

DIE NEUE

# EU-Datenschutz-Grundverordnung

Worauf kommt es an?



Dieses Whitepaper ist eine Kooperation zwischen



HÄNDLERBUND



Newsletter2Go

# Inhaltsverzeichnis

---

Editorial 02

---

Die fünf Gebote im Datenschutz 03

---

Setup im E-Mail Marketing nach DSGVO 04

---

Newsletter-Abonnenten rechtssicher sammeln nach DSGVO und UWG 06

---

Der Newsletterversand 08

---

Informationspflichten nach Art. 13, 14 DSGVO 09

---

Auskunftsrechte der betroffenen Personen - Art. 15 DSGVO 11

---

Über Newsletter2Go 12

---

# Editorial

---

Am 25. Mai 2018 tritt die europaweit gültige Datenschutz-Grundverordnung (DSGVO) in allen Ländern der Europäischen Union alleinig in Kraft und ersetzt das bisher gültige Bundesdatenschutzgesetz. Aus diesem Grund haben wir gemeinsam mit dem Händlerbund und unserem internen Datenschutzbeauftragten und Justiziar ein Whitepaper entwickelt, das Ihnen die zentralen Inhalte und Veränderungen übersichtlich und so kurz wie möglich darstellen soll.

Bereits vor dem alleinigen Inkrafttreten der DSGVO müssen Vorbereitungen getroffen und zahlreiche Geschäftsprozesse angepasst werden. Eine intensive Vorbereitung ist eine notwendige Voraussetzung für die Sicherstellung Ihrer Datenschutzkonformität.

## Die wichtigsten Fakten zur DSGVO:

- 88 Seiten
- 99 Artikel
- offizieller Titel: „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“
- Der erste Entwurf wurde 2011 fertiggestellt
- die DSGVO gilt alleinig ab dem 25. Mai 2018.



Ich wünsche Ihnen ein schönes und erfolgreiches Jahr 2018,  
Ihre Sarah Weingarten

*Diese Broschüre dient nur Informationszwecken und ist ausdrücklich nicht als rechtliche Beratung zu verstehen. Wir übernehmen keinerlei Haftung für die Richtigkeit und Vollständigkeit der dargelegten Informationen.*

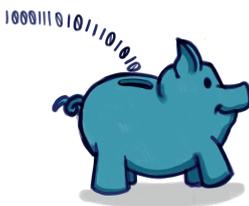
# Die 5 Gebote im Datenschutz



## Verbot mit Erlaubnisvorbehalt

Jede Datenverarbeitung, die nicht durch eine Einwilligung des Betroffenen abgedeckt ist, bedarf einer gesetzlichen Erlaubnis. Soweit kein Erlaubnistatbestand vorliegt, dürfen die Daten nicht verarbeitet werden.

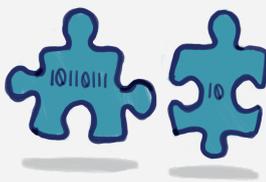
*Beispiel:* Für das Versenden von Newslettern gibt es keine pauschale gesetzliche Erlaubnis. Die Einwilligung ist von jedem Empfänger gesondert sowie vorab einzuholen.



## Datensparsamkeit

Eine Datenverarbeitung muss dem Zweck angemessen und sachlich relevant sowie auf das notwendige Maß beschränkt sein.

*Beispiel:* Bei einer Warenbestellung darf keine Telefonnummer erhoben werden, wenn sie für die Bestellungsabwicklung nicht notwendig ist.



## Zweckbindung

Die Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben wurden. Im Fall einer Zweckerreichung sind die Daten zu löschen.

*Beispiel:* Die erhobene Adresse bei der Bestellung darf nur für die Bestellabwicklung genutzt werden.



## Datensicherheit

Bei der Verarbeitung von Daten müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um den Schutz vor Datenmissbrauch zu gewährleisten.

*Beispiel:* Wer mit sensiblen Kundendaten arbeitet, muss gewährleisten, dass keine unberechtigte Person Zugriff auf sie hat (z. B. durch Passwörter, Verschlüsselung).



## Transparenz

Betroffene sollen wissen, dass und welche Daten in Bezug auf ihre Person erhoben wurden (u.a. Verzeichnisse, Löschkonzept, etc.).

*Beispiel:* Wer Daten ohne Wissen des Webseitenbesuchers, erhebt, muss mindestens in der Datenschutzerklärung transparent darüber aufklären.

# Setup im E-Mail Marketing nach DSGVO

## Zusammenfassung: Anforderungen an die Versandsoftware:

- Vertrag zur Auftragsverarbeitung schließen
- Geprüfte technische und organisatorische Maßnahmen
- Serverstandort in Deutschland oder der EU
- Datenschutz-Zertifizierung des Dienstleisters

## Rechtliche Erläuterung

Zur datenschutzkonformen Gestaltung des E-Mail Marketings sind unterschiedliche Maßnahmen erforderlich. Die nachfolgend aufgeführten Maßnahmen sind nach unserer Ansicht besonders praxisnah und verdienen daher eine genauere Darstellung.

Die Erhebung oder Verarbeitung von personenbezogenen Daten bedarf grundsätzlich einer gesetzlichen Erlaubnis oder einer Einwilligung durch den jeweiligen Betroffenen. Gemäß Art. 4 DSGVO sind personenbezogene Daten sämtliche Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Soweit Datenerhebungen rechtswidrig erfolgen, drohen hohe Bußgelder anhand des Bußgeldkataloges in Art. 83 DSGVO.

Darüber hinaus sind die technischen und organisatorischen Maßnahmen des Auftragnehmers (Dienstleisters) durch eine Folgenabschätzung nach Art. 35 DSGVO und ein diesbezügliches IT-Sicherheitskonzept darzustellen. Diese Folgenabschätzung ersetzt die bisherige datenschutzrechtliche Vorabkontrolle nach § 4d Abs. 5 BDSG sowie den Katalog bezüglich technischer und organisatorischer Maßnahmen nach der Anlage zu § 9 BDSG. Nunmehr ist eine Risikoabschätzung von Datenverarbeitungsvorgängen zu erarbeiten, soweit die Datenverarbeitungsvorgänge eine Gefährdung von Rechten und Freiheiten der Betroffenen inne haben.

**Nach Art. 32 Abs. 3 DSGVO kann insbesondere im Auftragsverhältnis eine Zertifizierung gemäß Art. 42 DSGVO als Faktor herangezogen werden, um die Erfüllung der Anforderungen an eine Folgenabschätzung zu gewährleisten. Eine solche Zertifizierung dient jedoch nur als einzelner Nachweis der Datenschutzkonformität und beseitigt nicht die Pflicht der Erarbeitung einer eigenen Folgenabschätzung.**

## Auftragsverarbeitung bei Subunternehmen (Art. 28, 32 DSGVO)

### Aktuell: Datenerhebungen durch Unternehmen

- Grundsätzlich ist jedes Unternehmen für Datenerhebungen vollumfänglich verantwortlich.
- Eine Erweiterung der eigenen Verantwortlichkeit auf die jeweils eingesetzten Dienstleister war bisher durch den Abschluss eines Vertrages zur Auftragsdatenverarbeitung möglich.
- Der eingesetzte Dienstleister wurde bei Abschluss eines solchen Vertrages rechtlich wie ein Teil des Auftraggebers behandelt, weshalb keine erneute gesetzliche Erlaubnis oder Einwilligung durch die Betroffenen notwendig war.

### Zukünftig: Vertrag zur Auftragsverarbeitung mit Subunternehmern

- Erweiterung der Verantwortlichkeit für die verantwortliche Stelle durch Vertrag zur Auftragsverarbeitung.
- Voraussetzung: Es muss tatsächlich eine Verarbeitung im Auftrag vorliegen.
- Diese Verarbeitung ist abzugrenzen von einer Funktionsübertragung zwischen Unternehmen, welche durch das Vorliegen eigener Entscheidungsbefugnisse und einem eigenen Interesse des Dienstleisters an den Daten definiert wird.
- Soweit zwischen der verantwortlichen Stelle und dem Dienstleister keine Funktionsübertragung besteht, sollte zwischen den Unternehmen ein Vertrag zur Auftragsverarbeitung abgeschlossen werden, welcher sich an den Vorgaben der Art. 28, 32 DSGVO orientiert.
- Zwischen Newsletter2Go und seinen Kunden sind die Voraussetzungen an eine Auftragsverarbeitung gegeben, sodass stets ein solcher Vertrag zur Auftragsverarbeitung abgeschlossen werden kann.

# Newsletter-Abonnenten rechtssicher sammeln nach DSGVO und UWG

## Zusammenfassung

- Double-Opt-in (DOI)
- Werbefreie DOI
- Es muss ein Zweck im Formular angegeben werden!
- Es muss einen Hinweis auf die Datenschutzerklärung in der Einwilligung geben
- Die Verwendung von Newsletter2Go muss in der Datenschutzerklärung aufgeführt werden.

## Rechtliche Erläuterung

Der Newsletterversand darf bereits nach der aktuellen Gesetzeslage nicht ohne Einwilligung des Empfängers vorgenommen werden. Künftig wird diese Gesetzeslage weiter verschärft: Eine Einwilligung für den Erhalt von Newslettern darf ferner aufgrund des sogenannten Kopplungsverbots nicht vom Vertragsabschluss abhängig gemacht werden, sofern diese nicht für die Erfüllung des Vertrages erforderlich ist. Wenn Sie also beispielsweise ein Produkt verkaufen, dann darf dies nicht von einer Einwilligung in den Newsletterversand abhängig gemacht werden.

Explizite Regelungen für den Newsletterversand sind in der DSGVO nicht enthalten. Daher gelten für einen Newsletterversand die allgemeinen Prinzipien des Datenschutzrechts. Darüber hinaus sind die Regelungen des Gesetzes gegen den unlauteren Wettbewerb (UWG) sowie die aktuellen Entwicklungen zur EU-Privacy-Verordnung zu beachten.

Zur Gewährleistung einer einverständlichen Newsletter-Versendung sollte das sogenannte Double-Opt-in-Verfahren genutzt werden. Im Zuge dessen lässt sich der potentielle Empfänger in einen Verteiler aufnehmen. Anschließend erhält der Nutzer durch eine Bestätigungs-E-Mail die Möglichkeit, die Anmeldung rechtssicher zu bestätigen. Erst mit Bestätigung dieser E-Mail ist der DOI-Prozess abgeschlossen.

**Hinweis:** Bei jeglicher Datenverarbeitung personenbezogener Daten abseits des Newsletter-Versands ist eine separate datenschutzrechtliche Einwilligung des jeweiligen Betroffenen erforderlich.

### Die folgenden Mindestanforderungen sind für eine datenschutzrechtliche Einwilligung sind nach der DSGVO zu beachten:

1. Einwilligung durch ausdrückliche Handlung des Adressaten (bewusst und eindeutig).
2. Inhalt der Einwilligungserklärung muss für Adressaten jederzeit abrufbar sein und den Zweck der Datenverarbeitung hinreichend beschreiben (Datenschutzerklärung).
3. Protokollierung der Einwilligung (wird durch Verwendung von Newsletter2Go automatisch gemacht).
4. Der Adressat muss vor der Einwilligungserklärung auf die jederzeitige Widerrufsmöglichkeit (Abbestellmöglichkeit) hingewiesen werden. Wir empfehlen, eine solche Abbestellmöglichkeit in die Datenschutzerklärung aufzunehmen und den Betroffenen im Rahmen der Einwilligungserklärung um Kenntnisnahme bezüglich der Datenschutzerklärung zu bitten.

Darüber hinaus muss jeder Datenverarbeiter als verantwortliche Stelle in seiner Datenschutzerklärung nach dem Katalog des Art. 13 DSGVO den jeweiligen Nutzer umfassend über die Datenverarbeitungsvorgänge durch die Internetnutzung informieren. Den Kunden und Nutzern von Newsletter2Go wird daher empfohlen, einen diesbezüglichen Hinweis in die Datenschutzerklärung auf der Website zu implementieren. Innerhalb des DOI-Prozesses sowie im Rahmen der Einwilligungserklärung ist ein Verweis auf die Datenschutzerklärung mit der Bitte um deren Kenntnisnahme notwendig.

## Sonderfall: Direktwerbung

Nur im Ausnahmefall ist eine vorherige, ausdrücklich erteilte Einwilligung des Adressaten für den Erhalt eines Newsletters, Telefon- oder E-Mail-Werbung nicht erforderlich.

**Eine solche Ausnahme kann vorliegen, wenn die nachfolgend aufgeführten Voraussetzungen gegeben sind:**

1. der Kunde Bestandskunde ist
2. Werbung für ähnliche Waren erfolgt
3. der Kunde der Verwendung nicht widersprochen hat
4. bei Erhebung der E-Mail-Adresse und bei jeder Zusendung von Direktwerbung ein klarer und deutlicher Hinweis auf das Widerspruchsrecht erfolgt.

Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann unter gewissen Umständen als eine dem berechtigten Interesse dienende Verarbeitung betrachtet werden. Bitte beachten Sie diesbezüglich die Vorgaben des § 7 UWG und die damit verbundene, differenzierte Rechtsprechung. Darüber hinaus sind die aktuellen Entwicklungen der geplanten E-Privacy-Verordnung zu beachten, sobald diese in Kraft tritt.

# Der Newsletterversand

---

## Zusammenfassung

- Das Telemediengesetz (TMG)
- Impressum
- Opt-Out

## Rechtliche Erläuterung

---

Unabhängig von der DSGVO sind weiterhin die gesetzlichen Vorgaben des Telemediengesetzes (TMG) beim Newsletterversand zu beachten.

Neben der Impressumspflicht für Webseiten muss auch der Versender von kommerziellen Newslettern ein Impressum im Newsletter bereithalten, welches gemäß der Vorgaben des § 6 TMG beschaffen sein muss. Newsletter bilden im Zuge dessen geschäftsmäßige Teledienste im Sinne dieser Vorschrift, welche als Dienste im Internet mit wirtschaftlichen Interesse des Diensteanbieters definiert werden.

### Die Mindestangaben eines Impressums im Newsletter sind:

- Name und Anschrift des Anbieters
- Vertretungsberechtigter
- Aufsichtsbehörde, soweit eine behördliche Zulassung erforderlich ist (z.B. im Gaststättenrecht)
- Registergericht, Registernummer

 **Darüber hinaus können sich weitere Pflichtangaben für besondere Berufsgruppen ergeben.**

Ferner muss in Newslettern jederzeit eine sogenannte Opt-Out-Möglichkeit vorhanden sein. Dies erfolgt zumeist durch einen Abmeldelink innerhalb des Newsletters. Dabei ist zu beachten, dass der Newsletter mittels eines Klicks abbestellt werden kann, um die Abmeldung unkompliziert und benutzerfreundlich zu gestalten. Von einem zweistufigen Abmeldeverfahren im Sinne eines Double-Opt-out sollte abgesehen werden.

# Informationspflichten nach Art. 13, 14 DSGVO

## Zusammenfassung

- Handlungsanweisung Datenschutzerklärung
- Informationspflicht bei Direkterhebung
- Information bei Dritterhebung
- Darstellungsformen

Jeder Webseitenbetreiber, der personenbezogene Daten erhebt und verarbeitet, ist nach § 13 DSGVO auch zukünftig zur Einarbeitung einer Datenschutzerklärung im Internet-Auftritt verpflichtet. Die Datenschutzerklärung gibt einen Überblick über die Erhebung und Verarbeitung von Daten durch die jeweils verantwortliche Stelle. Darüber hinaus bestehen die nachfolgend aufgeführten Informationspflichten:

Informationspflichten nach der DSGVO:	
<b>Informationspflichten allgemein</b>	<ul style="list-style-type: none"><li>• Firmierung und Kontaktdaten der verantwortlichen Stelle</li><li>• Kontaktdaten des Datenschutzbeauftragten bzw. des zuständigen Ansprechpartners für die Themenbereiche Datenschutz und Datensicherheit</li><li>• die Zwecke der Datenverarbeitung</li><li>• die Rechtsgrundlage für die Verarbeitung</li><li>• Informationen zu den berechtigten Interessen, die mit der Datenverarbeitung verfolgt werden</li><li>• die Empfänger der Daten</li><li>• Informationen zur Absicht des Verantwortlichen, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln</li><li>• die Speicherdauer</li><li>• das Auskunftsrecht</li><li>• das Berichtigungs-, Lösungs- oder Einschränkungrecht</li><li>• das Widerspruchsrechts oder Widerrufsrechts der Einwilligung</li><li>• das Rechts auf Datenübertragbarkeit</li><li>• das Recht, die Einwilligung jederzeit zu widerrufen</li><li>• das Beschwerderecht bei der jeweiligen Aufsichtsbehörde</li></ul>
<b>Informationspflicht bei Direkterhebung<sup>1</sup> Art. 13 DSGVO</b>	<ul style="list-style-type: none"><li>• Informationen, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist</li><li>• Informationen, ob die Person verpflichtet ist, die Daten bereitzustellen und welche möglichen Folgen eine Nichtbereitstellung hätte</li><li>• Änderung des Zwecks der Datenverarbeitung</li></ul>
<b>Informationspflicht bei Dritterhebung<sup>2</sup> Art. 14 DSGVO</b>	<ul style="list-style-type: none"><li>• die Kategorien von Daten, die verarbeitet werden</li><li>• Informationen zur Herkunft der Daten</li></ul>

<sup>1</sup> Informationspflicht bei Erhebung von Daten direkt bei der Person

<sup>2</sup> Informationspflicht, wenn die personenbezogenen Daten nicht bei der Person erhoben wurden

Der Verantwortliche hat der betroffenen Person alle Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.

Dabei ist die Nutzung der folgenden Darstellungsformen möglich:

- schriftlich,
- elektronisch,
- in Piktogramm-Form.

Ein besonderes Problem ist das Spannungsfeld zwischen mitunter komplexen technischen Vorgängen, z.B. Analyse-Tools, und einer verständlichen Sprache. Darüber hinaus sind zahlreiche Datenschutzerklärungen in der Praxis unvollständig oder inhaltlich widersprüchlich gestaltet.

**Aufgrund der Komplexität der Regelungsgehalte der Datenschutzerklärung empfehlen wir Ihnen zur Erarbeitung Ihrer Datenschutzerklärung nachdrücklich, eine datenschutzrechtliche Rechtsberatung bei einem Datenschutz-Experten in Anspruch zu nehmen.**



# Auskunftsrechte der betroffenen Personen - Art. 15 DSGVO

## Zusammenfassung

- Auskunftsanspruch von Betroffenen beachten
- Bereitstellende Informationen und Datenkategorien
- Ausnahmen vom Auskunftsanspruch

## Rechtliche Erläuterung

Die betroffenen Personen haben darüber hinaus ein Auskunftsrecht nach Art. 15 DSGVO. Dieses Auskunftsrecht ist aus datenschutzrechtlicher Sicht eine Entsprechung des § 34 BDSG. Hinsichtlich der genauen Ausgestaltung des Auskunftsanspruchs bestehen jedoch zwischen den beiden Regelungen Unterschiede. Zunächst hat die betroffene Person das Recht, von der verantwortlichen Stelle eine Bestätigung über den Umstand zu verlangen, ob personenbezogene Daten über sie verarbeitet werden. Soweit dies besteht, hat die Betroffene Person ein Recht auf Auskunft bezüglich dieser personenbezogenen Daten.

**Darüber hinaus hat der Verantwortliche in einem solchen Fall die folgenden Informationen herauszugeben:**

- die Verarbeitungszwecke
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

**Bezüglich des Auskunftsrechts bestehen mitunter Ausnahmen, weshalb unter gewissen Umständen eine Auskunft abgelehnt werden kann. Dies ist u. U. gegeben bei Anträgen bezüglich Big-Data, die nicht hinreichend präzisiert sind. Ebenso sieht § 15 Abs. 4 DSGVO eine gesetzliche Ausnahme bezüglich des Auskunftsanspruchs vor, soweit durch die Auskunftserteilung in die Rechte und Freiheiten anderer unzulässig eingegriffen würde.**

## Über Newsletter2Go

---

Die Newsletter2Go GmbH wurde 2011 gegründet und konnte sich innerhalb weniger Jahre zu einem der führenden Anbieter von E-Mail Marketing Software in Deutschland entwickeln. Allein innerhalb der letzten 2 Jahre ist Newsletter2Go von 4 auf nunmehr insgesamt 58 Mitarbeiter und von 7.000 auf über 120.000 Kunden gewachsen. Damit ist Newsletter2Go unter den Top 30 der wachstumsstärksten Digitalunternehmen Deutschlands (Gründerszene Wachstums-Ranking 2015, 2016). Bei der Kundenzufriedenheit ist Newsletter2Go mit über 99,5% zufriedenen Kunden in Deutschland Spitzenreiter. Zu den Kunden zählen vor allem E-Commerce-Händler, Vereine, Agenturen, kleine und mittelständische Unternehmen und Großunternehmen.

Erstellen und gestalten Sie anspruchsvolle E-Mail-Marketing-Kampagnen direkt in Ihrem Browser. Verwalten Sie Ihre Empfänger und versenden Sie zielgerichtete Lifecycle Mailings mit unserer Newsletter Software. Newsletter2Go steht für eine verkaufsstarke E-Mail Marketing Software.



Newsletter2Go

Jetzt kostenlos testen und 1.000 E-Mails im Monat gratis versenden:

<https://www.newsletter2go.de/registrierung/>

Kontaktieren Sie uns für Ihre individuelle  
E-Mail-Marketing-Lösung



**Lukasz Jakubczak**  
Head of Sales  
Tel.: +49 (0)30 / 311 994 04

Newsletter2Go GmbH - Nürnberger Straße 8 - 10787 Berlin