



**DIE NEUE  
EU-DATENSCHUTZGRUNDVERORDNUNG  
IST DA. WAS BEDEUTET DAS FÜR  
KOMMUNIKATIONSPROFIS?**

Rainer Maassen  
Geschäftsführer  
Convento GmbH

# Einleitung

Seit dem 25. Mai 2018 müssen in Deutschland und allen anderen EU-Mitgliedstaaten die Regeln der EU-Datenschutzgrundverordnung (im Folgenden DSGVO) beachtet und umgesetzt werden. In Deutschland kommt zusätzlich das auf der DSGVO basierende Bundesdatenschutzgesetz in neuer Fassung (BDSG-neu) zur Anwendung. Die DSGVO und das BDSG-neu lösten in Deutschland das bis zum 24. Mai 2018 gültige Bundesdatenschutzgesetz (BDSG) ab.

Sie als Professional in der Kommunikationsbranche fragen sich jetzt sicherlich: Was bedeutet das konkret für mich und meine Arbeit?

Mit diesem Ratgeber beantworte ich Ihre wichtigsten Fragen. Ich konzentriere mich dabei auf die Behandlung der Kern-Zielgruppe der Kommunikation, die Journalisten und Blogger. Bitte beachten Sie: Meine Zusammenstellung stellt keine Rechtsberatung dar und erhebt keinen Anspruch auf Vollständigkeit. Bitte lassen Sie sich im Zweifelsfall von einem Juristen beraten.

## 1. Warum betrifft die DSGVO unsere Arbeit?

Beim Datenschutz geht es streng genommen nicht um den Schutz von Daten sondern von Personen, deren personenbezogene Daten verarbeitet werden. Das sind in unserem Fall meist Ansprechpartner der Kommunikation, deren Kontakt- und Profildaten wir speichern, um ihnen Nachrichten zu senden und mit ihnen zu kommunizieren. Deren „informationelle Selbstbestimmung“ soll durch die DSGVO gestärkt werden.

### Definitionen

Sie speichern und verarbeiten Daten Ihrer Kommunikations-Zielgruppen. Nach dem DSGVO gelten Sie deshalb als „Verantwortlicher“ gegenüber den „Betroffenen“, deren Daten Sie speichern. Oft geschieht diese Verarbeitung mit Hilfe von IT-Dienstleistern. Diese nennt das Gesetz „Auftragsverarbeiter“.

### Konkretisierung und Erweiterung der Betroffenen-Rechte

Sie als „Verantwortlicher“ im Sinne der DSGVO müssen transparenter werden und die Rechte der Betroffenen genau beachten. Bereits das BDSG räumte den betroffenen Personen das Recht ein zu erfahren, was genau über sie gespeichert und verarbeitet wurde und warum. Jetzt haben diese auch das Recht auf Löschung.

Wenn sich also ein Journalist aus einem Newsletter oder Pressemitteilungs-Versand ausgetragen hat, sind Sie als Verantwortlicher für die technisch sichere Umsetzung des Blacklistings verantwortlich. Hier hilft Ihnen ein gutes IT-System.

## Verzeichnis der Verarbeitungstätigkeiten

In vielen Unternehmen oder Organisationen werden personenbezogene Daten in verschiedenen Abteilungen und aus unterschiedlichen Gründen verarbeitet und oft auch langfristig gespeichert. Meist gibt es niemanden, der darüber noch den Überblick hat. Es fehlt an einer zentralen Stelle, die diese Verarbeitungen sammelt und dokumentiert.

Hier greift die DSGVO mit Dokumentations- und Nachweispflichten für die „Verantwortlichen“ ein. Dazu gehört das Erstellen und Führen eines sogenannten „Verzeichnisses der Verarbeitungstätigkeiten“ (Art. 30 DSGVO). Von dieser Pflicht ausgenommen sind nur Unternehmen mit weniger als 250 Mitarbeitern, aber auch nur dann, wenn sie (laut Art. 30 Abs.5) nur gelegentlich personenbezogene Daten verarbeiten.

Das kann beispielsweise bei PR- und Marketingagenturen ausgeschlossen werden: Hier werden regelmäßig personenbezogene Daten verarbeitet. Aber keine Sorge: als Agentur mit einem überschaubaren Geschäftsmodell haben Sie das Verzeichnis schnell ausgefüllt. Nur größere Unternehmen, die Daten in vielen Abteilungen verarbeiten, haben oder hatten Aufwand damit. Hinweise zum Führen des Verzeichnisses und ein Word-Dokument als Muster stellen wir Ihnen gern zur Verfügung.

## Erweiterte Pflichten in Bezug auf die Datensicherheit und das Vertragswesen

Änderungen ergeben sich für Sie auch bei der Einhaltung der „Datensicherheit“ und bei den vertraglichen Beziehungen mit Ihrem IT-Dienstleister. Sehen Sie dazu die Ausführungen weiter unten (3. und 4.).

## 2. Dürfen wir Daten von Journalisten so verarbeiten wie bisher?

Wie bisher benötigt ein Unternehmen eine Rechtsgrundlage, um personenbezogene Daten rechtmäßig verarbeiten zu dürfen. Die DSGVO nennt konkrete Gründe, unter denen eine Verarbeitung personenbezogener Daten rechtmäßig ist.

### Zwei für uns wesentliche Gründe sind:

1. Die betroffene Person erteilt ihre „Einwilligung“ zur Verarbeitung.
2. Es liegt ein „berechtigtes Interesse“ der verarbeitenden Stelle vor.

### Ad 1.

Journalisten und Blogger, die sich auf Ihrer Website für Newsletter oder Pressemitteilungen eintragen, haben Ihnen damit die erforderliche Einwilligung erteilt. **Solche expliziten Einwilligungen bleiben auch mit der DSGVO bestehen und müssen nicht neu eingeholt werden.** Darüber hinaus dürfen Sie von einer „impliziten Einwilligung“ zur Verarbeitung zum Zweck der Zusendung von Pressemitteilungen ausgehen, wenn die Kontaktdaten eines Journalisten im Impressum eines Mediums oder auf der Website eines Mediums veröffentlicht werden. Das Gleiche gilt, wenn ein Journalist seine E-Mail Adresse auf einer eigenen Website oder in seinem Social Media Account veröffentlicht.

### Ad 2.

Sie als Kommunikationsprofi haben ein „berechtigtes Interesse“, Journalisten aktiv mit Informationen zu versorgen. Dazu benötigen Sie Kontaktdaten, wie die E-Mail Adresse und die geschäftliche Telefonnummer der betroffenen Person. Gemäß Art. 6 Abs. 1 lit. f) der DSGVO bedeutet dies, dass die Interessen, Grundrechte und Grundfreiheiten des Journalisten, die den Schutz seiner personenbezogenen Daten erfordern, nicht das berechtigte Interesse des Verarbeiters seiner Daten überwiegen.

Darüber hinaus heißt es aus den Reihen der Berufsverbände (DPRG, BdP, DJV), dass auch Journalisten ein „berechtigtes Interesse“ an Unternehmensnachrichten haben und somit quasi eine „implizite Einwilligung“ zur Zusendung von Nachrichten besteht.

### Grenzen der Einwilligung und des berechtigten Interesses:

Einwilligung und berechtigtes Interesse von Journalisten an der Zusendung von Nachrichten gilt aber nur für aus deren Sicht „relevante Meldungen“. Es muss sich also um eine „Pressemitteilung“ handeln und nicht etwa um Werbung (das wäre Spam), und die Meldung muss zumindest im weitesten Sinne auch mit den Themen des Journalisten zu tun haben (andernfalls wird diese auch als Spam wahrgenommen).

Außerdem muss es sich definitiv um einen Journalisten handeln. Diese Frage ist nicht immer eindeutig und sofort zu beantworten. Blogger und sonstige Autoren im Web, die sich selbst nicht als Journalisten sehen, sollten tunlichst nicht ohne explizite Einwilligung angeschrieben werden. Hier empfiehlt es sich, zunächst genau deren Websites und Texte zu studieren, und sie dann gegebenenfalls dezent per Brief zu kontaktieren. Leider ist die Grenze zwischen Journalisten und Bloggern nicht eindeutig zu ziehen.

### 3. Was hat sich bei den Regelungen zur Einhaltung der „Datensicherheit“ geändert?

Die DSGVO, ebenso wie das BDSG-neu, verlangen auch zukünftig eine besondere Sorgfalt in Bezug auf die „Datensicherheit“. Darunter versteht man alle technischen und organisatorischen Maßnahmen (TOM), die dem Schutz vor u.a. Verlust, Diebstahl oder Beschädigung von Daten dienen. Beispiele: Datensicherung, Firewall, unterbrechungsfreie Stromversorgung, aber auch organisatorische Maßnahmen wie Zugriffskontrolle, Zutrittskontrolle zu IT-Anlagen usw.

Falls es trotz aller Maßnahmen zu einem Verlust, Diebstahl oder einer Beschädigung kommt, ist jetzt aber die **Beweislast umgekehrt**: Bisher mussten betroffene Personen im Schadensfall nachweisen können, dass die verarbeitende Stelle als „Verantwortlicher“ nicht sauber gearbeitet hat. In Zukunft muss der „Verantwortliche“ nachweisen, dass er „in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“.

Dieselbe Nachweispflicht trifft zukünftig auch im Schadensfall alle Auftragsverarbeiter gegenüber betroffenen Personen. Der Verantwortliche und sein Auftragsverarbeiter können so Gesamtschuldner gegenüber geschädigten betroffenen Personen werden.

Unbeschadet einer möglichen zivilrechtlichen Haftung gegenüber geschädigten betroffenen Personen können nach der DSGVO die zuständigen Aufsichtsbehörden auch weiterhin Bußgelder verhängen, deren maximaler Rahmen deutlich erhöht wurde, um so dem Datenschutz in der EU noch mehr Nachdruck zu verleihen.

Wichtig ist daher eine möglichst lückenlose Dokumentation aller Maßnahmen und Verarbeitungsschritte und eine entsprechend risikobasierte Ausprägung der „TOM“ (technischen und organisatorischen Maßnahmen).

### 4. Was hat sich in Bezug auf das benötigte Vertragswesen geändert?

Wenn Sie mit einem IT-Dienstleister zusammenarbeiten, der theoretisch mit personen-bezogenen Daten in Kontakt kommen kann, für die Sie verantwortlich sind, sollten Sie diese Zusammenarbeit durch einen „Vertrag zur Auftragsdatenverarbeitung“ (ADV-Vertrag) absichern. Der ADV-Vertrag enthält eine klare Definition der gegenseitigen Rechte und Pflichten im Einklang mit allen geltenden Datenschutzbestimmungen.

Dieser Vertrag mit Ihrem Dienstleister ist wichtig, weil Sie gegenüber den betroffenen Personen, zum Beispiel den Journalisten, „Verantwortlicher“ bleiben. Mit dem ADV-Vertrag sichern Sie sich die Mithilfe und Arbeitsqualität des Auftragsverarbeiters in Bezug auf den erforderlichen Datenschutz.

## 5. Welche Informationen dürfen wir überhaupt verarbeiten?

Die DSGVO spricht hier von der „Verhältnismäßigkeit der Verarbeitungsvorgänge“ in Bezug auf den Zweck. Es sollen nur diejenigen Informationen verarbeitet werden, an denen ein „berechtigtes Interesse“ besteht. Nicht legitimierte personenbezogene Daten sollten daher nicht verarbeitet werden.

Damit einher geht das Gebot der „Datensparsamkeit“. Daten sollen nur zum angegebenen Zweck erhoben werden und nicht ohne konkreten Anlass, und nur in dem Umfang, den man für den Zweck auch wirklich braucht („Privacy by Default“). Die dabei verwendeten Systeme sollen so aufgebaut sein, dass sie Datensparsamkeit automatisch unterstützen („Privacy by Design“).

Was das im Einzelnen für Sie bedeutet, hängt von der konkreten Praxis ab. Das Geburtsdatum mag normalerweise nicht wichtig sein. Wenn Sie aber ein Automobilhersteller sind und zu Testfahrten nur Personen mit gültiger Fahrerlaubnis zwischen dem 25. und 60. Lebensjahr zulassen wollen, ist es in Bezug auf den Zweck für Sie wichtig. Dahinter steht ein legitimes Interesse, welches insofern als verhältnismäßig bewertet werden kann. Ein Schuhhersteller, der neue Modelle an Journalisten verteilt, darf daher auch deren Schuhgröße speichern. Wichtig sind möglicherweise auch Details aus den Veröffentlichungen der Journalisten, soweit sie selbst mit vollem Namen als Autor für den Inhalt verantwortlich zeichnen.

## 6. Zusammenfassung: Pflichten der Verantwortlichen

Die Erschaffer der neuen EU Datenschutzgrundverordnung wurden von der Überzeugung geleitet, dass persönliche Daten im Digitalen Zeitalter einen hohen und wachsenden Wert haben. Auf ihrer Basis entstehen immer neue Geschäftsmodelle.

Die DSGVO soll das Bewusstsein der Menschen für den Wert der eigenen Daten stärken. Ebenso soll sie den Menschen die Kontrolle über ihre Daten zurückgeben.

Für Unternehmen und Organisationen, die als „Verantwortliche“ personenbezogene Daten pflegen und verwenden, ergeben sich daraus Pflichten, die diese auf vertraglicher, organisatorischer und technischer Ebene erfüllen müssen. Die wesentlichen Punkte:

- **Sicherstellung der Rechte Betroffener**
- **Transparenz der Datenverarbeitung**
- **Angemessene Verträge**
- **Umsetzung der technischen und organisatorischen Maßnahmen**
- **Führen eines Verfahrenszeichnisses**

Darüber hinaus wird für bestimmte Unternehmen und Organisationen eine Risikoabschätzung gefordert, auch „Datenschutzfolgenabschätzung“ (Data Protection Impact Assessment) genannt. Hier einmal eine gute Nachricht: Nur bei kritischen und besonders schützenswerten Daten ist dies notwendig. Daten von Ansprechpartnern der Kommunikation gehören üblicherweise nicht dazu, insbesondere wenn die Daten aus deren Veröffentlichungen gewonnen werden.

## 7. Wie hilft eine professionelle PR-Lösung wie myconvento?

- **Betroffene haben das Recht auf Einsichtnahme ihrer Daten und Transparenz der Verarbeitung:**  
myconvento bietet eine lückenlose Änderungshistorie, die automatisch geführt wird und den Betroffenen auf Wunsch ohne großen Aufwand zur Verfügung gestellt werden kann.
- **Verantwortliche müssen den Export von personenbezogenen Daten in Länder außerhalb der EU in ihrem Verzeichnis führen und den Zweck des Exports angeben:**  
Die Daten sind und bleiben im Rechenzentrum in Düsseldorf und werden nicht ins Ausland außerhalb der EU exportiert.
- **Betroffene haben das Recht auf Änderung und Löschung ihrer Daten:**  
Empfänger können sich einfach und sicher von Informationen an- und abmelden. myconvento überträgt die Anmelder-Daten direkt in korrespondierende Verteiler. Dadurch erhalten die Personen in Ihrer Datenbank später genau die Informationen, zu denen sie sich angemeldet haben. Abmeldungen führen wiederum zu einem sicheren „Blacklisting“ der abgemeldeten Person.
- **Angemessene Verträge und Umsetzung der technischen und organisatorischen Maßnahmen:**  
myconvento bietet seinen Kunden ein regelkonformes Vertragswesen, einen festen Ansprechpartner für den Datenschutz, ein TÜV zertifiziertes Rechenzentrum und ausgearbeitete und überprüfbare TOMs. Datenschutz sehen wir als Kernkompetenz.
- **Führen eines Verfahrensverzeichnisses:**  
Auf Wunsch stellen wir unseren Anwendern alle Informationen für das Führen ihres Verfahrensverzeichnisses zur Verfügung.



Convento GmbH  
Oberstrasse 4  
41460 Neuss

[info@convento.de](mailto:info@convento.de)  
[www.myconvento.com](http://www.myconvento.com)



Cloudservice  
made and hosted  
in Germany