von Rechtsanwalt **Jan Lennart Müller**

# Sicherer Umgang mit der DSGVO: Die wichtigsten Datenschutz-Tipps

Der Datenschutz verlangt Online-Händlern im Alltag viel ab. Wir beleuchten in diesem Beitrag, in welchen Bereichen Online-Händler im Tagesgeschäft die häufigsten Berührungspunkte mit der DSGVO haben und welche datenschutzrechtlichen Aspekte besonders relevant sind. Was Online-Händler in diesem Zusammenhang gesetzlich beachten müssen und wie Ihnen die IT-Recht Kanzlei bei der Einhaltung der datenschutzrechtlichen Verpflichtungen nach der DSGVO behilflich sein kann, haben wir in den folgenden Datenschutz-Tipps zusammengetragen.

## 1. Tipp: Datenschutzerklärung

Spätestens seit Inkrafttreten der DSGVO ist die Datenschutzerklärung einer der zentralen Punkte im Bereich des Datenschutzes. Die **Datenschutzerklärung** ist heute für Online-Händler wichtiger denn je. Nicht nur für die eigenen Verkaufskanäle, sondern auch und insbesondere für kommerziell betriebene Social-Media-Accounts.

Und gerade hier können sich Fehler besonders rächen. Zu den Problemen im Bereich der Datenschutzerklärung zählt neben einer gänzlich fehlenden Datenschutzerklärung eine solche Erklärung, die den strengen Anforderungen der DSGVO nicht genügt. Bereits vor dem Hintergrund zahlreicher gerichtlicher Entscheidungen ist deutlich ersichtlich, dass im Bereich der Datenschutzerklärung nicht selten **abgemahnt** wird bzw. **Ordnungsgelder** der Datenschutzaufsichtsbehörden ergehen.

Doch welche Anforderungen werden konkret an eine Datenschutzerklärung gestellt? Die Datenschutz-Grundverordnung (DSGVO) stellt die maßgeblichen Vorgaben für den Inhalt einer Datenschutzerklärung in **Art. 13 Abs. 1 DSGVO** auf. Diese dort genannten **Pflichtinformationen** müssen zwingend in der Datenschutzerklärung enthalten sein.

Hierdurch soll gewährleistet werden, dass betroffene Personen sich ausreichend über die relevanten Datenverarbeitungsvorgänge **informieren** können.

Der Katalog in Art. 13 Abs. 1 DSGVO schreibt Online-Händlern konkret vor, worüber in der Datenschutzerklärung zu informieren ist.

Im Falle von Verstößen drohen Ordnungsgelder von Datenschutzaufsichtsbehörden. Auch wettbewerbsrechtliche Abmahnungen werden in diesem Bereich ausgesprochen, wobei noch nicht gerichtlich geklärt ist, ob derartige Verstöße als Wettbewerbsverstöße geahndet werden können.

Weitere Informationen zum Thema Abmahnbarkeit von Datenschutzverstößen können Sie in unserem Beitrag „Wie ist der aktuelle Stand - sind Verstöße gegen die DSGVO wettbewerbsrechtlich abmahnbar?“ nachlesen!

**Tipp für Mandanten der IT-Recht Kanzlei:**

Sie können in Ihrem Online-Mandantenportal Ihre Datenschutzerklärung ganz einfach selbst erstellen!

## 2. Tipp: Verarbeitungsverzeichnis

Neben der obligatorischen Datenschutzerklärung bereitet auch das sog. **Verfahrensverzeichnis** Händlern immer noch Kopfzerbrechen. Das Verfahrensverzeichnis, welches häufig auch als „Verarbeitungsverzeichnis“ bezeichnet wird, findet seine rechtliche Grundlage in Art. 30 DSGVO.

Nach dieser Norm ist der datenschutzrechtlich Verantwortliche zur Führung eines elektronischen oder schriftlichen Dokuments verpflichtet. In diesem Dokument sind neben diversen Pflichtangaben generell-abstrakt die Verarbeitungsvorgänge durch den Verantwortlichen aufzulisten. Das Dokument des Verarbeitungsverzeichnisses ist nicht öffentlich, sondern betriebsintern und muss weder auf der Webseite veröffentlicht werden noch Dritten (mit Ausnahme der Aufsichtsbehörden) in irgendeiner Form zugänglich gemacht werden.

Das Verarbeitungsverzeichnis dient einerseits der **Dokumentation** sowie andererseits als **Nachweis** dafür, dass die Vorgaben der DSGVO durch den Verantwortlichen auch eingehalten werden.

Somit ist jeder Online-Händler verpflichtet, ein solches Verzeichnis anzulegen und zu pflegen, um seiner Dokumentationspflicht nachzukommen. Die Dokumentationspflicht wird dann relevant, sobald eine Aufsichtsbehörde die Offenlegung des Verarbeitungsverzeichnisses verlangt. Online-Händler tun also gut daran, dieses Verzeichnis mit großer Sorgfalt zu erstellen und aktuell zu halten.

**Welche Bereiche sind betroffen?**

Das Verarbeitungsverzeichnis betrifft sämtliche ganz oder **teilweise automatisierte** Verarbeitungen sowie **nichtautomatisierte Verarbeitungen** personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Für **jede einzelne** Verarbeitungstätigkeit ist eine Beschreibung nach Maßgabe des Art. 30 DSGVO anzufertigen. Dabei können die konkreten Bereiche, in denen personenbezogene Daten in der beschriebenen Weise verarbeitet werden, je nach Branche bzw. Unternehmen variieren.

Die für den Online-Handel besonders relevante Verarbeitungstätigkeiten fallen beispielsweise in folgenden Bereichen an:

- Lohnabrechnung für Beschäftigte
- Abwicklung von Bestellungen
- Werbung
- Lieferung von Waren
- Zahlungsabwicklung
- Bonitätsprüfung
- Analyse des Nutzerverhaltens

**Tipp für Mandanten der IT-Recht Kanzlei:**

Sie können in Ihrem Online-Mandantenportal Ihr Verarbeitungsverzeichnis schnell und einfach selbst erstellen!

## 3. Tipp: Cookie-Consent-Tool

Spätestens nach der Entscheidung des EuGH (Urt. v. 01.10.2019, Az. C-673/17) hat sich im Bereich Einwilligungen einiges getan. Nach diesem wegweisenden Urteil ist für den Einsatz von Cookies, die für den Betrieb einer Website **nicht zwingend technisch erforderlich** sind, immer eine ausdrückliche Nutzereinwilligung für jedes einzelne Cookie notwendig (der BGH hat dies in seiner zeitlich nachgelagerten Entscheidung bestätigt).

Die Notwendigkeit einer ausdrücklichen Nutzereinwilligung für jedes einzelne Cookie gilt auch unabhängig davon, ob durch das jeweilige Cookie personenbezogene Daten verarbeitet werden oder nicht. Von dieser Problematik betroffen sind Webseitenbetreiber (und damit auch Online-Händler, die einen eigenen Online-Shop betreiben) insbesondere dann, wenn diese cookiebasierte **Tracking-, Analyse- und sonstige Marketingtools** auf ihren Seiten implementiert haben.

Für die Wirksamkeit solcher Cookie-Einwilligungen ist erforderlich, dass der Seitenbesucher über die Funktionsweise jedes Cookies bei der Einwilligungserteilung umfänglich informiert wird.

Cookie-Banner, die **lediglich allgemein** über den Einsatz von Cookies informieren und sich über eine Bestätigungs-Schaltfläche (etwa mit der Aufschrift „OK“) wegklicken lassen, genügen den Anforderungen an einer wirksam erteilten Einwilligung nicht. Weitergehende Informationen, weshalb derartige Banner nicht die Voraussetzungen für eine wirksame Einwilligung erfüllen, können Sie in diesem Beitrag nachlesen.

### a) Was Seitenbetreiber tun müssen

Nach dem EuGH-Urteil und der Entscheidung des BGH-Urteils (Urt. v. 28.05.2020, Az.: I ZR 7/16) steht fest: Alle Seitenbetreiber dürfen Cookies, die für den Betrieb einer Webseite nicht zwingend erforderlich sind, nur nach entsprechender **aktiver Nutzereinwilligung** setzen.

Seitenbetreiber, die technisch nicht erforderliche Cookies setzen, müssen auf ihren Präsenzen zwingend rechtskonforme Cookie-Einwilligungslösungen implementieren. Diese müssen technisch sicherstellen, dass

- für jede cookie-basierte und nicht technisch erforderliche Anwendung eine individuelle Cookie-Einwilligung abgefragt wird,
- Cookies dieser Anwendungen erst dann gesetzt werden, wenn der Nutzer hierin jeweils individuell eingewilligt hat,
- Nutzer ihre Einwilligungen über entsprechende Optionen jederzeit wieder widerrufen können und dadurch die Cookie-Setzung wieder gestoppt wird.

Für cookie-basierte Verarbeitungen haben sich sog. „Cookie-Consent-Tools“ durchgesetzt, welche eine rechtssichere Einwilligung der Nutzer einholen (können).

Seitenbetreiber, die bereits ein rechtssicheres Cookie-Consent Tool auf ihren Präsenzen eingerichtet haben, müssen nichts weiter unternehmen. Seitenbetreiber, die bisher kein oder kein hinreichendes Cookie-Consent-Tool verwenden, müssen ein solches unbedingt einbinden, um sich vor teuren Konsequenzen zu schützen.

## b) Anforderungen an ein Cookie-Consent-Tool

Cookie-Consent-Tools müssen nur dort eingesetzt werden, wo der Betreiber die Cookie-Setzung eigenständig kontrollieren kann, also beispielsweise auf der eigenen Website.

Die Pflicht gilt insofern **nicht** auf Handelsplattformen (eBay, Amazon, etsy und Co.) und in sozialen Netzwerken (Facebook, Instagram und Co.).

**Hinweis:** Welche Cookie Consent-Tools für Shopsysteme genügen überhaupt den rechtlichen Anforderungen? Unser Test klärt hier auf. Vergessen Sie zudem nicht, dass das verwendete Cookie-Consent Tool auch in Ihrer **Datenschutzerklärung** erwähnt werden muss!

Als vorgeschaltete Abfrage werden Cookie-Consent-Tools beim erstmaligen Aufruf einer Website angezeigt und bieten dem Betroffenen die Möglichkeit einer Einwilligungserteilung. Damit über derartige Banner und Tools datenschutzkonforme Einwilligungen eingeholt werden können, sind allerdings besondere technische Einstellungen und Ausgestaltungen unbedingt zu beachten.

**Tipp für Mandanten der IT-Recht Kanzlei:**

Mandanten der IT-Recht Kanzlei können diverse Cookie-Consent-Tools in plattformunabhängigen Varianten oder für bestimmte Hosting-Umgebungen entweder gänzlich kostenlos oder stark vergünstigt beziehen. Die IT-Recht Kanzlei stellt unter anderem in Kooperation mit PRIVE ein kostenloses Cookie-Consent-Tool zur Einbindung in Shops und auf Webseiten zur Verfügung. Das Cookie Consent Tool ist nicht auf eine bestimmte Anzahl von Seitenaufrufen pro Monat oder eine Höchstzahl an verwendeten Unterseiten beschränkt. Weitere Informationen erhalten Sie in Ihrem Mandantenportal

# 4. Tipp: Auftragsverarbeitungsverträge

Beauftragt ein Online-Händler einen Dienstleister für ihn personenbezogene Daten in einer gewissen Art und Weise zu verarbeiten, ruft dies regelmäßig die Notwendigkeit zum Abschluss eines sog. Auftragsverarbeitungsvertrags (kurz AV) auf den Plan.

Dieser Auftragsverarbeitungsvertrag muss den umfangreichen Anforderungen des Art. 28 DSGVO genügen. Auch der Vertragspartner - der Auftragsverarbeiter - ist in diesem Zusammenhang verpflichtet, ein Verzeichnis über seine Verarbeitungstätigkeiten zu führen. Das Instrument der

Auftragsverarbeitung führt somit zu einer ganzen Reihe an Pflichten - für beide Vertragsparteien.

Umso wichtiger ist die Frage, in welchen Fällen denn nun eine Auftragsverarbeitung vorliegt. Sind z.B. Transport- und Bezahldienstleister, die die meisten Online-Händler einschalten, sogenannte Auftragsverarbeiter, mit denen der Online-Händler einen Vertrag über die Auftragsverarbeitung schließen muss? Diese und weitere Fragen haben wir in unserem speziellen Beitrag für Sie beantwortet!

Liegt eine Auftragsverarbeitung vor, muss auch ein Auftragsverarbeitungsvertrag abgeschlossen werden. Dies ist in Art. 28 Abs. 3 DSGVO normiert. Danach verlangt **jedes auftragsgebundene Verarbeitungsverhältnis** den Abschluss eines Verarbeitungsvertrags mit dem Auftragsverarbeiter.

In diesem Vertrag sind Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festzulegen.

Der Auftragsverarbeitungsvertrag kann schriftlich oder elektronisch abgeschlossen werden. Ein solcher Vertrag kann je nach Unternehmung schnell sehr komplex werden. Der verantwortliche Online-Händler kann bei Verträgen zur Auftragsverarbeitung, die nicht den Vorgaben der DSGVO entsprechen, mit empfindlichen Bußgeldern belegt werden. Es ist somit sicherzustellen, dass beim Abschluss solcher Verträge alle Vorgaben der DSGVO einwandfrei umgesetzt werden.

**Tipp für Mandanten der IT-Recht Kanzlei:**

Sie können in Ihrem Online-Mandantenportal mit dem entsprechenden Muster einen Auftragsverarbeitungsvertrag schnell und einfach selbst erstellen!

## 5. Tipp: Auskunftsanspruch nach Art. 15 DSGVO (Antwortschreiben an Kunden)

Die DSGVO räumt einer natürlichen Person das Recht ein, zu erfahren, wer welche personenbezogenen Daten über sie gespeichert hat.

Das Auskunftsrecht wird nur **auf Antrag** gewährt. Ein bestimmtes Form- oder Begründungserfordernis besteht nicht. Nach Art. 12 DSGVO trifft den datenschutzrechtlich Verantwortlichen (= Online-Händler) die Pflicht, die Informationen in präziser, transparenter, verständlicher, leicht zugänglicher Form und in einer klaren und einfachen Sprache zu übermitteln.

Grundsätzlich können die zu erteilenden Informationen schriftlich oder in elektronischer Form erteilt werden. Stellt der Betroffene den Antrag auf Auskunft auf elektronischem Wege, muss auch die Auskunft in einem gängigen elektronischen Format erteilt werden. In zeitlicher Hinsicht sind dem Antragssteller die Informationen unverzüglich, jedenfalls aber **innerhalb eines Monats** nach Eingang des Antrags zur Verfügung zu stellen, Art. 12 Absatz 3 DSGVO. In komplexen Fällen kann diese Frist um zwei weitere Monate verlängert werden. Dies ist dem Betroffenen jedoch innerhalb eines Monats, unter Angaben von Gründen, mitzuteilen.

Doch welcher Inhalt hat eine korrekte Auskunft in Form eines Antwortschreibens? Der Online-Händler muss den Betroffenen darüber informieren, **was** er **zu welchem Zweck** mit dessen personenbezogenen Daten macht. Der Betroffene hat auch ein Recht darauf, informiert zu werden, **an wen** eine Übermittlung der personenbezogenen Daten durch den Online-Händler erfolgt und **zu welchen Zwecken** sie von Dritten weiterverarbeitet werden.

Er hat auch ein Auskunftsrecht über die Weiterleitung seiner personenbezogenen Daten an Drittländer, wobei in der Praxis vor allem eine Weiterleitung von Daten in die USA relevant ist. Der Auskunftsanspruch nach Art. 15 DSGVO erfasst des Weiteren auch Informationen bspw. über die Art der verarbeiteten Daten, die Speicherdauer sowie die Herkunft der Daten.

**Tipp für Mandanten der IT-Recht Kanzlei:**

Der Auskunftsanspruch hält in der Praxis für Online-Händler den ein oder anderen juristischen Fallstrick bereit. Aus diesem Grund stellt die IT-Recht Kanzlei ihren Mandanten im Bereich der datenschutzrechtlichen Auskunftserteilung zahlreiche Muster für Antwortschreiben zur Verfügung!

## 6. Tipp: Was tun bei einer Datenschutz-Panne?

Art. 4 Nr. 12 DSGVO definiert die „Datenpanne“ als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur **unbefugten Offenlegung** von beziehungsweise zum **unbefugten Zugang** zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Datenpannen sind Verletzungen des Schutzes personenbezogener Daten, die durch ein Versagen oder eine unzureichende Implementierung von angemessenen technischen und organisatorischen Maßnahmen entstehen. Im Internet bestehen derartige Verletzungen insbesondere darin, dass Daten von einem Verantwortlichen so gespeichert und verfügbar gehalten werden, dass Dritte ungehindert auf diese zugreifen können. Auch denkbar sind aber gezielte Hacking-Angriffe auf Shop-Systeme. Die Auswirkungen drohen massiv zu sein, wenn sensible private Informationen einem weltweiten Publikum zugänglich gemacht und so Missbrauch Tür und Tor geöffnet wird.

Datenpannen können sich vor allem rund um einen Online-Shop ereignen. Dort entstehen Datenpannen hauptsächlich durch Verarbeitungssituationen, die nicht von einer Rechtsgrundlage des Art. 6 DSGVO (bzw. bei sensiblen Daten zusätzlich des Art. 9 DSGVO) getragen werden oder durch unrechtmäßige Zugriffe erfolgen.

Doch wie muss auf eine Datenpanne reagiert werden und welche Schritte müssen zwingend durchlaufen werden? Zunächst muss die Datenpanne so behoben werden, dass von Ihr keine Gefahren mehr für den Schutz der betroffenen personenbezogenen Daten ausgehen.

Nach Art. 33 DSGVO sind Verantwortliche weiter dazu verpflichtet, **innerhalb von 72 Stunden nach Kenntniserlangung** von der Datenpanne die für sie zuständige Aufsichtsbehörde über die Verletzung zu **benachrichtigen**.

Dies gilt jedoch nur, sofern die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Neben einer Dokumentation der Datenpanne ist gegebenenfalls eine **Benachrichtigung des/der Betroffenen** vonnöten.

**Tipp für Mandanten der IT-Recht Kanzlei:**

Sie können auf dieser Seite ein Muster finden, welches Sie im Falle möglicher Datenpanne gegenüber Ihren Kunden verwenden können. Zudem finden Sie hier eine Musterbenachrichtigung an die Aufsichtsbehörde für den Fall einer festgestellten Datenschutzpanne.

## 7. Schutz vor Abmahnungen: Wir pflegen Ihre Rechtstexte

Sie erhalten die anwaltlich abgesicherte Datenschutzerklärung (inkl. Impressum) ab mtl. nur 5,90 Euro. In diesem Betrag inbegriffen ist ein juristischer Pflegeservice, der für eine dauerhafte Rechtssicherheit der Rechtstexte sorgt.

Interessierte Webseitenbetreiber können sich hier über unsere Datenschutzerklärung für Webseiten informieren.

Tipp: Sie möchten über Ihre Website nicht nur Ihr Unternehmen präsentieren, sondern auch direkt über einen Onlineshop verkaufen? In dem Fall macht dieses Schutzpaket für Sie Sinn.

Autor:
**RA Jan Lennart Müller**
Rechtsanwalt