

# Richtlinien und Empfehlungen zur Datenschutzgrundverordnung (DSGVO) für freie Reisejournalisten, Online-Publizisten und Blogger

Eine Initiative des Journalisten-Kreises der VDRJ,  
zusammengestellt von Franz Neumeier

Stand: 31. Mai 2018

*Wichtiger Hinweis: Dieses Dokument ersetzt keine Rechtsberatung im Einzelfall, sondern bietet lediglich soweit möglich einen Überblick über die in Deutschland geltenden datenschutzrechtlichen Regelungen zum Stand der Erstellung. Die Anwendung dieser Regeln ist aber von Fall zu Fall verschieden. Das Dokument erhebt keinen Anspruch auf Vollständigkeit.*

*Zudem gibt es selbst bei Experten Fragezeichen, wie die Rechtsprechung die DSGVO interpretiert und die verschiedenen Rechte und Pflichten tatsächlich umzusetzen sind. Es kann also jederzeit Veränderungen geben.*

Die Datenschutzgrundverordnung (DSGVO) sorgt für viel Aufregung. Niemand – auch Fachjuristen nicht – hat Antworten auf viele Aspekte der Verordnung, die bereits am 25. Mai 2016 in Kraft getreten ist und nach einer Übergangszeit nun seit 25. Mai 2018 tatsächlich zur Anwendung kommt. Als VDRJ können wir deshalb dieses Problem auch nicht abschließend lösen – aber mit dieser Zusammenfassung ein wenig Ordnung in das Durcheinander bringen.

Mit grob irreführenden Informationen macht so mancher profitgieriger Anwalt Werbung für sein eigenes Business und sorgt für noch mehr Verwirrung, als die DSGVO ohnehin schon auslöst. Dieser Beitrag soll eine konkrete Hilfestellung für freie Reisejournalisten liefern, das Thema DSGVO mit möglichst wenig Zeitaufwand abzuwickeln: mit einigen grundlegenden Informationen zur DSGVO selbst, sowie mit Links zu guten Fachbeiträgen, Mustertext-Generatoren und Ähnlichem.

Wichtiger Hinweis: Dieses Dokument ist keine Rechtsberatung und ersetzt erst Recht keine Rechtsberatung im jeweiligen Einzelfall. Vielmehr enthält es vor allem pragmatische Hilfestellungen, die teils sogar bewusst nicht den Buchstaben des Gesetzes folgen, sondern mit gesundem Menschenverstand auf die Realisierbarkeit im Alltag schauen. Die Tipps sollen außerdem helfen, eventuelle Risiken in Zusammenhang mit datenschutzrechtlichen Vorschriften zu reduzieren. Das Dokument erhebt keinen Anspruch auf Vollständigkeit.

## Anmerkungen zur Einordnung und Bedeutung der DSGVO

Am wichtigsten: nicht irre machen lassen von juristischem Absolutismus. Juristen schreiben meist nur das, was dem Gesetz nach vorgeschrieben ist. Pragmatisch kann man aber vieles davon (mit schlechtem Gewissen, aber ohne Folgen) erst einmal hinten anstellen.

Wer ist nicht schonmal bei Tempo 130 auf der Autobahn trotzdem 150 gefahren? Und? Sind Sie dabei hysterisch geworden und haben ernsthaft darüber nachgedacht, ihr Auto sofort zu verschrotten? Natürlich nicht. Warum also sollte man bei der DSGVO gegen jeden gesunden Menschenverstand plötzlich alles wortwörtlich befolgen, obwohl man das in seinem restlichen Leben nicht tut? Weil hohe Strafen drohen? Siehe den Abschnitt zum Thema „Folgen“ – dann relativiert sich dieser Aspekt erheblich.

Vieles, was jetzt im Rahmen der DSGVO diskutiert wird, galt eigentlich auch schon lange vor der DSGVO – es hat nur niemand wahrgenommen oder zumindest nicht ernstgenommen.

Die DSGVO führt uns all diese Dinge jetzt nur deutlich vor Augen. In Deutschland ändert sich sogar besonders wenig, denn die Regelungen der DSGVO basieren in weiten Teilen auf dem bisherigen deutschen Datenschutzrecht.

## Rechtsgrundlagen – mehr als eine einzelne Verordnung

Die Datenschutzgrundverordnung (DSGVO) ist eine EU-Verordnung und damit (anders als Richtlinien) direkt geltendes Recht. In englischsprachigen Texten heißt die DSGVO übrigens General Data Protection Regulation (GDPR). Die DSGVO gilt nicht für ausschließlich private Datenverarbeitung, also beispielsweise im Freundeskreis oder in der Familie. Nicht ganz klar ist, ob das auch gilt, wenn Privatleute personenbezogene Daten beispielsweise bei Facebook veröffentlicht werden.

Aber schon bei einem Blog, das auch nur einen einzigen Affiliate-Link, einen Werbebanner oder einen Sponsored Post enthält, kann man nicht mehr von „privat“ ausgehen. Bloggt ein freier Reisejournalist zu Reisetemen, wird wohl auch dann die Datenschutzvorschriften einhalten müssen, wenn er das Blog selbst in keiner Weise kommerzialisiert. Denn es steht wohl in Zusammenhang mit seiner beruflichen Tätigkeit und ist damit zumindest eine Art Werbung für seine berufliche Tätigkeit und hat damit kommerzielle Ziele. Im Zweifel sollte man also besser davon ausgehen, dass die DSGVO anwendbar ist. Deshalb gilt auch die Impressumspflicht gemäß §13 TMG (Telemediengesetz) und §5 RStV (Rundfunkstaatsvertrag).

Neben der DSGVO gibt es weitere Gesetze: das neue Bundesdatenschutzgesetz (<https://dsgvo-gesetz.de/bdsg-neu/>), oft „BDSG-neu“ oder „BDSG 2018“ genannt, weil es den gleichen Titel wie das Vorgängergesetz BDSG trägt. Außerdem gelten neue Landesdatenschutzgesetze, in Bayern beispielsweise das Bayerische Datenschutzgesetz BayDSG ([http://www.gesetze-bayern.de/Content/Document/BayDSG 9](http://www.gesetze-bayern.de/Content/Document/BayDSG_9)). Diese Gesetze konkretisieren einige Regeln der DSGVO beziehungsweise regeln die Durchführung.

Was gerne übersehen wird: Datenschutz-Recht ist in Deutschland auch in zahllosen weiteren Gesetzen enthalten und schafft in vielen Fällen Ausnahmen oder Konkretisierungen der DSGVO. Das ist beispielsweise auch das jeweilige Landespressegesetz. In solchen Spezialgesetzen findet sich beispielsweise auch die Präzisierung des in der DSGVO

vorgesehenen Medienprivilegs, das die Presse von bestimmten Auskunftspflichten im Datenschutz ausnimmt oder weitere Argumente liefert, „berechtigtes Interesse“ an der Verarbeitung von Daten zu begründen.

Wichtig zu verstehen: Spezialgesetze gehen in der Regel vor. Gibt es also ein Gesetz, in dem sehr konkret definiert wird, wie in einer bestimmten Situation mit Datenschutzaspekten umgegangen werden muss, kann man erst einmal davon ausgehen, dass das so auch gilt – selbst wenn die DSGVO in diesem Aspekt anders klingt. Möglicherweise kippt der EuGH dieses nationale Gesetz dann irgendwann, aber bis dahin kann man sich darauf erst einmal halbwegs verlassen. Relevant ist das beispielsweise beim in den Landespressegesetzen teils konkretisierten Medienprivileg oder bei den Regelungen des Kunsturhebergesetzes.

## **ePrivacy-Verordnung**

Und noch ein wichtiger Punkt: die so genannte ePrivacy-Verordnung, die gelegentlich angesprochen wird – und die Dinge vor allem für Websitebetreiber und Blogger möglicherweise wirklich schwierig macht – wird voraussichtlich erst Ende 2019 in Kraft treten und wie die DSGVO eine Übergangsfrist für die tatsächliche Anwendbarkeit haben. Sie dürfte also erst Ende 2020 tatsächlich relevant werden. Insofern ist es aktuell weitgehend sinnlos, darüber zu spekulieren und vorsorglich schonmal Aspekte zu berücksichtigen, die in dieser Verordnung vielleicht enthalten sein könnten.

## **Welche Gefahren drohen?**

Die DSGVO wirkt auf den ersten Blick verwirrend, überwältigend, nicht umsetzbar. Tatsächlich sind sich auch Fachjuristen in vielen Aspekten alles andere als sicher oder einig, wie die DSGVO genau umzusetzen ist und was man genau tun muss, um auf der sicheren Seite zu sein. Andererseits propagieren die Profiteure dieses Durcheinanders, dass immense Strafen drohen, wenn man sich nicht exakt an die DSGVO hält.

Doch so schlimm ist es in der Realität längst nicht. Weil eben auch Juristen sich nicht einig sind – einschließlich der Datenschutzbeauftragten, die genauso von der Rechtsunsicherheit betroffen sind wie diejenigen, die die DSGVO umsetzen müssen.

Rechtssicherheit wird in den unklaren Aspekten erst über die Jahre entstehen, wenn der Europäische Gerichtshof (EuGH) einige grundlegende Dinge geklärt hat. Bis dahin ist die Rechtslage zwar unklar, was aber gerade für freie Journalisten und Blogger durchaus auch ein Vorteil sein kann, wie ich gleich erklären werde.

## **Bußgelder und Abmahnungen**

Grundsätzlich drohen bei Verstößen gegen die DSGVO Bußgelder, die von Datenschutz-Aufsichtsbehörden verhängt werden können. Daneben könnte es Abmahnungen von Konkurrenten im Rahmen des Wettbewerbsrechts geben.

Aber: Aufsichtsbehörden haben besseres zu tun, als sich mit Bloggern und freien Journalisten zu beschäftigen, schon weil deren Personal dafür gar nicht ausreicht. Deren Ziel ist es, die

„großen Fische“ zu fangen: große Unternehmen, die absichtlich gegen Datenschutzbestimmungen verstoßen und europäisches Datenschutzrecht mit Füßen treten.

Und ebenfalls aber: Abmahner werden sich tendenziell eher auf einfache Ziele stürzen, also auf Unternehmen, die eklatant und offensichtlich gegen die DSGVO verstoßen. Denn wer abmahnt, muss damit rechnen, dass die Angelegenheit vor Gericht landet und da will man sich halbwegs sicher sein, dass man auch gewinnt, um nicht auf den Prozess- und Anwaltskosten sitzen zu bleiben. Eine Abmahnung wird sich also eher nicht mit den eher schwammigen und unklaren Aspekten der DSGVO beschäftigen.

Ein Abmahner müsste sich seiner Sache auch sehr sicher sein, dass zum Beispiel seine eigene Website absolut DSGVO-konform ist, um sich nicht dem Risiko einer Gegenabmahnung auszusetzen.

Ohnehin dürfte das Thema „Abmahnung“ nur für Websitebetreiber und Blogger überhaupt relevant sein, denn für die sonstige Tätigkeit eines freien Journalisten gibt es kaum Ansatzpunkte für eine Abmahnung.

Das ist weder bei den Bußgeldern noch bei den Abmahnungen eine Garantie, aber doch eine hohe Wahrscheinlichkeit.

Eine durchaus relevante, juristische Sichtweise ist übrigens, dass Abmahnungen aufgrund eines Verstoßes gegen die DSGVO vielleicht überhaupt nicht möglich sind (<http://www.rechtzweinnull.de/archives/2579-abmahnwellen-wegen-dsgvo-verstoessen-dagegen-spricht-und-wie-man-abmahnungen-gegebenenfalls-abwehren-kann.html>). Ob das allerdings auch die Gerichte und letztlich der EuGH so sehen, muss sich aber erst noch zeigen. Auch das ist aber ein erhebliches Risiko für Abmahnanwälte.

## **Erlaubt oder verboten?**

Die DSGVO – wie auch schon zuvor das deutsche Datenschutzrecht – hat ein Grundprinzip, das das Verständnis der Regelungen sehr vereinfacht: Alles, was nicht ausdrücklich erlaubt ist, ist verboten. Steht im Gesetz also nichts, ist eine entsprechende Datenverarbeitung erst einmal nicht erlaubt. Aber ...

Letztlich erlaubt das Gesetz dann doch sehr viel. Verarbeitet werden dürfen Daten, die

- zur Vertragserfüllung dienen oder für vorvertragliche Maßnahmen (also beispielsweise E-Mail-Adresse eines Users, der mit dem Blogger Kontakt aufnimmt; „Vertrag“ muss nicht unbedingt ein Kaufvertrag in einem Shop sein, sondern kann auch z.B. ein Vertrag zur Zusendung eines Newsletters sein; oder die Diskussion eines Angebots an eine Zeitung für eine Reportage)
- lebenswichtige Interessen des Betroffenen schützen
- in öffentlichem Interesse sind (das hilft vor allem Behörden)
- aufgrund einer Interessen-Abwägung verarbeitet dürfen (bei „berechtigtem Interesse“ – das ist der weitaus wichtigste Aspekt)
- auf Basis einer ausdrücklichen Einwilligung des Betroffenen verarbeitet werden.

Um die Verordnung wirklich zu verstehen, muss man also vor allem unterscheiden zwischen „informieren“ und „Einwilligung“. Ist etwas erlaubt, muss ich in der Datenschutzerklärung lediglich (ausführlich und in klar verständlicher Sprache) informieren – soweit das Medienprivileg einen als Journalisten davon nicht entbindet. Es schadet dennoch nicht, explizit auf diese Entbindung auf Basis des Medienprivilegs hinzuweisen.

Nur wenn etwas nicht erlaubt ist, benötigt man eine explizite Zustimmung der Betroffenen, dessen Daten verarbeitet werden sollen.

Den größten Spielraum lässt die Verarbeitung bei „berechtigtem Interesse“: Hier geht es darum abzuwägen, ob mögliche Schutzrechte (etwa Persönlichkeitsrechte) wichtiger sind als das Interesse desjenigen, der die Daten verarbeitet.

„Berechtigtes Interesse“ ist ein umfangreiches Themenfeld, deshalb seien hier nur ein paar Beispiele fürs Verständnis genannt, was ein berechtigtes Interesse für den Betrieb eines Blogs sein kann (aber immer im Einzelfall individuell geprüft und begründet werden muss!):

- Abwehr von Gefahren, beispielsweise von Online-Betrug oder Hacker-Angriffen
- Ordnungsgemäßer Betrieb der Website (z.B. vorübergehende Speicherung der IP-Adresse)
- geschäftliche Interessen wie die Erhebung von Traffic-Statistiken
- technisch unkomplizierte Einbindung von Videos (z.B. Youtube, weil selbst gehostetes Video wirtschaftlich sehr aufwändig wäre)

Entscheidend ist, dass das berechtigte Interesse mit Interessen der Betroffenen jeweils im konkreten Fall abgewogen und begründet wird.

## **Medienprivileg**

Artikel 85 der DSGVO erlaubt es den einzelnen Mitgliedsstaaten der EU (Öffnungsklausel), die Regelungen mit der Freiheit der Meinungsäußerung und Informationsfreiheit in Einklang zu bringen. In Deutschland geschieht dies beispielsweise im Bayerischen Datenschutzgesetz in Art. 38 (<http://www.gesetze-bayern.de/Content/Document/BayDSG-38>) oder im bayerischen Staatsvertrag für Rundfunk und Telemedien in §57.

Im Grund ändert sich hier also erst einmal fast nichts. Denn dieses „Medienprivileg“ befreit Journalisten von Teilen der DSGVO, um Presse- und Meinungsfreiheit sicherzustellen, weil beispielsweise ein Auskunfts- oder gar Löschungsanspruch von personenbezogenen Daten bei investigativen Recherchen jede Recherche zunichtemachen würde. Dennoch gilt aber beispielsweise die Verpflichtung zur Sicherung von Daten vor fremdem Zugriff und Ähnliches.

## **Zweckbindung**

Ebenso wichtig: Die verarbeiteten Daten dürfen nur zu dem ursprünglich vorgesehenen und genannten Zweck verwendet werden. Einmal legal erhobene Daten dürfen also nachträglich nicht frei für alles verwendet werden, sondern sind zweckgebunden. Insbesondere auch unter Anwendung des Medienprivilegs verarbeitete/gespeicherte Daten dürfen also ebenfalls nicht für andere Zwecke genutzt werden.

Personenbezogene Daten müssen außerdem gelöscht werden, wenn der ursprüngliche Verarbeitungszweck entfällt. Das ist insbesondere in Hinblick auf E-Mail-Verkehr und darin enthaltene, personenbezogene Daten ein bislang kaum praktikabel lösbares Problem. Aus pragmatischer Sicht: Von außen ist nicht festzustellen, wie, ob und wo E-Mails gespeichert werden. Insofern gibt es auch kaum einen Angriffspunkt, deswegen in Schwierigkeiten zu geraten. Das gibt zeitlichen Spielraum um abzuwarten, welche Lösungen sich in der Praxis oder über die Rechtsprechung hierfür ergeben.

## Was sind personenbezogene Daten?

Die DSGVO beschäftigt sich mit der Verarbeitung von personenbezogenen Daten. Auslegen muss man das sehr weit. Personenbezogen sind Daten nämlich auch dann schon, wenn sie sich irgendwie mit einer natürlichen Person in Verbindung bringen lassen. Das bezieht sich also auch auf Daten, die erst einmal nicht persönlich erscheinen wie ein Foto, eine IP-Adresse oder ein anonymes Cookie.

Lassen sich solche Daten aber nachträglich irgendwie mit einer Person in Verbindung bringen, muss man sie als personenbezogen betrachten. Das kann beispielsweise ein Verfahren zur Gesichtserkennung bei Fotos sein, oder die Kombination von verschiedenen Datensätzen, um beispielsweise eine IP-Adresse mit einer Person in Verbindung zu bringen. Oder eben ein anonymes Cookie, der durch das Einloggen auf einer bestimmten Website (Facebook, Amazon, Google etc.) plötzlich eben nicht mehr anonym ist.

Wichtig zu wissen: Es geht in der DSGVO um Daten in strukturierter Form ("Dateisystem"). Was ein Journalist also in seinem Notizblock aufschreibt, als ungeordnete Zettelsammlung im Schuhkarton ablegt oder im Gedächtnis speichert, bleibt davon unberührt. Sobald Daten aber systematisch beispielsweise in einem Aktenordner abgeheftet werden, handelt es sich dabei bereits ein Dateisystem (Erwägungsgrund 15 zum Art. 4, Nr. 6: <https://dsgvo-gesetz.de/erwaegungsgruende/nr-15/>).

## Melde- und Dokumentationspflichten

Ein kompliziertes und vor auf große Unternehmen zielender Aspekt sind Dokumentationspflichten in Hinblick auf die Verarbeitung von Daten und die Meldepflichten bei Datenschutz-Vorfällen („Data Breach Notification“).

Dieser Leitfaden blendet diese beiden Aspekte aber zunächst einmal aus. Grund: Die ganze Dokumentation ist natürlich auch wichtig und vorgeschrieben, nach außen hin aber erst einmal nicht zu erkennen, sodass hier keine unmittelbare Gefahr besteht. Auch hier sich hoffentlich in absehbarer Zeit ein gangbarer Weg für Blogger und freie Journalisten abzeichnen, wie man damit pragmatisch und sinnvoll umgehen kann und gegebenenfalls muss. Das Thema sollte man also zumindest beobachten und zu gegebener Zeit aktiv werden.

Bei den Meldepflichten ist reichlich unklar, wie das in der Praxis funktionieren soll. Denn schon wenn man einen USB-Stick verliert, auf dem beispielsweise Adressen und Telefonnummern gespeichert sind, müsste man dies eigentlich der Datenschutzbehörde melden. Beim Verlust eines Handys ohnehin. Würde aber jeder verlorene USB-Stick

tatsächlich gemeldet, bräche bei den Datenschutzbehörden aber vermutlich Chaos aus, weil das Personal zur Bearbeitung solcher Lappalien fehlt.

Auf die leichte Schulter sollte man das Thema dennoch nicht nehmen. Denn falls der unwahrscheinliche Fall eintritt und herauskommt, dass beispielsweise ein USB-Stick mit personenbezogenen Daten abhanden gekommen ist und die Aufsichtsbehörde davon erfährt, kann es teuer werden.

Tipp: Wenn Daten verloren gehen, die so gut verschlüsselt sind, dass sie sicher nicht entschlüsselt und damit lesbar gemacht werden können, muss zwar eine Meldung an die Datenschutz-Aufsichtsbehörde erfolgen. Immerhin kann man sich in diesem Fall aber sparen, auch die Personen zu informieren, deren Daten verloren gegangen sind. Deshalb empfiehlt es sich, insbesondere personenbezogene Daten auf mobilen Datenträgern wie USB-Sticks und Smartphones immer verschlüsselt zu speichern.

## Grundsätzliches Vorgehen

Freie Journalisten, die keine eigene Website oder Blog betreiben und keinen Newsletter versenden, sind von der DSGVO nur sehr begrenzt betroffen. Dennoch sollte jeder seine Arbeitsabläufe auf datenschutzrechtlich relevante Vorgänge prüfen und gegebenenfalls anpassen.

Relevant sind Vorgänge immer dann, wenn personenbezogene Daten verarbeitet werden und dies nicht nur für private Zwecke (Familie, Freundeskreis) geschieht. Daher sollte man die eigenen Tätigkeitsbereiche daraufhin durchprüfen, ob, wo und wie man personenbezogene Daten verarbeitet.

Typischerweise verarbeitet ein freier Journalist Kontaktdaten von Ansprechpartnern bei Redaktionen, Unternehmen und PR-Agenturen sowie von Informanten, aber auch weitergehende personenbezogene Daten als Teil der Recherche-Ergebnisse, beispielsweise aus Interviews. Zu persönlichen Daten zählen auch Fotos, auf denen Menschen abgebildet sind.

Die Verarbeitung findet am PC, Laptop, Smartphone statt. Bedacht werden müssen Speichermedien Festplatten, CDs und DVDs, SD-Karten und USB-Sticks. Aber auch Cloud-Speicher wie beispielsweise Dropbox oder Google Docs. Ebenfalls zu beachten: Übertragungswege wie E-Mail, Facebook Messenger, Whatsapp und Dateitransfers via Wettransfer und ähnliche Anbieter.

Whatsapp beispielsweise kann man nicht als DSGVO-konform betrachten, weil die komplette Kontaktliste des Smartphones an die Whatsapp-Server übertragen wird.

Bei Dropbox, Google Drive und ähnlichen Diensten liegt eine Auftragsverarbeitung von Daten vor, sodass ein entsprechender Vertrag mit dem jeweiligen Anbieter geschlossen werden muss.

Grundsätzlich ist zu empfehlen, Privates von Geschäftlichem zu trennen und für geschäftliche E-Mails eine eigene Adresse zu verwenden. Denn das ist übersichtlicher und die

Datenschutzvorschriften müssen nur auf den geschäftlichen Teil angewendet werden, beispielsweise Löschung von Daten, wenn der Verarbeitungszweck entfallen ist.

Weil zum Datenschutz auch die Datensicherheit gehört, spielt für freie Journalisten ohne Website/Blog/Newsletter vor allem die Sicherheit der verarbeiteten und gespeicherten Daten die größte Rolle. Mehr Details dazu weiter unten.

## Fotos als personenbezogene Daten

Hitzig – aber zumeist unter falschen Grundannahmen – diskutiert wird die Frage, ob man nach der DSGVO künftig von jedem einzelnen Menschen, den man fotografiert, eine schriftliche Zustimmung einholen muss. Fakt ist: Menschen waren für die Kameras von Journalisten auch vor der DSGVO kein Freiwild. Persönlichkeitsrechte und das Recht am eigenen Bild gibt es schon lange. Bildjournalisten haben auch in der Vergangenheit immer die Interessen der abgebildeten Personen gegenüber dem öffentlichen Interesse an Berichterstattung abwägen müssen.

Das Bild eines bettelnden Kindes an einem Straßenrand in Manila war (ohne Einwilligung der Eltern) auch bisher schon höchst problematisch. Daran ändert die DSGVO nichts. Auch das sogenannte „Beiwerk“ auf Fotos war bisher schon eine Interessenabwägung und nicht etwa ein gesetzlicher Freibrief. Die ominöse Zahl „8“, ab der Menschen angeblich automatisch „Beiwerk“ seien, war bisher schon ein juristisch nicht haltbarer Mythos.

Nichts anders gilt in Zusammenhang mit der DSGVO, insbesondere wenn man als freier Journalist das Medienprivileg in Anspruch nehmen kann.

Sehr vernünftige und umfassend hat diese Thema ein Beitrag auf der Website „Recht am Bild“ zusammengefasst: <https://www.rechtambild.de/2018/05/fotografieren-in-zeiten-der-dsgvo-grosse-panikmache-unangebracht/>

## Strategie für freie Journalisten, Online-Publizisten und Blogger

Für Blogger und auf der eigenen Website publizierende, freie Journalisten dürfte daher eine gute Strategie sein: Alles tun, um der Einhaltung der DSGVO so nahe zu kommen wie möglich, sich aber nicht vollends verrückt machen. Und dann das Thema weiter beobachten, um Anpassungen zu machen, sobald sich Teilaspekte nach und nach klären.

Konkret sind also folgende Punkte besonders wichtig:

- Prüfen, wo und wie Daten im Rahmen der geschäftlichen Tätigkeit verarbeitet werden
- Prüfen, wo und wie Daten im Blog oder auf der Website verarbeitet werden (insbes. Plugins und Themes)
- Verträge zur Auftragsverarbeitung schließen, soweit noch nicht vorhanden (z.B. mit Google Analytics, mit dem Hosting-Provider, mit Newsletter-Dienstleistern, E-Mail-Dienstleister, Cloud-Speicherdienst etc.)
- Bei Blog/Website Datenschutzerklärung online nehmen (soweit schon vorhanden auf die Anforderungen der DSGVO anpassen)

- Bei Blog/Website Cookie-Hinweis einbauen
- Newsletter-Einwilligung einholen (soweit nicht schon geschehen und halbwegs mit den neuen Bestimmungen konform)
- Beim Einsatz von Kontakt-Formular, Newsletter-Anmeldung oder Ähnlichem: Umstellung auf SSL-Verschlüsselung – denn zum Datenschutz gehört auch eine technische Absicherung der Daten bei der Übertragung und Speicherung
- Maßnahmen zur Datensicherheit ergreifen (Backups, Verschlüsselung, etc.)

Von den Datenschutzbehörden droht zunächst einmal wenig Gefahr, sobald man sich „Mühe gibt“. Denn wie schon erwähnt, haben die Behörden erst einmal andere Sorgen, als sich um Blogs und kleinere journalistische Websites zu kümmern.

Gegen Abmahnungen kann man sich ganz gut wappnen, indem man keine offensichtlichen Angriffspunkte bietet. Alles, was nach außen hin sichtbar oder feststellbar ist, sollte man also halbwegs rechtssicher machen. Das bedeutet vor allem eine ausführliche Datenschutzerklärung, in der alle Aspekte abgehandelt werden, die von außen erkennbar sind, also Einsatz von Google Analytics, von Plugins, die Daten sammeln und Ähnlichem.

Unvermeidlich ist da einiges an Recherche, weil auch vermeintlich harmlose Plugins oder Themes datenschutzrechtlich relevant sein können. Beispiel: Lädt ein Theme Google-Fonts von den Google-Servern, werden dabei IP-Adressen der User übertragen – also Daten verarbeitet. Das ist nicht per se unzulässig, muss aber eben entsprechend in der Datenschutzerklärung behandelt werden. Juristen bewerten gerade die Google Fonts recht unterschiedlich, sodass man auf der absolut sicheren Seite ist, wenn man die Fonts lokal hostet statt von den Google-Servern einzubinden.

## Newsletter-Versand

Wer einen Newsletter versendet, musste auch bisher schon die Zustimmung der Empfänger über das Double-Opt-in-Verfahren einholen. Durch die DSGVO ändert sich daran grundsätzlich nichts. Sie stellt aber höhere Anforderungen an die Informationen, die der Newsletter-Abonnent bei seiner Einwilligung bekommen muss:

- Inhalt der Newsletter (z.B. Produkt-Informationen, Werbung, News, o.ä.)
- Hinweis auf Protokollierung der Anmeldung, ggfs. auf Erfolgsanalysen
- Hinweis auf den Zweck Erhebung von Daten, die über die notwendige E-Mail-Adresse hinaus gehen
- Hinweis auf das Widerrufsrecht
- Verweis auf die Datenschutzerklärung mit ausführlichen Informationen
- der Newsletter-Abonnent sollte aktiv über eine nicht bereits standardmäßig angewählte Checkbox der Datenverarbeitung, so dass der Newsletter-Versender diese Einwilligung auch dokumentieren kann

Waren diese Kriterien schon bisher bei der Newsletter-Anmeldung erfüllt, muss man keine erneute Zustimmung einholen. Weit verbreitet ist daher die Praxis, die Abonnenten in einer E-Mail über die geänderten Bedingungen zu informieren und in dieser E-Mail auch einen deutlich erkennbaren Link zur Abmeldung vom Newsletter anzubieten.

Absolut rechtssicher ist, wer sich die Einwilligung per Double-Opt-in neu von seinen Abonnenten holt – allerdings mit dem großen Risiko, dabei viele Abonnenten zu verlieren, die das in der Flut der DSGVO-Mails schlicht übersehen oder die Anmeldung aus Bequemlichkeit nicht erneut durchführen. Hat man ursprünglich schon eine Zustimmung per Double-Opt-in eingeholt (und dies auch protokolliert), sollte ein erneutes Double-Opt-in überflüssig sein, dann genügt auch eine einfache Zustimmung, beispielsweise durch „Ja“-Antwort auf eine entsprechend informierende E-Mail. Ein erneutes Double-Opt-in hat aber den Vorteil, dass dies klar protokolliert und nachweisbar ist, wohingegen eine Zustimmung-E-Mail leicht verloren gehen oder versehentlich gelöscht werden kann.

Dr. Thomas Schwencke hat sich mit dem Thema Newsletter auf recht pragmatische Weise beschäftigt, zwar mit Schwerpunkt auf den Dienstleister Mailchimp, aber gut übertragbar auf eigenen Versand oder andere Dienstleister: <https://drschwenke.de/mailchimp-newsletter-datenschutz-muster-checkliste/>

## Datensicherheit

Wer sich um Backups, Datensicherheit und Verschlüsselung von personenbezogenen Daten bisher gedrückt hat, sollte die DSGVO zum Anlass nehmen, dieses Thema nun anzupacken. Denn zum Datenschutz gehört auch, personenbezogene Daten mit der notwendigen Sorgfalt zu behandeln, vor Verlust und Zugriffen Dritter zu schützen. In Zusammenhang mit dem Schutz journalistischer Quellen sollte man das Thema Datensicherheit besonders ernst nehmen.

Idealerweise sollten personenbezogene Daten also insbesondere auf USB-Sticks (aber eigentlich auch auf Festplatten und im Backup) nur verschlüsselt gespeichert werden. Nutzt man für Backups einen externen Dienstleister (beispielsweise bei Speicherung in einer Cloud bei Amazon, Dropbox, Strato o.ä.), sollte man mit diesem Dienstleister einen Vertrag zur Auftragsverarbeitung abschließen. Diese Verträge bieten alle einschlägigen Dienstleister inzwischen standardmäßig und unkompliziert unter dem Stichwort DSGVO (bzw. englisch: „GDPR“) zum Download an.

Wichtig: Wird ein Datenträger (USB-Stick, SD-Karte, Festplatte, Laptop mit eingebauter Festplatte o.ä.) ausgemustert, müssen alle Daten gelöscht werden, bevor der Datenträger in den Müll oder in Dritte Hände gelangt. Die einfache Löschfunktion von iOS oder Windows reicht dafür nicht aus, vielmehr müssen die Daten nach sicheren Standards mehrfach überschrieben werden, damit sie auch nicht forensisch wiederherstellbar sind.

Entsprechende Software zum Überschreiben gibt es als Freeware. Alternative: Datenträger mit dem Hammer physikalisch zerstören. Mehr Infos zum sicheren Löschen von Daten stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereit: [https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen\\_node.html](https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node.html)

Ein schwieriges Thema sind internationale Webmail-Anbieter, insbesondere Google Mail. Nach aktuellem Stand (Mai 2018) ist die kostenfreie Version von Google Mail wohl eher nicht mit der DSGVO in Einklang zu bringen. Google selbst empfiehlt, auf das kommerzielle Produkt „G Suite“ (ab 4 Euro pro Monat) zu wechseln, das entsprechend zertifiziert ist und damit wohl bedenkenlos genutzt werden kann. Auch in diesem Fall ist mit dem E-Mail-Provider ein Vertrag über Auftragsverarbeitung zu schließen.

# Links und Beiträge zur DSGVO

Links zu ein paar guten Aufsätzen zu bestimmten Themen:

**Newsletter** – sehr guter Leitfaden von Dr. Schwenke: <https://drschwenke.de/mailchimp-newsletter-datenschutz-muster-checkliste/>

Interessanter Beitrag zur Frage, ob **Abmahnungen aufgrund von Datenschutz-Verstößen** nach DSGVO überhaupt zulässig sind: <http://www.rechtzweinull.de/archives/2579-abmahnwellen-wegen-dsgvo-verstoessen-dagegen-spricht-und-wie-man-abmahnungen-gegebenenfalls-abwehren-kann.html>

## Wordpress datenschutzkonform machen

Wordpress selbst arbeitet an einigen Features, mit denen die Einhaltung der DSGVO mit einem Wordpress-Blog einfacher werden soll. Alle Aspekte deckt das aber keinesfalls ab, man sollte mit diesen Funktionen also kritisch umgehen und selbst genau prüfen, was zusätzlich nötig ist.

Einen übersichtlichen Beitrag zu wesentlichen Aspekten in Wordpress hat Sara Grasel bei Trending Topics zusammengestellt: <https://www.trendingtopics.at/dsgvo-so-passt-ihr-wordpress-an-den-neuen-eu-datenschutz-an/> Achtung: Der Beitrag bezieht sich auf die österreichische Umsetzung der DSGVO, insbesondere Mustertexte sind also mit Vorsicht zu genießen.

Eine sehr gute Check-Liste für den eigenen Wordpress-Blog hat René Dasbeck veröffentlicht: <https://www.netz-gaenger.de/blog/aktuelles/dsgvo-checkliste-fuer-meine-kunden-und-andere-wordpress-webseitenbetreiber/>

Mit dem speziellen Problem der IP-Adressen in Blog-Kommentaren setzt sich Jonas Tietgen bei WP Ninjas auseinander: <https://wp-ninjas.de/wordpress-kommentare-ip-entfernen>

## Online-Generatoren für die Datenschutzerklärung

Anwalt Dr. Thomas Schwenke hat Generator für die Datenschutzerklärung erarbeitet, der für nicht-kommerzielle Websites und Kleinunternehmer kostenlos ist. Die kommerzielle Lizenz kostet 99 Euro zzgl. MwSt. <https://datenschutz-generator.de/>

Kostenlos nutzbar ist der Generator der Deutschen Gesellschaft für Datenschutz: <https://dsgvo-muster-datenschutzerklaerung.dg-datenschutz.de/>

Beide Generatoren decken nicht sämtliche Aspekte und denkbaren Konstellationen ab. Deshalb sollte man immer zusätzlich individuell prüfen, welche weiteren Aspekte auf dem eigenen Blog noch hinzukommen und entsprechend ergänzen. Eine Kombination aus den beiden genannten Generatoren führt meist aber schon recht nahe ans Ziel.

## Auftragsverarbeitung

Werden Daten von einem Dritten verarbeitet – also dem eigenen Webhoster, einem Newsletter-Dienstleister, Google Analytics, Google AdSense oder Ähnlichen – ist ein Vertrag zur Auftragsverarbeitung zu schließen. Finn Hillebrandt hat auf Blogmojo eine ausführliche Liste mit Links zu zahlreichen möglichen Auftragsverarbeitern zusammengestellt und gibt Infos, wie man den Vertrag dort jeweils abschließen kann. <https://www.blogmojo.de/av-vertraege/>

## Google-Produkte

Wo Google überall seine Finger datenschutzrelevant im Spiel hat, zeigt ein Beitrag der Internet World Business: <https://www.internetworld.de/onlinemarketing/google/dsgvo-aendert-googles-werbeprodukten-1527598.html>

Mit Google Analytics setzt sich Rechtsanwältin Nina Diercks ausführlich auseinander: <https://diercks-digital-recht.de/2018/05/der-rechtskonforme-einsatz-von-google-analytics-bzw-universal-analytics-unter-der-dsgvo-teil-12-zur-eu-dsgvo-cookies-und-tracking/>

Links zu zahlreichen Detailspekten der DSGVO hat Blog Mojo zusammengestellt: <https://www.blogmojo.de/dsgvo-linksammlung/>

## Material der Aufsichtsbehörde

Muster-Texte, Check-Listen und halbwegs prägnante Informationen stellt das Bayerisches Landesamt für Datenschutzaufsicht bereit, speziell auch für Kleinunternehmer und Vereine: [https://www.lida.bayern.de/de/datenschutz\\_eu.html](https://www.lida.bayern.de/de/datenschutz_eu.html)

## Literatur-Empfehlung

„Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine: Das Sofortmaßnahmen-Paket“

Verlag C.H.Beck, ISBN 978-34067166216, 3 Seiten inkl. nützlicher Checklisten  
5,50 Euro

<https://www.amazon.de/gp/product/3406716628/>

## Allgemeine Empfehlung

Eine allgemeine Empfehlung zum Abschluss: Glauben Sie nicht alles, was in jedem beliebigen Beitrag zur DSGVO steht – auch nicht, wenn es von einem Anwalt geschrieben ist. DSGVO ist derzeit ein Thema, mit dem man sehr viel Traffic (und damit auch Geld) generieren kann und da nehmen es viele nicht so genau mit den Fakten – oder propagieren eigene juristische Thesen als Fakten, um aus der Masse der DSGVO-Beiträge herauszustechen.

Löschen eines Blogs aus Angst vor Konsequenzen der DSGVO ist eine völlig unsinnige und weit überzogene Reaktion. Wie überhaupt jede hektische oder gar panische Reaktion unsinnig ist. Die Gefahren sind ziemlich überschaubar und wie oben dargelegt teils kaum relevant, weil im Fokus von Abmahnern und Datenschutzbehörden zunächst mutmaßlich erst einmal die „großen Fische“ und Unternehmen stehen, die offensichtlich und eklatant gegen die DSGVO und begleitende Gesetze verstoßen – zumindest nicht in absehbarer Zeit.

Was tun? Sich in Ruhe mit dem Thema auseinandersetzen. Möglichst bald, aber nicht überstürzt versuchen, die Vorschriften umzusetzen und einzuhalten. Das Thema weiter beobachten und bei Veränderungen und Klarstellungen zügig reagieren.