

von **RA Alex Goldberg**, Rechtsanwalt

Gastbeitrag von PRIVE: Die 7 größten DSGVO-Fehlerquellen für Online-Shop-Betreiber

Seit Einführung der DSGVO im Mai 2018 halten die neuen Datenschutzvorschriften Unternehmen in der ganzen EU auf Trab. Erfahren Sie hier von unserem Gastautor RA Alex Goldberg von PRIVE, welche die 7 größten Fehlerquellen für Online-Shop-Betreiber sind und wie Sie teure Datenschutzverstöße vermeiden.

1. Fehlerquelle: Einwilligung für Cookies & Co.

Kein Online-Shop ohne Cookies und Plugins: Warenkorb oder Wunschliste würden ohne nicht funktionieren. Um solche technisch notwendigen Cookies einzusetzen, benötigen Sie in der Regel keine Einwilligung.

Sie müssen aber transparent und vollständig darüber informieren. Für das Marketing sind aber in der Regel noch ganz andere Cookies wichtig, nämlich solche, mit denen sich das Verhalten der Online-Shop-Besucher nachvollziehen und Auswerten lässt – die sog. Tracking- und Analyse-Cookies. Für den Einsatz dieser Cookies und ähnlicher Technologien wie z.B. Facebook Pixel muss jedoch eine Einwilligung eingeholt werden.

Werden solche Cookies ohne Einwilligung gesetzt oder vergleichbare Tracking-Technologien ohne Einwilligung angewendet, liegt ein Datenschutzverstoß vor und es droht ein Bußgeld.

Im Dezember 2020 verhängte die französische Datenschutzbehörde ein Bußgeld von insgesamt **60.000.000 Euro** gegen Google. Google hatte ohne Einwilligung Cookies zu Werbezwecken eingesetzt. Zudem wurden die Informationspflichten nicht erfüllt.

Jeder Online-Shop, der mit Cookies oder vergleichbaren Technologien das Besucherverhalten trackt, sollte daher über ein Consent-Tool verfügen, das die erforderlichen Einwilligungen der Shop-Besucher beim Betreten des Online-Shops abfragt und über Zweck, Speicherdauer und Rechtsgrundlage der eingesetzten Technologien informiert.

Als Mandant der IT-Recht Kanzlei München können Sie das [Consent-Tool von PRIVE mit bis zu 20.000 Sessions / Mo. kostenlos nutzen](#), um DSGVO-konform Einwilligungen für Cookies & Co einzuholen.

2. Fehlerquelle: Das Verarbeitungsverzeichnis

In einem Online-Shop finden zahlreiche spezifische Verarbeitungsvorgänge personenbezogener Daten statt.

Das beginnt beim Besuch des Online-Shops durch den Kunden, geht über die Merkzettel- und Warenkorb-Funktion, Bestellabwicklung, Rechnungsstellung und den Versand der Ware bis hin zu Retouren und Kundenbewertungen. Auch im Rahmen von Newslettern und Gewinnspielen werden Personendaten verarbeitet.

All diese Verarbeitungsvorgänge müssen als Verarbeitungstätigkeiten definiert und in einem Verarbeitungsverzeichnis geführt werden, das auf Verlangen der Datenschutzbehörde vorgelegt werden muss. Dazu müssen die einzelnen Verarbeitungsvorgänge inkl. Rechtsgrundlage, Zweck und Speicherdauer sowie die betroffenen Kategorien von Daten und Personen dokumentiert werden.

Wird das Verarbeitungsverzeichnis nur unvollständig oder fehlerhaft geführt oder fehlt es sogar ganz, müssen Sie mit empfindlichen Strafen rechnen.

Die italienische Datenschutzbehörde hat im Juli 2021 aufgrund eines fehlenden Verarbeitungsverzeichnisses ein Bußgeld in Höhe von **30.000 Euro** gegen einen Anbieter verhängt.

Das Verarbeitungsverzeichnis bildet alle Prozesse Ihres Online-Shops im Zusammenhang mit personenbezogenen Daten ab. Es handelt sich daher um ein Kernstück Ihres Datenschutz-Managements. Verlangt die Datenschutzbehörde die Vorlage des Verzeichnisses, sollten Sie nicht mit leeren Händen oder notdürftigen Alibi-Lösungen dastehen.

Mit der **DSGVO-Komplettlösung PRIVE** können Sie den gesamten internen Datenschutz für Ihr Unternehmen und/oder Ihren Online-Shop organisieren. Für das Verarbeitungsverzeichnis bietet PRIVE ein Tool, in dem Sie nicht nur individuelle Verarbeitungstätigkeiten selbst erstellen, sondern auch auf einen **umfangreichen Katalog bereits vollständig hinterlegter typischer Verarbeitungstätigkeiten für Online-Shops** zurückgreifen können, die ebenfalls bei Bedarf individualisiert werden können. So sparen Sie enorm viel Zeit bei der Erstellung und haben bei Bedarf **mit einem Klick ein übersichtliches PDF-Dokument** für die Datenschutzbehörde parat.

[Als Mandant der IT-Recht Kanzlei München erhalten Sie die spezielle Version PRIVE für Online-Shops für nur 29,00€ zzgl. USt. / Mo. im Jahrespaket](#)

3. Fehlerquelle: AV-Verträge

Als Online-Shop nehmen Sie zahlreiche Dienste in Anspruch, um Ihren Kunden ein rundum gelungenes Einkaufserlebnis bieten zu können. Viele dieser Dienste verarbeiten personenbezogene Daten Ihrer Kunden in Ihrem Auftrag. Es liegt dann ein sog. Auftragsverarbeitungs-Verhältnis vor. Das trifft z.B. auf Ihren Webhoster und viele von Ihnen eingesetzte Tracking- und Analyse-Tools auf Ihrer Webseite zu. Mit diesen Dienstleistern müssen Sie **Verträge über die Auftragsverarbeitung (AV-Verträge)** schließen. Ein AV-Vertrag soll sicherstellen, dass der Auftragnehmer sich bei der Verarbeitung der Daten an die Weisungen des Auftraggebers und das vereinbarte Datenschutzniveau hält. Viele Dienstleister bieten solche Verträge von sich aus an – aber längst nicht alle.

Gerade Betreiber kleiner Webagenturen sind sich oft nicht bewusst, dass auch sie Auftragsverarbeiter sein können – z.B. wenn sie das Webhosting als Reseller übernehmen oder Newsletter-Kampagnen für andere durchführen. Das Problem: Für den Abschluss des vorgeschriebenen AV-Vertrages sind beide Parteien zuständig – fehlt also ein Vertrag, wird dafür nicht nur Ihr Dienstleister, sondern werden auch Sie als Shop-Betreiber in die Verantwortung genommen.

Im Jahr 2020 verhängte die brandenburgische Datenschutzbehörde ein Bußgeld in Höhe von **50.000 Euro** gegen ein nicht näher benanntes Unternehmen wegen eines fehlenden AV-Vertrages und des Verstoßes gegen das Transparenzgebot.

Prüfen Sie daher Ihre Dienstleister genau: Verarbeiten einzelne Dienstleister Daten Ihrer Kunden oder Mitarbeiter, ohne dass ein AV-Vertrag geschlossen wurde? Wenn ja, gehen Sie auf den Dienstleister zu und wirken Sie auf den Abschluss eines AV-Vertrages hin. Dokumentieren Sie alle AV-Verträge so, dass Sie diese im Zweifel stets der Datenschutzbehörde vorlegen können.

Mit der [DSGVO-Komplettlösung PRIVE](#) können Sie sämtliche AV-Verträge direkt **online abschließen – mit digitaler Signatur**. Da meist der Dienstleister den Vertrag zur Verfügung stellt, können Sie aber auch außerhalb von PRIVE geschlossene AV-Verträge hochladen und so ebenfalls **dokumentieren**.

4. Fehlerquelle: Mitarbeiter-Verpflichtungen

Auch Ihre Mitarbeiter müssen sich an die geltenden datenschutzrechtlichen Vorschriften halten. Was vielen Shop-Betreibern nicht bewusst ist:

Als Verantwortlicher müssen Sie Ihre Mitarbeiter darüber informieren, und zwar so, dass Sie im Zweifel nachweisen können, dass Sie dieser Pflicht nachgekommen sind. Am besten eignen sich hierfür sogenannte **Mitarbeiterverpflichtung auf den Datenschutz**. Diese sollten neben allgemeinen Hinweisen zur Einhaltung des Datenschutzes auch Auszüge der wichtigsten Vorschriften enthalten.

Wenn Sie bei einer Untersuchung der Datenschutzbehörde nicht nachweisen können, dass Sie Ihre Mitarbeiter für den Datenschutz sensibilisiert haben, kann das drohende Bußgelder in die Höhe treiben.

Um später nachweisen zu können, dass Ihre Mitarbeiter die Verpflichtungen erhalten haben, und zur Sensibilisierung der Mitarbeiter empfiehlt es sich, die Verpflichtung von den Mitarbeitern unterschreiben zu lassen und zu dokumentieren.

Die [DSGVO-Komplettlösung PRIVE](#) beinhaltet rechtssichere **Mitarbeiterverpflichtungen auf den Datenschutz sowie Home-Office-Vereinbarungen**. Diese können Ihre Mitarbeiter direkt online unterzeichnen.

5. Fehlerquelle: Technische und Organisatorische Maßnahmen (TOMs)

In der DSGVO ist an vielen Stellen von **technischen und organisatorischen Maßnahmen** die Rede. Gemeint sind alle Maßnahmen, die zum Schutz personenbezogener Daten beitragen und die insbesondere den Grundsätzen „data protection by design“ und „data protection by default“ (Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen) Rechnung tragen sollen. Diese Maßnahmen können beispielsweise darin bestehen, dass weniger Daten erfasst werden, dass die Daten schnellstmöglich pseudonymisiert werden oder dass mehr Transparenz und Überwachungsmöglichkeiten für die Betroffenen geschaffen werden. Es zählen jedoch auch Maßnahmen zu den TOMs, die den Zugriff von außen verhindern sollen.

Als Online-Shop-Betreiber kommen Sie mit zahlreichen Daten Ihrer Kunden in Berührung: Wohnanschriften, Geburtsdaten, Zahlungsdaten, Kaufverhalten und vielen mehr. All diese Daten werden auf verschiedenste Art und Weise verarbeitet und weitergegeben (z.B. an Zahlungsdienstleister, Versanddienstleister, Fulfillment-Dienstleister etc.) und müssen dabei entsprechend geschützt werden – durch TOMs. Wie gut personenbezogene Daten in Ihrem Unternehmen geschützt sind, wird letztlich an Ihren getroffenen TOMs gemessen.

2020 hat die norwegische Datenschutzbehörde der Stadtverwaltung Bergen wegen unzureichender technischer und organisatorischer Maßnahmen bei einer Schul-App ein Bußgeld von umgerechnet **rund 275.000 Euro** auferlegt.

Als Shop-Betreiber sollten Sie daher geeignete technische und organisatorische Maßnahmen festlegen und dokumentieren.

Bei [PRIVE](#) finden Sie einen eigenen Bereich, der auch **zahlreiche Vorschläge für gängige TOMs** enthält und Ihnen bei der **Dokumentation und Übersicht** über Ihre eigenen TOMs hilft. Wenn die Behörde anfragt, können Sie mit einem Klick eine rechtssichere TOM-Liste als PDF exportieren und der Behörde vorlegen.

6. Fehlerquelle: Betroffenenanfragen

Als Shop-Betreiber hatten Sie vielleicht auch schon Kunden, die nach einer Bestellung Ihre Daten löschen lassen wollten oder die wissen wollten, welche Daten Sie zur Person gespeichert haben.

Wenn Kunden oder andere Personen sich bei Ihnen melden und Ihre Datenschutz-Rechte geltend machen wollen, spricht man von einer **Betroffenenanfrage**.

Da diese vermehrt dann gestellt werden, wenn schon etwas schiefgelaufen ist, z.B. ein Kunde sich beschwert hat, und die Anfragen manchmal etwas merkwürdig anmuten, werden sie oft nicht ernst genommen. Ein böser Fehler: Denn für die Beantwortung von Betroffenenanfragen – gerechtfertigt oder nicht – setzt die DSGVO eine **Frist von einem Monat**.

Werden solche Anfragen nicht beantwortet, können die Betroffenen sich bei der Datenschutzbehörde über Sie beschweren – **odersogar direkt klagen**.

Im Falle einer Beschwerde bei der Datenschutzbehörde muss diese tätig werden – egal, wie sehr die Beschwerde möglicherweise an den Haaren herbeigezogen sein mag.

Die griechische Datenschutzbehörde hat im Januar 2022 aufgrund einer verspäteten Beantwortung einer einzigen Betroffenenanfrage direkt ein Bußgeld in Höhe von **1.000 Euro** verhängt.

Wird die Frist für die Erteilung einer Auskunft versäumt, kann der Betroffene zudem **ohne vorherige Ankündigung Klage erheben**.

Damit Sie möglichst gar nicht erst in die Situation kommen, sich vor der Datenschutzbehörde oder einem Richter verantworten zu müssen, sollten Sie Betroffenenanfragen immer sorgfältig dokumentieren und rechtzeitig beantworten.

Die wichtigsten Punkte sind:

- Anfrage ernst nehmen
- den Eingang sofort bestätigen und Beantwortung spätestens innerhalb eines Monats zusichern
- Identität und Berechtigung überprüfen, und abschließend
- korrekt auf die Anfrage reagieren – entweder durch deren Stattgabe und entsprechende Mitteilung oder durch vollständige oder teilweise Ablehnung mit entsprechender Begründung.

Bei PRIVE steht Ihnen ein **Tool zur Verwaltung, Dokumentation und Beantwortung von Betroffenenanfragen** zur Verfügung - **mit automatischem Antwortgenerator und Fristenverwaltung**. Sie finden außerdem zahlreiche nützliche Tipps und Informationen zum Umgang mit Betroffenenanfragen. Falls Sie einmal gar nicht mehr weiterwissen sollten, können Sie außerdem eine individuelle Beratung mit einem Datenschutzexperten hinzubuchen.

[Mandanten der IT-Recht Kanzlei München erhalten die spezielle Version der DSGVO-Komplettlösung PRIVE für Online-Shops für nur 29,00€ zzgl. USt. / Mo. im Jahrespaket](#)

7. Fehlerquelle: Datenpannen

Auch dem besten Shop-Betreiber kann es mal passieren: Ein Mitarbeiter verlegt einen Dienstlaptop, ein Hacker stiehlt Daten Ihrer Kunden oder dem Shop-System fehlt ein wichtiges Sicherheitsupdate.

Datenpannen sind nicht nur für die Betroffenen unerfreulich, sie sind auch hochgradig unangenehm für den Verantwortlichen. Lieber alles unter den Teppich kehren? Besser nicht.

Denn laut DSGVO sind Sie verpflichtet, bestimmte **Datenpannen binnen 72 Stunden bei der Datenschutzbehörde anzuzeigen**. In manchen Fällen müssen zusätzlich die **Betroffenen informiert werden**.

Sie müssen also schnell und besonnen handeln, wenn es zum Ernstfall kommt, um sich nicht noch weitere Schwierigkeiten einzuhandeln.

Einem Anbieter aus Hamburg wurde im Jahr 2020 ein Bußgeld in Höhe von **20.000 Euro** auferlegt, da eine Datenpanne verspätet bei der Datenschutzbehörde angezeigt und die Betroffenen nicht über die Panne informiert hatte.

Auch Datenpannen sollten Sie gründlich dokumentieren. Zusätzlich müssen Sie schnell herausfinden, ob bereits ein Schaden entstanden ist, wie groß der Schaden ist und ob weiterhin ein Risiko besteht.

Schnellstmöglich müssen Maßnahmen getroffen werden, um weiteren Schaden möglichst zu verhindern und den entstandenen Schaden zu begrenzen. Treffen Sie am besten schon innerhalb der ersten 24 Stunden die Entscheidung, ob Sie den Vorfall der Datenschutzbehörde melden müssen. Falls Sie entscheiden, den Vorfall nicht zu melden, dokumentieren Sie die Gründe hierfür.

PRIVE bietet Ihnen ein **Tool zur Verwaltung, Dokumentation und Bearbeitung von Datenpannen zur Verfügung – mit Fristenverwaltung und Generator für rechtssichere Behördenmeldungen**. Sie finden außerdem hilfreiche Tipps und können bei Bedarf eine Beratung in Anspruch nehmen.

[Mandanten der IT-Recht Kanzlei München erhalten die spezielle Version der DSGVO-Komplettlösung PRIVE für Online-Shops für nur 29,00€ zzgl. USt. / Mo. im Jahrespaket](#)

8. Fazit

Shop-Betreiber sind beim Datenschutz zahlreichen Risiken ausgesetzt. Ein gut funktionierendes und auf die besonderen Anforderungen eines Online-Shops angepasstes Datenschutz-Management für die unternehmensinternen Prozesse und Abläufe ist daher unerlässlich. Sollte dennoch einmal etwas passieren, wird der Einsatz eines Datenschutz-Management-Systems von den Behörden bei der Bemessung von Bußgeldern berücksichtigt. Allein der Einsatz eines solches Systems führt also zu einer Reduzierung etwaiger Strafzahlungen.

Sichern Sie sich die DSGVO-Komplettlösung PRIVE für Online-Shops mit speziell angepassten Inhalten, Vorlagen und Dokumenten für Online-Shop-Betreiber. [Mandanten der IT-Recht Kanzlei zahlen nur 29,00€ zzgl. USt. / Mo. im Jahrespaket](#)

Weitere Details zu den Sonderkonditionen von PRIVE für Mandanten der IT-Recht Kanzlei stellen wir gerne [hier](#) bereit.

Autor:

RA Alex Goldberg, Rechtsanwalt