Seitenbetreiber über das juristische Fachwissen verfügen, bieten spezialisierte Rechtsanwaltskanzleien kostenpflichtige – manche auch kostenlose – Vorlagen an.

**Verschlüsselung:** Auch wenn die DSGVO nicht grundsätzlich ein SSL-Zertifikat voraussetzt, wird die SSL-Verschlüsselung der eigenen Seiten jedoch spätestens dann zur Pflicht, wenn der Seitenbetreiber Formulare zur Datenübermittlung bereitstellt.

Ein kostenloses Zertifikat, etwa von Let’s Encrypt, reicht völlig aus. Die meisten Hosting-Provider bieten SSL-Verschlüsselung inzwischen ohne Aufpreis an.

**Recht auf Auskunft und Löschung:** Werden personenbezogene Daten gespeichert, so hat die betreffende Person in jedem Fall das Recht, Auskunft über diese Daten zu erhalten und diese in weiterer Folge auch löschen zu lassen.

In Zusammenhang damit ist auch die in der DSGVO geforderte Datenportabilität zu sehen: Websitebetreiber müssen ihren Nutzern die von diesen selbst bereitgestellten personenbezogenen Daten auf deren Verlangen in einem wiederverwendbaren Format zur Verfügung stellen.

**Abschließen eines Datenverarbeitungsvertrags:** Daten europäischer Nutzer dürfen nur dann an Server außerhalb der EU übertragen werden, wenn der jeweilige Anbieter nach den Bestimmungen des Privacy Shield Framework zertifiziert ist und einen sogenannten Datenverarbeitungsvertrag (DVV) anbietet. Dieses Dokument regelt den gegenseitigen Umgang mit personenbezogenen Daten und kann in digitaler Form angeboten werden. Nutzt man also Google Analytics, den Newsletter-Service von Mailchimp oder die Dienste anderer nichteuropäischer Anbieter, ist der Abschluss eines DVV mit diesen zwingend erforderlich.

## DSGVO-verträglich mit WordPress-Bordmitteln

WordPress ist längst kein reines Blog-CMS mehr, sondern wird zur Erstellung

### iX-TRACT

- Auch für „die Kleinen“ (Blogger, Vereine, Freelancer und Kleinstunternehmen) gelten die neuen Datenschutzbestimmungen der DSGVO.
- Für Websitebetreiber, die auf WordPress setzen, gibt es eine Reihe von Stellschrauben, mit denen sich das CMS DSGVO-konform betreiben lässt.
- Ein „Rundum-sorglos-Plug-in“, das hundertprozentigen Schutz vor Abmahnungen oder Bußgeldern bietet, gibt es nicht.

zahlreicher Content-Formate von der Portfolioseite bis hin zum Webshop genutzt. Entsprechend groß ist die Zahl der verfügbaren Themes (Designs) und Plug-ins (funktionalen Erweiterungen). Für eine Bewertung möglicher DSGVO-Risiken müssen Webseitenbetreiber daher zwischen dem Core-WordPress-System und optionalen Add-ons und Drittanbieterdiensten unterscheiden.

Grundsätzlich sind zwei Punkte potenziell heikel: die Speicherung personenbezogener Daten sowie die Übertragung derselben an Dritte. Letzteres passiert zum Beispiel, wenn Webmaster das beliebte Analyse-Tool Google Analytics einsetzen, aber auch, wenn sie Inhalte von Plattformen wie YouTube in ihre Seiten einbetten.

Das Entwicklerteam von WordPress begann erst wenige Wochen vor dem 25. Mai damit, DSGVO-Werkzeuge in die Software zu integrieren. Eine Roadmap für die Implementierung findet sich auf GitHub. Der Großteil der angedachten Features ist jedoch in der Anfang August freigegebenen Version 4.9.8 bereits enthalten. So findet man im aktuellen WordPress zwei neue Tools zum Exportieren und Löschen personenbezogener Daten (unter „Werkzeuge“) sowie ein neues Untermenü mit der Bezeichnung „Datenschutz“ unter „Einstellungen“.

Auf dieser Einstellungsseite wählt der Webmaster die Seite mit den Informationen zur Datenschutzerklärung aus. Ein Leitfaden mit kommentierten Textvorschlägen hilft auch Neulingen bei der Erstellung einer DSGVO-konformen Erklärung. Die Hersteller von Plug-ins können über den neuen Privacy-Layer optional eigene Datenschutzbeschreibungen ihrer Software hinzufügen.

## Rechtlicher Stolperstein Nutzerkommentare

Neu in WordPress ist zudem eine Checkbox für die Kommentarfunktion. Sie fragt ab, ob die Daten des Nutzers (E-Mail-Adresse, Name und gegebenenfalls die URL seiner Webseite) bis zum nächsten Kommentar in einem Cookie gespeichert werden sollen.

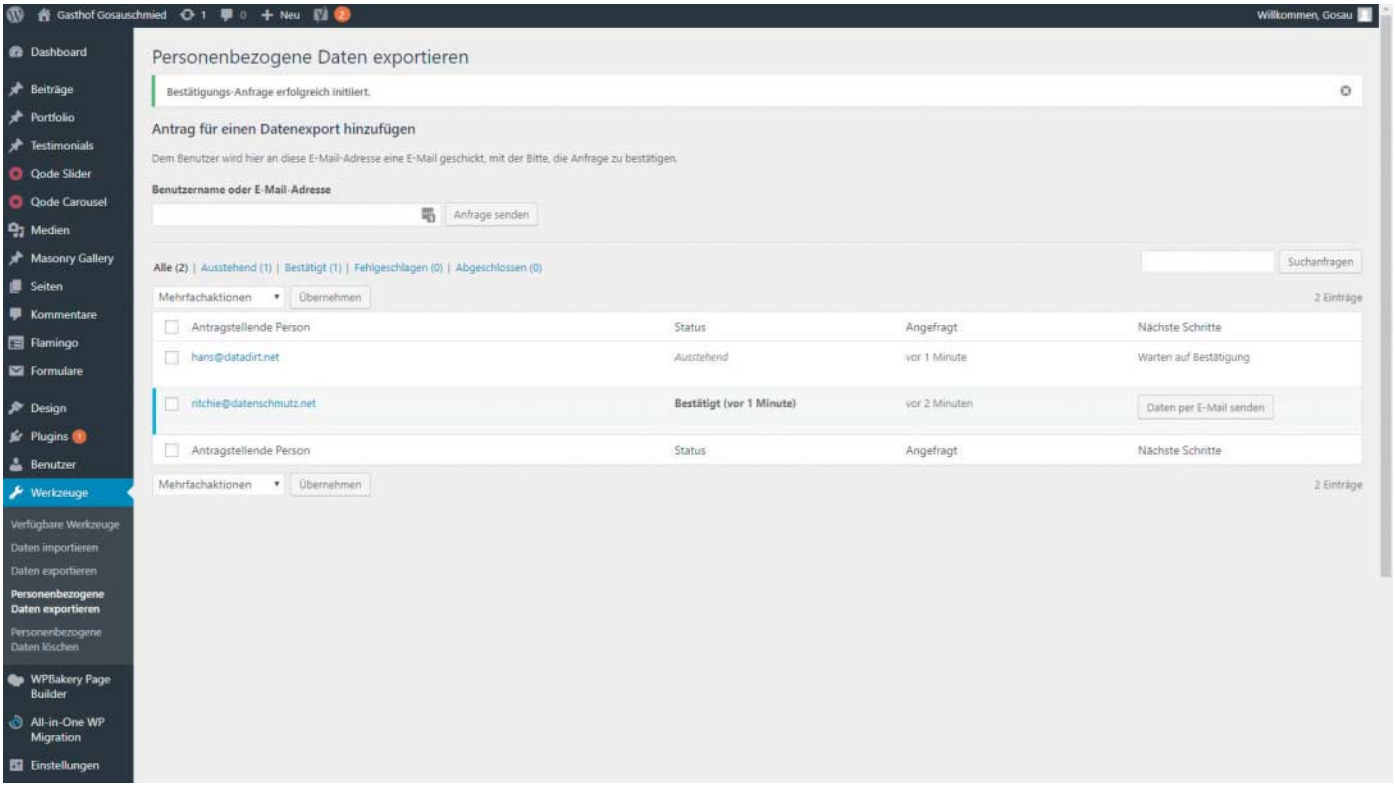
Da sich WordPress in den Standardeinstellungen neben den eingetragenen Kommentardaten auch Zeitstempel und IP-Adresse merkt, besteht auch hier Handlungsbedarf. Als personenbezogenes Datum darf Letztere nur dann gespeichert werden, wenn es unbedingt erforderlich ist.

An der praktischen Auslegung scheiden sich die Geister: Besonders Vorsichtige empfehlen, die Speicherung der IP-Adressen generell zu deaktivieren. Das lässt sich entweder mittels Plug-in oder über eine Anpassung der *functions.php* lösen. Andererseits kann die IP-Adresse bei einem möglichen Rechtsverstoß wesentliche Anhaltspunkte für eine allfällige Strafverfolgung bieten.

Ein Mittelweg besteht darin, die Adressen zwar zuerst zu speichern, dann jedoch nach Ablauf eines definierten Zeitraums automatisch aus der Datenbank zu entfernen. Realisieren lässt sich ein solches Vorgehen mit einem Cronjob-gesteuerten MySQL-Skript.

In jedem Fall jedoch sollte der Webseitenbetreiber IP-Adressen aus der Vergangenheit löschen. Das funktioniert am einfachsten direkt über die Datenbank: WordPress speichert sie in der Tabelle „wp-comments“ in der Spalte „comment_author_IP“. Die Löschung der Daten hat keinerlei Auswirkung auf die Funktionalität der Seite.

Mit der Entsorgung der IP-Adressen ist es allerdings noch nicht getan. WordPress reichert Kommentare optional mit Gravatar-Bildern an. Das sind Avatare, die der Nutzer auf gravatar.com, einem von Automattic, dem Unternehmen hinter WordPress, betriebenen Service, für seine E-Mail-Adresse hinterlegen kann. Schreibt jemand einen neuen Kommentar, schickt WordPress die zugehörige




**Bei den in WordPress integrierten Export- und Löschtools muss ein Admin den Vorgang anstoßen. Ein Shortcode für das Frontend ist derzeit nicht verfügbar (Abb. 1).**

gehashte E-Mail-Adresse zum Gravatar-Service, um zu überprüfen, ob ein Bild vorhanden ist.

Die Gravatar-Bilder lassen sich unter „Einstellungen –> Diskussion“ komplett deaktivieren. Wer die Bilder trotzdem gerne beibehalten möchte, sollte das Plug-in Avatar Privacy installieren. Es holt die Zustimmung des Nutzers ein und cacht bereits verwendete Avatare auf dem eigenen Server.

Auch die von WordPress angebotenen Smileys und Emojis sind nicht Teil der lokalen Installation, sondern werden bei Bedarf von Automattic-Servern abgerufen. Auch hier hat der Webmaster die Wahl: Entweder er deaktiviert diese Funktion komplett oder er ersetzt die Bildchen durch lokale Versionen. Ersteres lässt sich elegant mit Clearfy bewerkstelligen. Das kostenlose Plug-in vereint eine ganz Reihe von System- und Performance-Tweaks unter einer gemeinsamen Oberfläche. Wer auf die Emojis nicht verzichten möchte, kann sie per Plug-in auch vom eigenen Server laden lassen.

Nach wie vor umstritten unter Juristen ist jene Checkbox, die vom Nutzer vor dem Verfassen eines Kommentars explizit die Zustimmung zur Datenspeicherung fordert. Wer eine solche einbauen möchte, kann dafür das Plug-in WP GDPR verwenden.

Unbedingt deaktivieren und löschen sollte man WordPress’ integrierten Spamschutz Akismet. Der funktioniert zwar einwandfrei, überträgt aber ebenfalls Kommentarinhalte und IP-Adressen an Automattic-Server. Genauso zuverlässig, aber datenschutzkonform arbeitet Anti-Spam Bee. In der aktuellen Version kann man sogar die Option „Kommentare aus bestimmten Ländern blockieren oder zulassen“ aktiviert lassen, denn das Plug-in anonymisiert die IP-Adresse vor der Übertragung an den Dienst IP2Country.

## Gesprächige Google-Tools und eingebettete Inhalte

Webmaster schätzen Googles kostenloses Analyse-Tool. Vergleichbare Lösungen bieten entweder deutlich weniger Funktionen, sprengen das Budget von KMUs und Bloggern oder erfordern umfangreiches Expertenwissen. Man kann Google Analytics DSGVO-konform einsetzen, muss jedoch einige Punkte beachten. Wirklich neu sind diese allerdings nicht. Sie waren bereits vor Inkrafttreten der DSGVO Pflicht.

So müssen IP-Adressen vor der Übertragung auf Googles Server anonymisiert werden, erweiterte Tracking-Funktionen dürfen nicht genutzt werden und der Webmaster muss einen Datenverarbeitungsvertrag mit Google abschließen. Auch muss dem Besucher eine Opt-out-Möglichkeit angeboten werden. Das geschieht wahlweise per Cookie oder mithilfe von Browsererweiterungen. Die Hinweise darauf gehören in die Datenschutzerklärung, für die technische Umsetzung empfiehlt sich das Plug-in GA Opt-Out.

Die meisten modernen WordPress-Themes binden Googles frei verfügbare Webfonts und Maps ein. Beim Aufruf der betreffenden Seiten wird die IP-Adresse an Googles Server weitergeleitet. Ob man bei der Einbindung dieser Dienste „berechtigtes Interesse“ anführen kann, bleibt unter Juristen umstritten. Wer Googles Maps oder Fonts in seine Seiten einbindet, sollte auf jeden Fall seine Datenschutzerklärung um entsprechende Abschnitte ergänzen.

Zumindest die Fonts lassen sich alternativ auch auf dem eigenen Server ablegen. Das Vorgehen unterscheidet sich dabei je nach Theme. Das populäre Enfold Framework etwa bietet seit Mitte Mai die Möglichkeit, die gewünschten Schriftarten direkt über die Theme-Optionen hochzuladen. Bei anderen Themes sind häufig händische Anpassungen am Stylesheet erforderlich. Eine dritte Option ist eine Deaktivierung der Google-Fonts über das bereits genannte Plug-in Clearfy. Allerdings bleibt dann die Typografie der eigenen Website auf die wenigen Fallback-Standardschriften beschränkt.

Bei Google Maps untersagen Googles AGB leider das lokale Hosting eines Screenshots. Als Alternativen bieten sich entweder die Lizenzierung von einem Fachverlag oder der Rückgriff auf das kostenlose OpenStreetMap an.

## YouTube, SlideShare, SoundCloud und Co.

Auch bei der Einbindung von Drittinhalten, also Videos, Audio-Dateien, SlideShare-Präsentationen und anderen Embeds, sollten Webmaster Vorsicht walten lassen. Was immer an Inhalten von Drittservern geladen wird, birgt ein DSGVO-Risiko.

Videos könnte man gegebenenfalls selbst hosten, Tweets ließen sich auch als Screenshots einbinden – aber so richtig elegant ist das alles nicht. In der Praxis haben sich zwei Vorgangsweisen herauskristallisiert: Vorsichtige Webseitenbetreiber verwenden ein Opt-in-Plug-in, das vor dem Laden der Inhalte auf die Datenübertragung hinweist und die Zustimmung des Nutzers einholt. Borlabs Cookie bietet dafür zum Beispiel eine entsprechende iFrame-Container-Funktion. Risikofreudigere Naturen binden Drittinhalte ein wie bisher und argumentieren in ihrer DSE mit „berechtigtem Interesse“. Wer regelmäßig Tweets, Instagram- und Facebook-Postings einbindet, kann alternativ auch auf Plug-ins mit integriertem Caching zurückgreifen. Weiterführende Infos dazu finden sich unter ix.de/ix1809052.

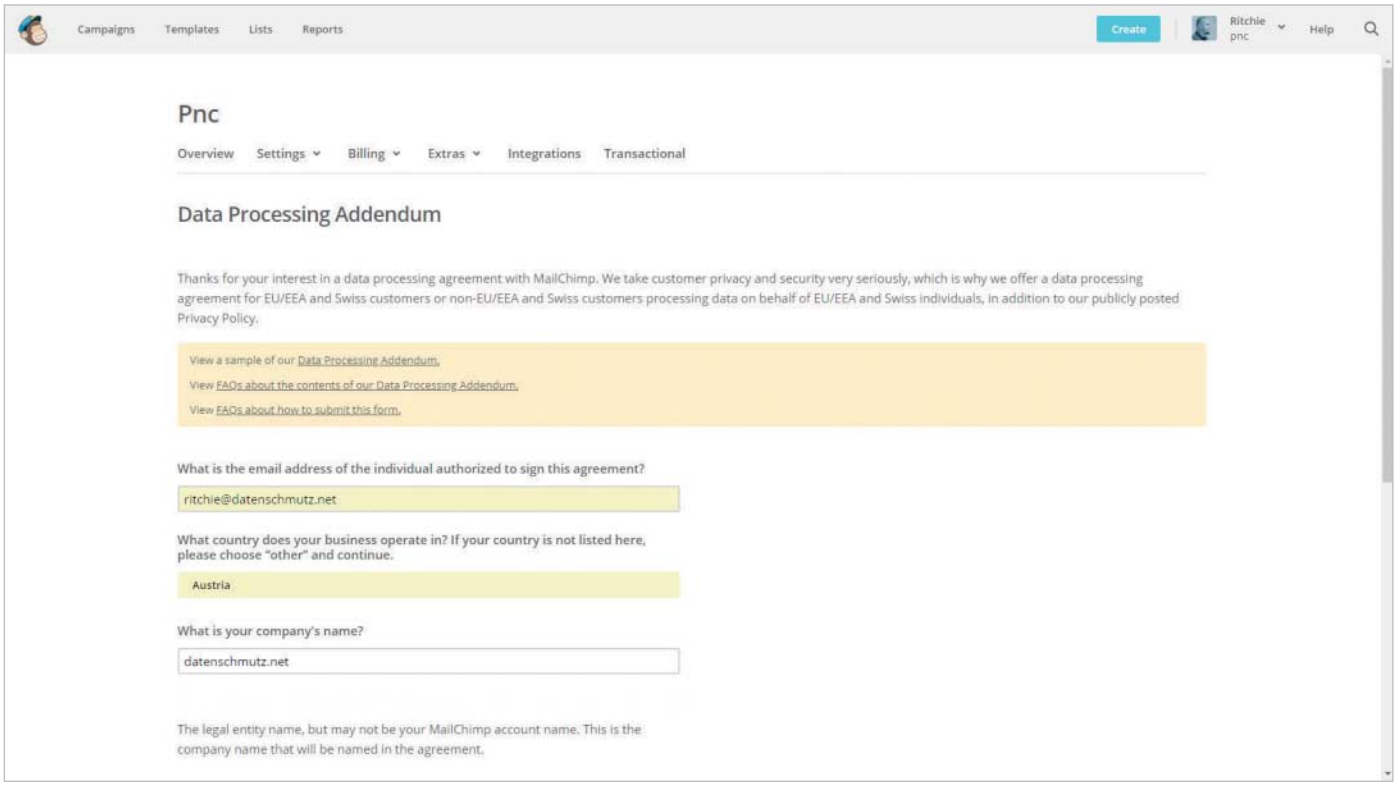
## Webhoster und Plug-ins

Wer seine WordPress-Seite auf einem Shared Hosting Space oder einem Managed Server betreibt, wird in der Regel eine Datenverarbeitungsvereinbarung mit seinem Hoster benötigen – denn der hat ja zumindest theoretisch Zugriff auf die Serverlogs samt gespeicherten IP-Adressen. Alle großen Provider bieten in ihrer Verwaltungsoberfläche mittlerweile solche DVVs an. Je nach Serverkonfiguration achten penible Webmaster darauf, die Serverlogs entweder ganz zu deaktivieren (nicht optimal für Fehlersuche und Monitoring), sie regelmäßig zu anonymisieren oder sie nach einer bestimmten Zeit automatisch zu löschen.

Ob ein Plug-in möglicherweise einen GDPR-Verstoß verursacht, lässt sich von außen gar nicht so leicht beurteilen. Bei Social-Sharing-Buttons kommt es ganz darauf an, wie die Programmierer die jeweiligen Funktionen umgesetzt haben: Greift ein Plug-in bereits beim Aufruf der Seite auf die APIs von Facebook und Co. zu, etwa um in Echtzeit Counter anzuzeigen, müsste der Nutzer eigentlich vorher zustimmen. In vielen Fällen lassen sich solche Funktionen auch auf datensparsameren Wegen umsetzen. So steht mit dem „Shariff Wrapper“, einem Nachfolgeprojekt des von der c’t entwickelten Plug-ins Shariff, eine hundertprozentig DSGVO-konforme und sehr flexibel konfigurierbare Sharing-Lösung zur Verfügung.

In manchen Fällen ist es prinzipbedingt schlicht unmöglich, ganz auf die Datenübertragung zum Anbieter zu verzichten. So erkennt das populäre Sicherheits-Plug-in Wordfence IP-Floods und andere Angriffe durch den Abgleich von IP-Adressen mit hauseigenen Blacklists. Wordfence hat jedoch wie die meisten großen Anbieter ein umfangreiches GDPR-Portal aufgebaut und bietet auch Nutzern der kostenlosen Version den Abschluss eines Datenverarbeitungsvertrags an. Die Abwägung zwischen Datensparsamkeit und berechtigtem Interesse obliegt also kurz gesagt letztendlich in jedem einzelnen Fall dem Webmaster selbst. Dem Argument des sicheren und ungestörten Betriebs einer Webseite wird aber voraussichtlich kein Richter widersprechen.

Auch andere große Anbieter wie Mailchimp haben sich auf die neuen Datenschutz-Spielregeln der EU vorbereitet. Generell gilt beim Einsatz von Formularen und Formular-Plug-ins, dass eine Zustimmung zur Datenspeicherung via standardmäßig deaktivierter Checkbox eingeholt werden sollte. Dabei sind unterschiedliche Szenarien möglich: Je nach Konfiguration schicken Formular-Plug-ins die Nutzerdaten per E-Mail an den Admin, sodass sie auf dessen Mailserver gespeichert werden, oder sie landen in der WordPress-Datenbank. Das Vorgehen muss in der DSE beschrieben und erklärt werden. Im Zweifelsfall hilft ein Blick in Blogmojos




**Fast alle großen Anbieter haben für ihre Kunden aus der EU DSGVO-Portale eingerichtet und stellen Datenverarbeitungsverträge zur Verfügung (Abb. 2).**

laufend aktualisierte Liste zur DSGVO-Kompatibilität von über 200 populären WordPress-Plug-ins.

## Jemand noch einen Keks?

Parallel zu den Bemühungen des Core-Teams haben auch verschiedene Entwickler GDPR-Plug-ins auf den Markt gebracht, die teils den irreführenden Eindruck erwecken, mit nur einem Klick alle Probleme zu lösen. Seit dem letzten WordPress-Update können diese Erweiterungen sogar kontraproduktiv sein und Funktionen, die WordPress ohnehin enthält, unnötig verdoppeln. Empfehlenswert sind das Plug-in GDPR und Co. vor allem für umfangreiche Membership-Seiten.

Der sogenannte „Cookie-Hinweis“ wird gern mit den erwähnten DSGVO-Maßnahmen in einen Topf geworfen. Tatsächlich handelt sich dabei um eine gänzlich andere Baustelle. Deutschland hat die Cookie-Richtlinie der EU nie in nationales Recht umgesetzt. Hierzulande gilt nach wie vor § 15 Abs. 3 des Telemediengesetzes. Dieses fordert, den Nutzer ausreichend zu unterrichten und auf sein Widerspruchsrecht hinzuweisen. Beides kann durch einen Cookie-Hinweis erfolgen, rechtlich erforderlich ist dieser zurzeit aber nicht. Das ändert sich voraussichtlich erst mit der ePrivacy-Richtlinie im kommenden Jahr. Sie verlangt ein explizites Opt-in des Webseitenbesuchers vor dem Setzen von Cookies.

Anders verhält es sich mit dem Einsatz sogenannter Retargeting-Systeme: Wer das Facebook-Pixel oder Retargeting-Cookies von AdSense und Co. verwendet, die IP-Adressen übertragen und speichern, ist mit einem expliziten Opt-in, wie es zum Beispiel Borlabs Cookie anbietet, auf der sicheren Seite.

## Fazit

Zusammenfassend lässt sich über die DSGVO und WordPress vor allem eines sagen: Wenn sich die Fachjuristen in vielen Detailfragen ausgesprochen uneinig sind, bleibt dem ambitionierten Blogger oder Kleinunternehmer mit Website nur ein pragmatischer Ansatz: Eine hundertprozentige DSGVO-Komformität kann zum derzeitigen Wissensstand niemand garantieren. Wer jedoch die in diesem Artikel genannten Tipps umsetzt, verringert das Risiko von Beschwerden um mehrere Größenordnungen. Die entsprechenden Eintragungen in das vorgeschriebene Datenverarbeitungsverzeichnis sollten dann auch keine Schwierigkeiten mehr bereiten.

Bei all dem Aufwand, den der Betrieb einer DSGVO-konformen WordPress-Website verursacht, darf man nicht vergessen: Besserer Datenschutz hat seinen Preis. Und wenn erst die DSGVO den einen oder anderen Webmaster dazu zwingt, sich damit auseinanderzusetzen, wohin seine Webseite welche Besucherdaten schickt, dann ist das gewiss kein Nachteil. (akl@ix.de)

**Ritchie Pettauer**

ist Online-Strategie-Berater und Lektor am Institut für Publizistik- und Kommunikationswissenschaft der Uni Wien.

Alle Links: ix.de/ix1809052