Newsletter Datenschutz
Ausgabe 08 | 2017

AdOrga Solutions

# Datenschutz *Now!*

## Die Mandatenzeitung von AdOrga Solutions

Liebe Leserin, lieber Leser,

Kommunikation ist alles, so sagt man. Aber ohne richtigen Datenschutz geht es nicht. In dieser Ausgabe lesen Sie, worauf Sie achten müssen, wenn Sie Mail-Verteiler verwenden. Zudem erfahren Sie, warum auch bei Messenger-Programmen die Gefahr besteht, dass es zu einer Rufschädigung kommt.

Informieren Sie sich deshalb immer genau, wie es zum Beispiel bei Online-Anbietern um den Datenschutz steht. Bei Online-Diensten hilft ein Blick in die Datenschutzerklärung. Diese Ausgabe gibt Tipps, wie die Lektüre der Datenschutzerklärung einfacher fällt. Außerdem: Wissen Sie, welche Daten welchen Schutz benötigen? Hinweise dazu liefern die letzte Seite und der Wissenstest.

Ich wünsche Ihnen viel Spaß beim Lesen!
*Regina Mühlich*
*Ihre Datenschutzbeauftragte*

## Ärger mit E-Mail-Verteilern

**Praktikanten passiert es, erfahrenen Mitarbeitern allerdings auch: Eine größere Zahl von Adressaten soll parallel eine inhaltlich identische Mail erhalten. Der Versand erfolgt versehentlich so, dass jeder Empfänger alle anderen Adressaten sehen kann. Ein klarer Verstoß gegen den Datenschutz ! Manchmal verhängt die Datenschutzaufsicht auch ein Bußgeld gegen den "Täter". Lesen Sie, wie sich solche Pannen leicht vermeiden lassen!**

### Erst denken, dann klicken!

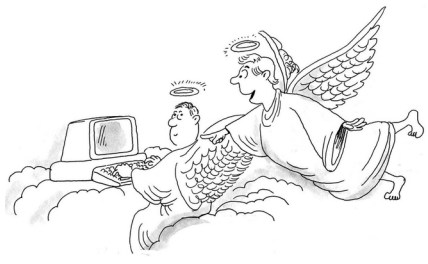
Wie so oft sollte es schnell gehen. Der Kunden-Newsletter war diesen Monat sowieso schon spät dran. Also schnell einen früheren Text für die Mail an die Kunden herüberkopiert, ihn inhaltlich leicht angepasst, den Newsletter angehängt und dann hinaus damit!

Schon nach wenigen Minuten kam der erste Anruf. Ein Kunde war stocksauer und beschwerte sich: "Wie kann es sein, dass auch alle anderen Newsletter-Empfänger sehen können, dass ich den Newsletter beziehe?" Die ehrliche Antwort wäre gewesen: Die Aushilfe hat aus den drei Möglichkeiten der Adressierung leider die falsche ausgewählt und mit dem Cc-Feld gearbeitet!

### Drei Varianten des Mailversands

Wenn eine Mail an viele Adressaten zugleich gehen soll, gibt es drei Varianten:

**Variante 1**: Alle Empfänger werden in das An-Feld eingetragen.
**Variante 2:** In das An-Feld schreibt man die eigene Mail-Adresse. Die eigentlichen Adressaten kommen in das Cc-Feld.
**Variante 3:** Wieder schreibt man in das An-Feld die eigene Mail-Adresse. Die eigentlichen Adressaten kommen in das Bcc-Feld.



"Do we use CC or BCC to answer the prayer requests?"

*Im Zweifelsfall ist Bcc immer die bessere Variante. Geht es um große Verteiler, bei denen die einzelnen Empfänger nicht erkennbar sein dürfen, ist es die einzige Lösung.*

### Im Normalfall immer nur Bcc nehmen!

Dass Variante 1 nicht geht, war auch der Aushilfe klar. Hier sieht jeder Empfänger auch alle anderen Empfänger, das wusste sie. Allerdings meinte sie, dass Variante 2 und Variante 3 irgendwie dasselbe sind. Ein großer Irrtum! Bei Variante 2 kann jeder Empfänger die vollständigen Adressen aller anderen Empfänger im Cc-Feld sehen. Bei Variante 3 sieht ein Empfänger die Adressen der anderen Empfänger im Bcc-Feld dagegen gerade nicht!

### Kopie und Blindkopie: zwei verschiedene Dinge!

Wie das? Des Rätsels Lösung ist einfach. Cc (also Variante 2) bedeutet "für alle sichtbare Kopie", Bcc (also Variante 3) heißt dagegen "Blindkopie, für die anderen Empfänger nicht sichtbar". Damit ist klar: Wer den Datenschutz beachtet, verwendet in solchen Fällen immer Variante 3 (Bcc) und nie Variante 2 (Cc)!

### Bußgeld für Mitarbeiter persönlich

Einfach nur blöd gelaufen und mit einem "Tut mir leid!" für die Aushilfe erledigt? Leider nein. Mehrere Aufsichtsbehörden für den Datenschutz (unter anderem in Bayern) haben in solchen Fällen auch schon gegen Mitarbeiter persönlich Bußgelder von einigen 100 Euro verhängt. Die Rufschädigung für das Unternehmen kommt hinzu. Sie ist oft erheblich.

# Tipps zur Prüfung einer Datenschutzerklärung

**Was macht der Betreiber der Webseite eigentlich mit meinen Daten? Die Antwort sollten Sie in der Datenschutzerklärung finden. Doch wie verschafft man sich da eine Übersicht angesichts oft langer Texte?**

### Wer liest das schon?

Es erscheint paradox: Datenschützer pochen darauf, dass es bei Internetauftritten, Online-Shops und anderen Online-Diensten eine Datenschutzerklärung gibt. Rechtlich gefordert wird dies im sogenannten Telemediengesetz (TMG). Wie Umfragen unter Internetnutzern zeigen, werden diese Datenschutzerklärungen aber kaum gelesen.

### Wichtige Informationen

Dabei sind in den Datenschutzerklärungen wichtige Informationen enthalten: Sie können dort erfahren, welche personenbezogenen Daten der Anbieter erhebt, zu welchem Zweck er sie erhebt, ob er Cookies einsetzt, an wen der Anbieter die Daten wozu weitergibt, welche Analyseprogramme (wie Google Analytics) im Einsatz sind, was getan wird, um Ihre Daten zu schützen, und an wen Sie sich bei Fragen zum Datenschutz bei diesem Unternehmen wenden können.

### Viele Webseiten bieten eine Zusammenfassung

Da viele Datenschutzerklärungen sehr lang erscheinen und die meisten Internetnutzer keine rechte Freude an juristisch anmutenden Texten haben, bleiben die Informationen zum Datenschutz meistens ungelesen. Doch es gibt Möglichkeiten, sich einen ersten Überblick zu verschaffen, ohne die langen Ausführungen lesen zu müssen.

Immer mehr Webseiten bieten neben der Datenschutzerklärung eine kurze Übersicht, die zwar rechtlich gesehen die Datenschutzerklärung nicht ersetzt, aber dem Nutzer eine große Hilfe sein kann. Bereits 2015 hat die vom Bundesministerium der Justiz und für Verbraucherschutz geleitete Plattform "Verbraucherschutz in der digitalen Welt" ein Muster für Datenschutzhinweise auf einer Seite vorgestellt, den sogenannten One-Pager. Auf vielen Webseiten wurde dies bereits umgesetzt. Sie finden das Muster unter http://ogy.de/muster-onepager.

Mit der Datenschutz-Grundverordnung (DSGVO/GDPR) kommt zudem die Verpflichtung, die Informationen zum Datenschutz verständlicher zu formulieren. So sagt die DSGVO: "Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen (...), die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln."

*Die Datenschutzerklärung ist eine wichtige Informationsquelle dazu, was Anbieter mit Daten tun*

### Auch Apps brauchen eine Datenschutzerklärung

Während die meisten Webseiten bereits über eine Datenschutzerklärung verfügen, haben mobile Applikationen, die Apps für Smartphones und Tablets, häufig noch keine entsprechende Privacy Policy, wie dies international genannt wird. Das ist nicht richtig so, auch wenn es auf den relativ kleinen Displays der mobilen Geräte meist noch weniger Vergnügen bereitet, Texte wie eine Datenschutzerklärung zu lesen.

Im Bereich der Smartphones und Tablets jedoch gibt es Werkzeuge, die bei der Prüfung des Datenschutzes helfen können. Meist werden diese Werkzeuge Datenschutz-Scanner oder Privacy-Scanner genannt. Sie finden diese Scanner entweder als eigene App im jeweiligen App-Store Ihres mobilen Betriebssystems (wie Google Play Store bei Android-Geräten) oder als Funktion einer App für mobile Sicherheit (Mobile Security App).

Die Privacy-Scanner-Apps oder -Funktionen untersuchen andere Apps auf die Nutzung und Weitergabe von Daten. Entsprechend helfen die Privacy-Scanner auch bei der Prüfung einer Datenschutzerklärung - sogar dann, wenn es noch gar keine Datenschutzerklärung für eine App gibt. Denn diese Scanner untersuchen die Datennutzung direkt und nicht nur die Erklärung zur App.

### Bald könnte es Datenschutzerklärer geben

In Zukunft wird es weitere Helfer geben, wenn es um die Prüfung der Datenschutzerklärung geht. Fast könnte man sagen, dass es bald Datenschutzerklärer geben wird. Es wird an sogenannten Privacy Bots gearbeitet. Bots sind virtuelle Assistenten. Die Privacy Bots sollen die Datenschutzerklärungen von Internetdiensten scannen und mit den Voreinstellungen des Nutzers abgleichen. Bestehende Wahlmöglichkeiten bei den Datenschutzeinstellungen sollen so leichter im Sinne des Anwenders genutzt werden. Die Privacy Bots sollen sich dabei nicht nur an einzelne Anbieter wie Facebook, Amazon oder Reiseportale richten, sondern für sämtliche Dienste nutzbar sein.

Das Ziel ist es, dass der Nutzer mithilfe des Bots nur einmal seine gewünschten Datenschutzstandards eingibt und der digitale Assistent daraufhin sämtliche Internetdienste prüft, Datenschutzeinstellungen darin anpasst oder Dienste nicht akzeptiert. Dem Nutzer bleibt es damit erspart, sich bei jedem Dienst mit den Datenschutzeinstellungen und Datenschutzerklärungen auseinandersetzen zu müssen.

Noch ist dies Zukunftsmusik, doch es wird nicht mehr lange dauern, bis es digitale Helfer gibt, die die Prüfung der Datenschutzerklärungen einfacher machen.

**Impressum**

**Redaktion:**
Regina Mühlich (V.i.S.d.P.)
Expertin für Datenschutz

**Anschrift:**
AdOrga Solutions
Drachenseestraße 15
D-81373 München
Tel.-Nr. +49 (0)89 411 726 - 35
E-Mail: info@adorgasolutions.de

# Rufschädigung in Facebook-Nachrichten

**In Facebook (aber natürlich auch in anderen sozialen Netzwerken!) schreibt so mancher Nachrichten, die er als Brief nie versenden würde. Wenn die Nachricht einen geschäftlichen Bezug hat, gibt es rasch Ärger. Das ist den meisten klar. Aber wenn es um private Dinge geht? Dass es auch dann Grenzen gibt, hat das Landgericht Düsseldorf kürzlich klargestellt.**

### Ein Darlehen unter "Freunden"

Ein Mann und eine Frau lernten sich über Facebook kennen. Rasch freundeten sie sich an. Im Mai/Juni 2016 war die Frau finanziell klamm. Gerne gab ihr der Mann ein Darlehen in Höhe von 3.050 Euro. Wie so oft hörte dann leider beim Geld die Freundschaft auf. Es gab Streitereien wegen der Rückzahlung.

Die Frau wollte dem Mann ihre finanzielle Lage erklären. Deshalb schickte sie ihm einen Kontoauszug als Screenshot. Der Kontoauszug zeigte einen Kontostand von minus 5.865,70 Euro. Als Dispo-Rahmen waren 6.000 Euro genannt, als noch "frei verfügbar" 134,30 Euro.

### Weitergabe eines Kontoauszugs

Kaum hatte der Mann den Screenshot auf dem Bildschirm, schickte er ihn an einen Herrn T. Dabei gab er folgende Erläuterungen zum Besten: "Kontostand Deiner Teilhaberin. Die ist pleite. Bei mir hat sie auch noch 3.000 Euro Schulden. Nur zur Info. Bei uns hat es richtig geknallt." Wie zu erwarten leitete Herr T. die Nachricht an die Frau weiter.

### Antrag auf einstweilige Verfügung beim Landgericht Düsseldorf

Den Inhalt der Nachricht fand die Frau überhaupt nicht lustig. Sie betreibt nämlich zusammen mit Herrn T. einen Friseursalon. Deshalb fürchtete sie geschäftliche Schwierigkeiten. Sofort schaltete sie daher einen Rechtsanwalt ein. Der forderte von dem Mann, der die Nachricht an Herrn T weitergegeben hatte, zwei Dinge:

1. Hören Sie auf, Daten über den Kontostand meiner Mandantin an Dritte weiterzugeben!
2. Hören Sie auf, gegenüber Dritten zu behaupten, meine Mandantin sei pleite!

Das war dem Mann reichlich egal. Er reagierte auf das Schreiben des Anwalts schlicht nicht. Daraufhin schaltete der Anwalt das zuständige Landgericht Düsseldorf ein und beantragte eine einstweilige Verfügung.

### Eine harte Entscheidung des Gerichts

Eine solche einstweilige Verfügung erließ das Landgericht tatsächlich. Der Inhalt lässt sich als "hammerhart" bezeichnen:

- Dem Mann wird untersagt, Daten über den Kontostand weiterzugeben. Außerdem wird ihm untersagt, zu behaupten, die Frau sei pleite.
- Für den Fall, dass er gegen diese Anordnungen verstößt, droht ihm das Gericht ein Ordnungsgeld in Höhe von bis zu 250.000 Euro an.
- Alternativ kann eine Ordnungshaft von bis zu sechs Monaten verhängt werden.

### "Die ist pleite" - was heißt das?

Die rechtliche Begründung des Gerichts ist für den geschäftlichen wie für den privaten Bereich gleichermaßen interessant. Das gilt vor allem für die Frage, ob man behaupten darf, dass jemand pleite sei. Dazu hält das Gericht fest:

*Vorsicht vor nicht zu beweisenden Behauptungen in sozialen Netzwerken!*

- Eine solche Aussage ist nicht nur eine Meinungsäußerung, sondern die Behauptung einer Tatsache. Übersetzt heißt eine solche Behauptung nämlich: Der, um den es geht, ist zahlungsunfähig, finanziell ruiniert oder bankrott.
- Eine solche Behauptung schädigt den Ruf. Wer sie aufstellt, muss deshalb beweisen, dass sie wahr ist.
- Kann er dies nicht, muss er die Behauptung unterlassen.

### Beweisen oder schweigen!

Daraus folgt: Bevor man behauptet, jemand sei pleite, sollte man erst einmal Unterlagen haben, die das beweisen. Die Maßstäbe sind dabei streng. Zwar befand sich das Konto der Frau, um die es hier ging, im Minus. Auch hatte sie zumindest auf diesem Konto kaum noch einen freien Kreditrahmen.

Aber all dies sagt im Zweifelsfall nichts. Denn möglicherweise hat sie noch ein anderes Konto, auf dem sie zusätzlichen Spielraum hat. Und vielleicht hat sie sogar so viel Bargeld, dass sie das Konto leicht ausgleichen könnte. All das sind Dinge, die ein Außenstehender normalerweise nicht weiß und daher nicht beurteilen kann. Deshalb lautet die Devise: Vorsicht mit solchen Behauptungen!

### Datenschutz "unter Privatleuten" oder nicht?

Klargestellt hat das Gericht auch, dass sich der Mann an die Datenschutzgesetze halten muss, wenn er eine solche Nachricht in sozialen Netzwerken schreibt.

Immer wieder hört man, die Datenschutzgesetze würden für "ausschließlich persönliche Tätigkeiten" nicht gelten. Das steht so tatsächlich in § 27 Abs. 1 Bundesdatenschutzgesetz. Allerdings: Wer in einem Netzwerk eine persönliche Nachricht erhält und sie an andere Personen weitergibt, der verlässt damit den rein persönlichen Bereich. Das gilt vor allem dann, wenn besonders vertrauliche Daten enthalten sind wie etwa Kontodaten. Ähnliches würde für medizinische Daten gelten. Wenn Nachrichten im geschäftlichen Bereich weitergegeben werden, ist das ohnehin nie eine "ausschließlich persönliche Tätigkeit".

Der Beschluss des Landgerichts ist im Internet leicht zu finden, wenn man das Aktenzeichen des Urteils 5 O 400/16 eingibt (Vorsicht: O wie "Opa", keine Null!).

# Woran erkenne ich den Schutzbedarf personenbezogener Daten?

**Personenbezogene Daten sind zu schützen, einige Daten haben sogar einen besonders hohen Schutzbedarf. Kann man das den Daten eigentlich ansehen?**

### Was bedeutet Personenbezug?

Im Datenschutz geht es um den Schutz personenbezogener Daten. Das klingt nach einer Binsenweisheit. Doch was hat es mit dem Personenbezug auf sich? Was versteht man unter personenbezogenen Daten? Im Bundesdatenschutzgesetz (BDSG) findet man dazu: "Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)."

In der Datenschutz-Grundverordnung (DSGVO/GDPR), die ab 25. Mai 2018 anzuwenden ist, steht: "Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann."

### Nicht alle Daten sind gleich

Bei den personenbezogenen Daten gibt es Unterschiede hinsichtlich des Schutzbedarfs. So besagt das BDSG: Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Diese Daten haben einen besonders hohen Schutzbedarf.

Auch die DSGVO nennt besondere Kategorien personenbezogener Daten. Dies sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Solche Daten dürfen nur unter ganz bestimmten Bedingungen verarbeitet werden (Artikel 9 DSGVO), entsprechend hoch ist ihr Schutzbedarf vor missbräuchlicher Nutzung.

### Es kommt auf die möglichen Folgen an

Damit die Verarbeiter der Daten noch genauer den Schutzbedarf und damit die Sensibilität der jeweiligen personenbezogenen Daten einschätzen können, haben die Aufsichtsbehörden für den Datenschutz ein sogenanntes Schutzstufen-Konzept entwickelt. Die Idee dahinter ist, dass die personenbezogenen Daten in einer höheren Schutzstufe einen entsprechend höheren Schutzbedarf haben. Die Schutzstufe hängt davon ab, welche Folgen es für die Betroffenen hätte, wenn die Daten missbraucht werden. Ein gängiges Schutzstufen-Konzept finden Sie unter http://bit.ly/2v5HxtG.

So werden zum Beispiel Daten über das Einkommen einer Person oder über Sozialleistungen, die eine Person erhält, eingestuft als Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte, also sein Ansehen negativ beeinflussen könnte. Entsprechend befindet sich die Schutzstufe für diese Daten bei einer Skala von A (sehr niedrig) bis E (sehr hoch) auf der Stufe C.

Weitere Beispiele zu Daten und ihrem Schutzbedarf finden Sie auch unter http://ogy.de/schutzstufen-2 (PDF).

## Kennen Sie den Schutzbedarf personenbezogener Daten? Machen Sie den Test.

**Frage: Der Beruf einer Person hat oftmals mit dem Ansehen zu tun. Deshalb hat der Beruf genauso wie der Kontostand einen mittleren Schutzbedarf. Stimmt das?**

**a) Ja, denn beide Daten können erfahrungsgemäß Einfluss auf das Ansehen einer Person haben.**
**b) Nein, denn der Beruf lässt sich im Gegensatz zum Kontostand häufig in öffentlichen Verzeichnissen nachsehen.**

Lösung: Die Antwort b) ist richtig. Berufsangaben findet man häufig in Branchenverzeichnissen, im Telefonbuch oder im Internet. Nach Schutzstufen-Konzept ist deshalb der Beruf eine Angabe mit niedrigem oder geringem Schutzbedarf.

**Frage: Personenbezogene Daten, die man im Internet findet, haben keinen Schutzbedarf, sie sind ja öffentlich. Stimmt das?**

**a) Nein. Zum einen dürfen Daten aus dem Internet nicht einfach verwendet werden, zum anderen können die Daten ungewollt (z.B. durch kriminelle Dritte) ins Internet gelangt sein.**
**b) Ja: Alles, was man im Internet findet, ist öffentlich zugänglich und damit frei zu verwenden.**

Lösung: Die Antwort a) ist richtig. Daten im Internet können nicht einfach genutzt werden, nur weil man sie über den Browser findet. Zum Beispiel dürfen Unternehmen Telefonnummern von Verbrauchern, die sich im Internet finden, nicht einfach für Werbeanrufe missbrauchen. Zudem passiert es leider häufig, dass Daten ungewollt im Internet landen, sogar Passwörter lassen sich ungeschützt im Internet aufspüren. Die Verwendung ist natürlich nicht erlaubt.