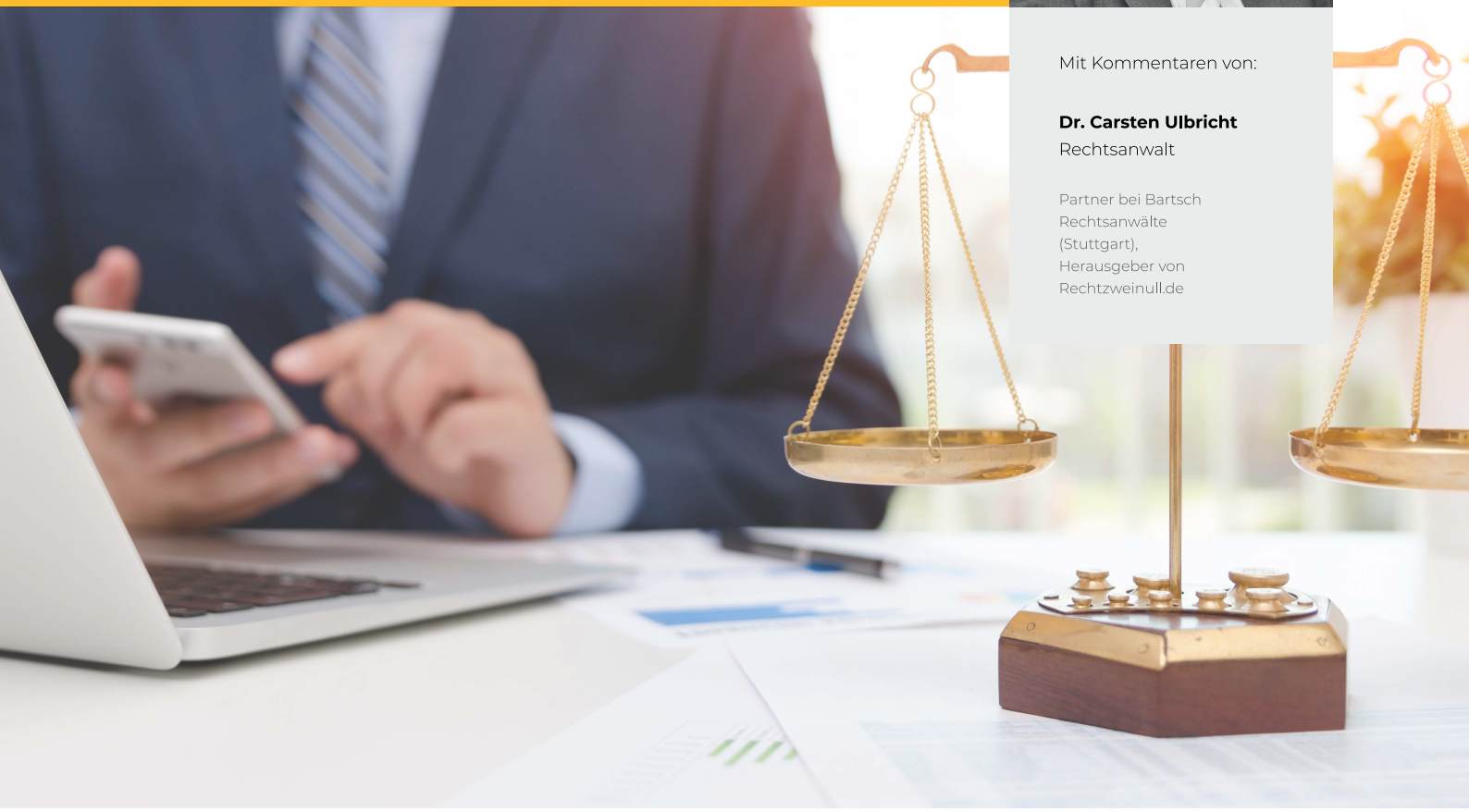
Wann und wie Sie personenbezogene Daten für Ihren Vertrieb nutzen dürfen und dabei rechtliche Risiken minimieren.

B2B-VERTRIEB UND KALTAKQUISE DSGVO-KONFORM GESTALTEN – SO GEHT´S

Mit Kommentaren von:

Dr. Carsten Ulbricht
Rechtsanwalt

Partner bei Bartsch Rechtsanwälte (Stuttgart), Herausgeber von Rechtzweinull.de



Inhaltsverzeichnis

1. PERSONENBEZOGENE DATEN UND DER VERBRAUCHERSCHUTZ

Mit Einführung der Datenschutz-Grundverordnung (DSGVO) hat sich die Europäische Union auf einen einheitlichen Datenschutz-Standard geeinigt, der nicht nur EU-Bürger, sondern auch alle, die sich innerhalb der Europäischen Union aufhalten, schützen soll. Die 99 Artikel regeln und regulieren den Umgang mit personenbezogene Daten. Seit am 25. Mai 2018 die Übergangsfrist endete, findet die DSGVO unmittelbare Anwendung.

Da sich die technischen Möglichkeiten von datenbasierten Algorithmen wie Gesichtserkennung, DNA-Analysen bis hin zur automatischen Ermittlung der politischen Orientierung aus Facebook Likes sehr schnell entwickelt haben, war eine Anpassung der Gesetzgebung an die neuen Gegebenheiten dringend nötig. Gleichzeitig findet eine Entwicklung statt, bei der wir über mobile Geräte und soziale Netzwerke immer mehr Informationen über uns preisgeben. Die aus dieser Kombination entstehenden Risiken sind vielen Verbrauchern so nicht bewusst. Deswegen dient die DSGVO primär dem Daten- und Verbraucherschutz, indem sie Unternehmen zu einem verantwortungsvollen Umgang mit Kundendaten zwingt.

Leider unterscheidet die DSGVO dabei jedoch nicht zwischen B2C- und B2B-Anwendungsfällen. Dadurch sind auch Geschäftspartner und deren Mitarbeiter wie Verbraucher zu betrachten und auch wie andere Verbraucher zu schützen. Zum Glück gibt es jedoch einige Ausnahmen und Erlaubnisvorbehalte, damit das wirtschaftliche Leben nicht komplett lahmgelegt wird. In vielen Fällen hilft die DSGVO sogar, da sie Unternehmen dazu zwingt, ihre vertriebs- und kundenorientierten Prozesse neu zu durchdenken und diese auf rechtskonforme und transparente Grundlagen aufzubauen.

Unglücklicherweise lässt die DSGVO aber auch viele Fragen offen oder zumindest in einer rechtlichen Grauzone. Bevor also nicht Gerichte in höchster Instanz (BGH / EuGH) die endgültige Auslegung der unklaren neuen Regelungen geklärt haben, können wir in vielen Fällen nur Tipps geben, wie man mögliche Risiken minimieren, aber leider nicht ganz ausschließen kann. Falls Sie dieses Dokument nach dem Jahr 2018 lesen, sollten Sie eventuelle Änderungen durch bis dahin veröffentlichte Urteile prüfen.

Ziel dieser Orientierungshilfe ist es, Ihnen die folgenden Fragen zu beantworten:

- Welche Daten sind in welcher Form betroffen?
- Wie kann ich meine bestehende Vertriebsarbeit optimal mit der DSGVO vereinen?
- Wo sind aktuell Schranken und Grenzen, auf die ich achten muss?
- Wie schaffe ich es, Chancen aus der neuen Gesetzeslage zu ziehen?

Am Ende des Dokuments möchten wir Ihnen noch eine Best-Practice-Lösung präsentieren, die auf einem neuen Software-Modul von Echobot (dem sogenannten „Hunter-Modus“) basiert.

Jetzt wünschen wir aber erst einmal: Viel Spaß beim Lesen!

Ihr Echobot Team

ZUR ORIENTIERUNG

2. WELCHE DATEN SIND KRITISCH / UNKRITISCH?

Die DSGVO schützt die personenbezogenen Daten von natürlichen Personen (also „Menschen“, im Unterschied zu Firmen als „juristische Personen“) und zwar bei jeder Art der Nutzung.

LEITSATZ gemäß Art. 4 Nr. 1 DSGVO:

Die DSGVO ist anwendbar auf alle Daten, die von einer „natürlichen Person“ genutzt werden, sofern diese Person über die Daten oder eine Kennung (Name, Nummer, Merkmalskombination, …) eindeutig zu identifizieren ist.

Dies bedeutet im Umkehrschluss aber auch, dass Daten, welche sich nicht auf „natürliche Personen“, sondern lediglich auf eine Firma beziehen, grundsätzlich verarbeitet werden können (vgl. Spalte „nicht betroffene Daten“ in der folgenden Tabelle). Dasselbe gilt auch, wenn die Identifikation der Person später nicht mehr möglich ist, z.B. weil Sie die Daten in geeigneter Form anonymisiert haben.

Aber auch bei Daten, die sich auf Personen beziehen, ergibt sich aus der Struktur der DSGVO, dass der Gesetzgeber zwischen normalen und „besonders sensiblen“ Personenkategorien unterscheiden. Allgemein lässt sich Folgendes festhalten:

Je persönlicher, detaillierter und sensibler die Daten sind, umso höher werden die Anforderungen für eine rechtskonforme und erlaubte Verarbeitung.

Wir haben versucht das Ganze in einer kurzen Übersicht tabellarisch aufzuführen, damit Sie ein Gefühl bekommen können, mit welchen Daten Sie es ggf. im eigenen Unternehmen zu tun haben:

Nicht betroffen	**Betroffene Datenkategorien**		
Firmendaten	**zur Identifikation**	**Problematisch**	**Kritisch**
• Firmennamen juristischer Personen • Geschäftliche Adressdaten • Firmenkontakt-daten • Anonymisierte Daten	• Personennamen • Personalisierte E-Mail-Adressen • Handynummern, Durchwahlen • IP-Adressen	• Alter und Geburtsdatum • Geschlecht • Wohnort • Bankverbindungen • Finanzdaten & Scoring	• Gesundheitsdaten • Angaben zu Religion, ethnischer Herkunft, politischer Orientierung
Beispiele: ■ Müller GmbH Hauptstr. 4 ■ info@firma.de ■ Zentralnummer	Beispiele: ■ Peter Schwind ■ peter@firma.de ■ 0721 4442 -33 ■ IP 43.34.22.123	Beispiele: ■ Männlich ■ geb. 14.04.81 in Frankfurt ■ Kontostand	Beispiele: ■ Krankenhistorie ■ Biometrie-Daten ■ katholisch

Für die Verarbeitung der kritischen Datenkategorien legt die DSGVO zusätzlich besondere Voraussetzung fest, die in Art. 9 erklärt werden. Unternehmen, welche solche Daten verarbeiten wollen (z.B. Krankenversicherungen), müssen zusätzlich eine Gefährdungsbeurteilung erstellen.

Daten in der Grauzone

Bei einigen Daten ist es nicht auf den ersten Blick ersichtlich, ob diese einen direkten Bezug zu einer Person haben, oder ob sie sich eignen, um eine Person eindeutig zu identifizieren. So kann zum Beispiel die Abteilung eines Unternehmens die E-Mail-Adresse

- einkauf@firma.de

verwenden, z.B. um eine Bestellung zu tätigen. Zwar wird der Name des Bestellers in der Regel zur Bestellung erfasst, jedoch kann dies auch über einen Online-Zugang erfolgen, der von mehreren Personen verwendet wird.

Ein anderes Beispiel sind geschäftliche Durchwahlen. So wäre die Karlsruher Telefonnummer

- 0721 – 500 57 500 als Zentralnummer unkritisch, die
- 0721 – 500 57 -209 aber ggf. problematisch,

sofern sie verwendet werden kann, um zum Beispiel Gesprächsprotokolle einer bestimmten Person zu erstellen. Da beim Ausscheiden eines Mitarbeiters die Durchwahlen in der Regel an den Nachfolger weitergegeben werden, lässt sich hierüber aber gerade nicht zweifelsfrei die Person identifizieren. In der Praxis wird es daher immer auf den speziellen Einzelfall ankommen.

> KOMMENTAR RECHTSANWALT DR. CARSTEN ULBRICHT:
>
> „Geschäftliche Durchwahlnummern und E-Mail-Adressen sind personenbezogene Daten, wenn sie einem Mitarbeiter persönlich und nicht bestimmten Arbeitsplätzen, Teams oder Abteilungen zugewiesen sind. Das ist für den Außenstehenden nicht immer erkennbar. Im Zweifel sollte man daher aus Gründen der Vorsicht eher von einem Personenbezug ausgehen. Jedenfalls, wenn ein Klarname in der E-Mail-Adresse enthalten ist oder die Telefonnummer mit einer spezifischen Durchwahl dargestellt ist, die per Bindestrich vom Rest getrennt ist und nicht auf eine Null endet.“

Ausnahme 1: Geschäftsführer und andere handelnde Personen

Zum Glück eindeutig sind solche Fälle, bei denen der DSGVO andere rechtliche Regelungen und höchstrichterliche Entscheidungen explizit entgegenstehen. Ein solches Beispiel hat der Europäische Gerichtshof bezogen auf solche personenbezogenen Daten gefällt, die in öffentlichen Registern, wie dem deutschen Handelsregister, zwingend angegeben werden müssen. In der Urteilsbegründung heißt es frei interpretiert, dass das Interesse der Allgemeinheit an einem funktionierenden und verlässlichen Wirtschaftsverkehr und somit an der Veröffentlichung der Namen und bestimmter Daten von Geschäftsführern, Prokuristen und Vorständen höher wiegt als deren Recht auf Privatsphäre.

Datenverarbeitung ist bei Geschäftsführern, Prokuristen, Vorständen erlaubt,
weil folgende Daten von Rechtswegen aus öffentlich zugänglich gemacht werden müssen:

- Namen und Titel
- Zugehörigkeit zu Unternehmen
- weitere Angaben aus dem öffentlichen Handelsregister (z.B. Wohnort)

Achtung: bei dem Merkmal „Geburtsdatum" könnte eine Interessensabwägung zu Gunsten des Betroffenen kippen – achten Sie daher auf eine genaue Zweckbindung. Auch für Merkmale, die nicht im Register veröffentlicht sind (z.B. Telefonnummer) gilt die hier erwähnte Ausnahme nicht.

Die öffentlichen Register dienen genau dem Zweck, damit jeder sich über seinen (potentiellen) Geschäftspartner informieren kann. Eine Einschränkung der Verarbeitung würde diesen Zweck gefährden. Das genaue Urteil können Sie nachlesen unter:

► **Urteil des Gerichtshofs auf https://curia.europa.eu**

Ausnahme 2: Offensichtlich öffentliche Daten

Generell ist die DSGVO aus rechtlicher Sicht als „Verbot mit Erlaubnisvorbehalt" konstruiert. Das bedeutet, dass eine Datenverarbeitung untersagt ist, sofern nicht ein gesetzlicher Legitimationsbestand die jeweilige Verarbeitung erlaubt.

Die Erlaubnisnormen finden sich für „einfache" personenbezogene Daten in Art. 6 DSGVO, für besondere Kategorien personenbezogener Daten in Art. 9 DSGVO.

Eine Datenverarbeitung gemäß Art.9 ist laut Abs. 2 lit. e erlaubt,

- wenn sie sich auf personenbezogene Daten bezieht, die die betroffene Person über sich bereits „offensichtlich öffentlich" gemacht hat.

Dieser Gesetzestext bezieht sich dabei sogar auf „besondere Kategorien" von Daten, wie Sie sie in der Tabelle auf Seite 4 im kritischen Bereich vorfinden (z.B. ethnische Herkunft oder Gesundheitsdaten).

Als Anwender des Gesetzes kann man daher interpretieren, dass diese Regelung auch auf weniger kritische Daten zutrifft, wenn ein Mitarbeiter z.B. seine Position und seine geschäftliche Durchwahl auf der eigenen Unternehmenswebseite öffentlich angibt. Juristen bezeichnen dieses Vorgehen als „Argumentum a fortiori" oder deutsch „Erstrechtschluss". Da sogar sensible Daten verarbeitet werden dürfen, wenn diese offensichtlich öffentlich gemacht worden sind, gehen Juristen davon aus, dass dies auch für andere personenbezogene Daten gelten muss. In diesen Fällen wird im Regelfall eine Zulässigkeit der Datenverarbeitung auf Grundlage der Interessenabwägung des Art. 6 Abs.1 lit. f DSGVO angenommen.

In jedem Fall wird es bei der Auslegung darum gehen, wie die Interessensabwägung zwischen Betroffenem und Verarbeiter ausgeht (vgl. Kapitel 7) und ob der Betroffene bei der Veröffentlichung seiner Daten „angesichts der Umstände der Veröffentlichung vernünftigerweise hätte absehen müssen, dass eine solche Nutzung der Daten erfolgen wird." (vgl. Erwägungsgrund 47 DSGVO).

Auch wenn die Nutzung öffentlicher Daten also noch nicht 100% klar ist, empfiehlt es sich dennoch unbedingt verfügbare öffentliche Quellen und Links zu dokumentieren, um im Streitfall auf weitere Argumente zurückgreifen zu können.

Beispiele, wo Sie Quellen öffentlicher Daten finden:

- öffentliche (über Suchmaschinen auffindbare) Social-Media-Profile
- auf der Team-Seite einer Firmenhomepage
- auf einer Webseite im Kontaktbereich/Impressum
- in einem Artikel oder einer Pressemitteilung
- in Inhalten von öffentlichen Kommentaren der Person

Wichtig:

➔ Den Nachweis, dass die verarbeiteten Daten öffentlich sind/waren, muss das verarbeitende Unternehmen erbringen können. Im Prinzip muss zu jedem gespeicherten Feld sauber dokumentiert sein, woher die Information stammt und zu welchem Zeitpunkt diese dort öffentlich einsehbar war.

➔ Achten Sie dabei immer auch auf Speicherdauer, Zweckbindung und Informationspflicht (vgl. Kapitel 3).

Grenzen in der Nutzung öffentlicher Daten:

Nur weil jemand eine Information (vielleicht auch unabsichtlich) öffentlich gemacht hat, muss er nicht zwangsweise damit rechnen, dass diese Daten auch über ihn gespeichert werden. Betrachten wir folgendes Szenario:

Eine Geschäftskollegin twittert über ihren vierbeinigen Begleiter im Büro. Als guter Vertriebler wollen Sie sich diese Information zu Nutze machen und im CRM-System ablegen, dass Ihr Kontakt „Hundebesitzer“ ist. Darf man das?

Wir fragen unseren Rechtsexperten:

KOMMENTAR RECHTSANWALT DR. CARSTEN ULBRICHT:

„Das ist leider nicht zulässig. Es fehlt an einer gesetzlichen Erlaubnis. Es liegt weder ein Fall der Erforderlichkeit der Verarbeitung solcher Daten zur Durchführung vorvertraglicher Maßnahmen, noch ein Fall der Verarbeitung auf Basis berechtigter Interessen gemäß Art. 6 Abs. 1 lit. f DSGVO vor. Für Letzteres wären erforderlich: (i) ein berechtigtes Interesse, (ii) die Erforderlichkeit der konkreten Datenverarbeitung zur Wahrung dieses Interesses sowie (iii) das Nichtvorliegen eines überwiegenden Interesses des Betroffenen am Ausschluss der konkreten Datenverarbeitung.

Es ist schon fragwürdig, ob ein berechtigtes Interesse besteht, als Geschäftspartner ein ausschließlich der Privatsphäre zuzuordnendes Datum zu verarbeiten. Im Rahmen der hier vorzunehmenden Abwägung der Interessen des werbenden Unternehmens und der Interessen der betroffenen Person ist insbesondere auf die vernünftigen Erwartungen des Kunden abzustellen, ob eine derartige Datenverarbeitung erfolgt. Das ist wohl abzulehnen. Der Kunde muss wohl nicht ohne Weiteres davon ausgehen, dass ein solches privates Datum von einem Geschäftspartner zu seiner Person gespeichert wird.“

Seit der DSGVO gilt also Vorsicht also bei der Speicherung von Daten, wie:

- Haustiere
- Hobbies
- Namen der Ehefrau / der Kinder
- Geburtsdatum
- Urlaub
- …

Die DSGVO hat dafür sogar einen eigenen Begriff geprägt – den „Grundsatz der Datenminimierung“. Diese und weitere Richtlinien und wie Sie damit korrekt umgehen beschreiben wir im folgenden Kapitel.

3. WIE VERHALTE ICH MICH KORREKT IM UMGANG MIT DATEN?

Bei der Verarbeitung personenbezogener Daten gibt es seit der DSGVO einige Grundsätze und Pflichten zu beachten und nachzuweisen. Diese basieren auf den allgemeinen Grundsätzen wie sie in Art. 5 beschrieben sind. Zudem bestehen jetzt auch umfassende Rechte, die dem Betroffenen in den Art. 12 - 23 eingeräumt werden. In diesem Leitfaden betrachten wir nur solche Grundsätze näher, die für Ihre Vertriebsarbeit relevant sind:

Zweckbindung und Datenminimierung

Die Daten, die Sie speichern, müssen immer einem konkreten, legitimen Zweck dienen – im Unterschied zum Beispiel zur „Vorratsdatenspeicherung", bei der ohne konkreten Anlass unbegrenzt Daten angehäuft werden. Im direkten Zusammenhang steht der Grundsatz der Datenminimierung, der besagt, dass nur solche und so viele Daten gespeichert werden dürfen, wie es für den konkreten, zuvor definierten Zweck angemessen ist. Das gilt sowohl für den gesamten Datensatz, als auch für einzelne Merkmale, die Sie über den Kunden abgespeichert haben.

„Ein Vorgehen, wie es häufig in Marketing und Vertrieb anzutreffen ist, dass erstmal pauschal alle Informationen zu Kunden und Interessenten abgespeichert werden, ist nicht mehr zulässig."

Das bedeutet aber keinesfalls, dass Sie jetzt gar keine Informationen mehr speichern dürfen. Der Gesetzgeber fordert jedoch, dass Sie sich genau Gedanken machen, welche Felder ausgefüllt werden und weshalb.

Einfaches Beispiel:

Wer Sicherheitsschuhe verkauft, für den ist die Speicherung der Schuhgröße des Kunden durchaus entscheidend für die Erbringung der Leistung. Ein Büromöbelausstatter dagegen wird keinen Zweck vorbringen können, für den er die Schuhgröße seiner Kunden benötigt. Die Speicherung des Geschlechts (männlich / weiblich) hingegen ist für eine passende Anrede in der geschäftlichen Kommunikation aber universell zweckdienlich.

PRAXISTIPP:

So stellen Sie zweifelsfrei die geforderte Zweckbindung her:

Schon bei der Datenerfassung sollte die Zweckbestimmung eine entscheidende Rolle spielen. Orientieren Sie sich zum Beispiel an den Phasen des Prozesses der Kundengewinnung, indem Sie klar zwischen Neuakquise, Vertragsanbahnung und Vertragserfüllung unterscheiden. In Ihren Systemen legen Sie dann bestimmte Vorlagen, Eingabemasken, Formulare und Layouts an, die je nach Phase nur die jeweils nötigen Felder enthalten. Die Datensätze werden dann als „Potential", „Interessent" oder „Kunde" markiert. So wird jedem Mitarbeiter gleich klar, wie der Speicherumfang ausfallen darf.

Um den Überblick zu behalten, sobald mehrere Personen mit der Datenbank arbeiten, aktivieren Sie Funktionen zur „Versionierung" oder „Wiederherstellung". So können Sie später leicht nachvollziehen, wer wann welchen Datensatz editiert hat.

Spezielle Felder wie „Quell-Link“ können Ihnen dabei helfen zu dokumentieren, woher die eingegebenen Daten stammen und warum sie erfasst wurden. Denn Sie müssen auch sicherstellen, dass bestimmte Eingaben nicht „zweckentfremdet“ werden.

Beispiel: Ihr Unternehmen veranstaltet im Rahmen einer Kampagne ein Gewinnspiel, in dem ein T-Shirt verlost wird. Die Kleidergröße, die Sie hierfür abfragen, dürfen Sie anschließend nicht im zugehörigen Datensatz abspeichern, da Sie diese Information nur zum Zweck des Gewinnspiels erhalten haben.

Informationspflichten erfüllen

Der Gedanke hinter den Informationspflichten der DSGVO ist, dass ein Betroffener jederzeit darüber Bescheid weiß, wann, wo, wie und von wem seine Daten verarbeitet werden. Umgekehrt bedeutet das für Sie als Verarbeiter, dass Sie verpflichtet sind die Betroffenen proaktiv zu informieren. Da im Vertrieb die Datenerfassung zum Tagesgeschäft gehört, sollten Sie auf Ihre Kunden und Interessenten zugehen, sobald Daten eingegeben werden, jemand Ihre Website besucht oder wenn Sie ohne sein Wissen Informationen über ihn sammeln.

Die Inhalte, den Zeitpunkt und die Art dieser Hinweise regeln die Artikel 13 und 14.

Artikel 13	**Artikel 14**
Art. 13 gilt, wenn Sie die betroffenen Daten direkt von der Person erhalten (z.B. wenn diese ein Leadformular ausfüllt).	Art. 14 gilt, wenn Daten nicht direkt von der Person erhoben werden (z.B. Auskunft von Banken an die SCHUFA).
Wann muss man informieren? ✓ Zum Zeitpunkt der Erhebung ✓ Wenn ich den Datensatz ergänze UND sich die Informationen verändert haben ✓ Wenn sich der Zweck ändert	Wann muss man informieren? ✓ Innerhalb einer angemessenen Frist nach Erlangung der Daten, spätestens jedoch innerhalb eines Monats ODER ✓ Beim ersten Kontakt mit der Person ODER ✓ Bei Offenlegung der Daten gegenüber Dritten zu diesem Zeitpunkt
Wie Sie dem Betroffenen diese Informationen genau und korrekt übermitteln, lesen Sie in Kapitel 4.	

Informationspflicht im Vertrieb

Auch im Vertrieb erhalten Sie Daten entweder vom Ansprechpartner selbst (Art. 13), z.B.:

- wenn Sie eine Visitenkarte tauschen
- wenn dieser ein Leadformular ausfüllt

oder Sie ermitteln die Daten aus anderen Quellen (Art. 14) wie z.B.

- Recherche in Google oder XING
- Echtzeit-Daten aus Echobot CONNECT

Umfang der Informationspflicht

Die folgenden Inhalte müssen Sie dem Kunden mitteilen. Es empfiehlt sich, diese zentral in Ihrer Datenschutzerklärung zusammenzufassen. Dieses Dokument können Sie dann bei jedem datenschutzrelevanten Vorgang wirksam einbinden oder verlinken:

✓	**Kontakt des für die Datenverarbeitung Verantwortlichen** Geben Sie an, wer rechtlich für die Vorgänge der Datenverarbeitung verantwortlich ist. In der Regel ist dies die Geschäftsleitung Ihres Unternehmens.
✓	**Kontakt des Datenschutzbeauftragten** Wenn Ihr Unternehmen verpflichtet ist, einen Datenschutzbeauftragten zu stellen, der für die Einhaltung der gesetzlichen Vorgaben verantwortlich ist, soll der Kontakt einfach und formlos möglich sein. Geben Sie Kontaktdaten (Name, Anschrift, Telefon, E-Mail) an.
✓	**Zweck und Rechtsgrundlage** Erklären Sie allgemein die Zwecke, zu denen Sie Daten verarbeiten wollen (z.B. Vertrieb).
✓	**Ggf. Empfänger der Daten** Die DSGVO verlangt, dass Sie die Empfänger oder auch nur Empfängerklassen Ihrer Daten beschreiben. Dies sind in der Regel „Mitarbeiter“, aber auch „Geschäftspartner“ oder sogar „Kunden“, wenn Sie z.B. eine Community betreiben. Falls Dienstleister in die Verarbeitung eingebunden werden, denken Sie an einen Auftragsverarbeitungsvertrag (AVV).
✓	**Ob die Daten per Übermittlung in ein Drittland übertragen werden** Das trifft z.B. zu, wenn Sie die Daten in einem System oder einer Softwarelösung speichern, deren Anbieter außerhalb der EU sitzt. (vgl. Kapitel 5)
✓	**Wie lange die Daten gespeichert werden** Informieren Sie den Betroffenen darüber, wie lange Sie beabsichtigen, seine Daten zu speichern. Beachten Sie auch die gesetzlichen Aufbewahrungsfristen. (vgl. Abschnitt zur Speicherdauer in diesem Kapitel)
✓	**Falls Sie sich auf ein berechtigtes Interesse gemäß Art. 6 Abs. 1 lit. f berufen** Angabe und Ihre Einschätzung des berechtigten Interesses. (vgl. Kapitel 6 „So weisen Sie berechtigtes Interesse nach“)
✓	**Beabsichtigen Sie ein automatisches Profiling?** Hinter dem automatischen Profiling verbergen sich alle Verfahren, die Daten verwenden, um über Algorithmen automatisierte Entscheidungen treffen. Zum Beispiel, wenn Sie Werbebanner an Ihre Kunden auf Grundlage von deren Surfverhalten ausliefern lassen.
✓	**Welche Rechte der Betroffene hat** Zusätzlich ist es Ihre Pflicht, den Betroffenen über seine Rechte aufzuklären, damit die Verbraucher nicht nur wissen, was mit ihren Daten passiert, sondern auch über ihr Mitspracherecht informiert sind. (vgl. nächsten Abschnitt)
✓	**Quelle der Daten** Falls Sie die Informationen nicht selbst vom Betroffenen erhalten haben, hat er das Recht die Herkunft zu erfahren. Hier bietet sich an den Link und das Datum zur Quelle zu speichern (dies gilt insbesondere bei der Erhebung aus externen Quellen).

Bearbeitung und Änderung der Daten

Häufig erhalten wir die Frage unserer Kunden, ob diese Informationspflicht bei jeder Änderung eines Datensatzes erneut erfolgen muss. Der Gesetzestext bezieht sich zunächst nur auf die „Erhebung" von Daten, wobei darunter in der Regel auch Änderungen, Anpassungen oder Ergänzungen zu verstehen sind. Da jedoch eine erneute Information bei jeder kleinen Änderung als störend und unverhältnismäßig gesehen werden muss, ist unsere Empfehlung, Betroffene nur in folgenden Fällen erneut zu informieren:

a) wenn Sie ganz wesentliche Ergänzungen an deren Datensatz vornehmen
b) wenn sie gänzlich neue Datenkategorien oder sensible Daten erfassen
c) oder wenn sich auf Ihrer Seite der Zweck der Datenverwendung geändert hat.

Der Erwägungsgrund 171 besagt zudem, dass für den Fall einer einmal erteilten Einwilligung zur Datenverarbeitung „diese auch fortgesetzt werden kann …, wenn die Art [der Einwilligung] … den Bedingungen der DSGVO entspricht". Eine alte Einwilligung muss also ggf. erneuert werden, eine DSGVO-konforme Einwilligung kann dauerhaft fortgesetzt werden.

> DAZU RECHTSANWALT DR. CARSTEN ULBRICHT:
>
> „Gemäß Art. 13 Abs. 4 DSGVO besteht dann keine Informationspflicht, wenn die betroffene Person bereits über die Informationen der Datenverarbeitung verfügt. Das ist nur schlüssig. Wenn der Betroffene dieselben Informationen bereits einmal erhalten hat, wäre es unverhältnismäßig, den Datenverarbeiter dazu zu zwingen, ihm diese noch einmal zur Verfügung zu stellen. Dies gilt unabhängig vom Umfang der weiteren Datenerhebung. Die Fälle, in denen eine neue Informationspflicht besteht, werden sich daher auf einen geänderten Zweck oder andere berechtigte Interessen beschränken."

Rechte der Betroffenen korrekt umsetzen

Generell dient die DSGVO dem Schutz der personenbezogenen Daten und räumt daher den von der Datenverarbeitung Betroffenen auch entsprechend viele Rechte ein. Diese sind in den Art. 12 – 23 aufgeführt. Solche Rechte, die für den B2B-Bereich und den Vertrieb besonders relevant sind, möchten wir Ihnen kurz erläutern und Tipps für den Umgang geben:

a) Recht auf Auskunft

Immer wieder kommt es im Vertrieb vor, dass Sie jemanden kontaktieren und derjenige Sie fragt:

„*Woher haben Sie meine Daten?*"

Besonders, wenn eine Kundenbeziehung schon lange stillsteht oder Sie in der Kaltakquise unterwegs sind, werden Sie dieser Frage häufiger begegnen. Gemäß DSGVO sind solche Anliegen berechtigt und Sie müssen darauf eine plausible Antwort geben können.

Wie gehe ich damit um?

- **Erstauskunft des Mitarbeiters**

Insbesondere wenn der Kontakt von Ihnen initiiert wird, sollten Sie dem Kunden eine erste Antwort geben können. Unterscheiden Sie hierbei zwischen einer einfachen Anfrage, wie sie öfter vorkommen kann, und einem datenschutzrelevanten Auskunftsersuchen.

Prüfen Sie kurz, ob der Anfragende auch tatsächlich der Betroffene ist (geben Sie z.B. keine Informationen über den Geschäftsführer an das Sekretariat heraus). Falls begründete Zweifel an der Identität des Anfragenden vorliegen, dürfen Sie zusätzliche Informationen verlangen. Das kann vorkommen, wenn Sie eine Anfrage vom Absender peter.mueller@firmaA.de zu einem Datensatz mit der Adresse peter-mueller@firmaB.de erhalten. Aufgrund der Allgemeinheit des Namens Peter Müller können Sie nicht davon ausgehen, dass es sich um dieselbe Person handelt. Gleiches gilt übrigens auch immer, wenn Sie Dubletten in Ihrem System finden, die nicht eindeutig zusammengehören. Zusätzliche Angaben, wie die Adresse, können helfen, den Betroffenen eindeutig zu identifizieren.

Bei frisch recherchierten Daten und gut dokumentierten Quellen fällt die schnelle Erstauskunft leichter, als wenn Sie einen älteren Kontakt aus Ihrem CRM-System ziehen. Legen Sie eine Vorgehensweise fest und schulen Sie Ihre Mitarbeiter auf die beste Art eine Erstauskunft zu erteilen.

Beispiel: F: „Woher haben Sie meine Daten?“

A: „Wir hatten im letzten Jahr eine Geschäftsbeziehung mit Ihrem Unternehmen und auf der Webseite sind Sie als Ansprechpartner für den Einkauf genannt.“

Wenn Ihre Kollegen eine solche Antwort schnell und fundiert erteilen können, reicht dies in der Regel schon aus, um den Betroffenen zufrieden zu stellen.

Wenn Sie Echobot CONNECT nutzen, sind Sie im Vorteil, da Sie hierüber gleich Echtzeit-Kontaktdaten mit Quellenangaben beziehen können. Übrigens bietet Echobot auch Integrationsmöglichkeiten in CRM-Systeme an.

In allen weiteren Fällen oder wenn sich der Betroffene mit Ihrer Kurzauskunft nicht zufriedengibt, empfehlen wir unbedingt in einen formalen Prozess eines Auskunftsersuchens überzugehen und an den Datenschutzbeauftragten zu verweisen.

Beispiel: F: … „das kann ja jeder behaupten – ich möchte einen Beweis!“

A: „Aber gerne, in diesem Fall leite ich Ihre Anfrage sehr gerne an unseren Datenschutzbeauftragten Herr/Frau X weiter. Dieser hat auch Einsicht in die genaue Dokumentation unserer Datenherkunft. Sind Sie damit einverstanden?“ …

- **Der formale Auskunftsprozess und was dabei zu beachten ist**

Der Datenschutzbeauftragte zentralisiert Auskunfts- und Löschanfragen aller Art – Sie sollten diesen Prozess nicht den einzelnen Mitarbeitern überlassen. Besonders dann nicht, wenn der Betroffene auch wissen möchte, welche Daten Sie von ihm besitzen. Sie behalten dadurch nicht nur einen besseren Überblick, sondern vereinfachen auch Ihre Nachweispflicht und stellen einen einheitlichen Umgang sicher. Der Datenschutzbeauftragte kann die Identität des Betroffenen

prüfen und ihm unverzüglich (spätestens nach einem Monat) eine formlose und kostenfreie Auskunft erteilen. Wenn in Ihrem Geschäft das Risiko für Anfragen erhöht ist, sollten Sie genug Ressourcen einplanen, da ein Auskunftsverfahren recht aufwändig ist. Planen Sie auch ein, dass die Auskunft der Daten in einem maschinenlesbaren Format verlangt werden kann, also z.B. als CSV- oder Excel-Datei.

PRAXISTIPP:

Verwenden Sie für offizielle Anfragen eine zentrale E-Mail-Adresse (z.B. datenschutz@firma.de), an die jeder Mitarbeiter alle Anfragen dieser Art weiterleitet. Diese wird vom Datenschutzbeauftragten verwaltet und sollte über ein dokumentiertes Ticketsystem (z.B. Zendesk, OTRS, ...) verarbeitet werden.

Falls Sie Ihre Daten bisher nicht sauber gepflegt oder die Daten-Herkunft nicht eindeutig dokumentiert haben, kann das zum Problem werden. Lesen Sie hierzu unsere Tipps zur nachträglichen Legitimation von Altbeständen in Kapitel 4.

b) Recht auf Berichtigung

Haben sich die Daten eines Kunden geändert oder haben Sie sie falsch abgespeichert, dann kann er von Ihnen verlangen, dass Sie seine Daten korrigieren.

Wie gehe ich damit um?

Legen Sie auch hierfür ein System fest, wie der Datenabgleich zu erfolgen hat. Mündlich am Telefon kann es schnell zu Verständnisproblemen kommen, deshalb sollten Sie sich die Änderungen mindestens schriftlich per E-Mail bestätigen lassen. Das hat nicht nur den Vorteil, dass Sie so sicherer die richtige Schreibweise eines Nachnamens übermitteln, sondern auch über einen eindeutigen E-Mail-Absender einen Identitätsnachweis erhalten und gleichzeitig Ihrer Dokumentationspflicht besser nachkommen.

Bitte prüfen Sie: Darf jeder Ihrer Vertriebsmitarbeiter Daten im System ändern oder zentralisieren Sie auch dieses Vorgehen lieber bei Ihrem Datenschutzbeauftragten?

PRAXISTIPP:

Es empfiehlt sich, in Ihren Systemen zumindest ein Rechtekonzept einzurichten, indem Sie Mitarbeitern verschiedene Befugnisse zuteilen. Je größer Ihr Unternehmen ist, desto wichtiger ist dieses Vorgehen. Denn gemäß dem Grundsatz der Datenrichtigkeit in Art. 5 müssen Sie auch sicherstellen, dass Änderungen an Ihren Daten nicht willkürlich erfolgen.

Nicht alle Daten können vom Betroffenen korrigiert werden: Er kann z.B. keine „Korrektur“ einer Bonitätsbewertung verlangen, sondern nur eine Berichtigung der Datengrundlage, auf der die Berechnung basiert.

c) Recht auf Löschung

Hin und wieder kommt es vor, dass Sie von einem Kunden oder Interessenten einen der Sätze hören:

„*Ich verlange, dass Sie alle meine Daten löschen.*“ oder

„*Ich möchte nicht mehr von Ihnen kontaktiert werden.*“

Besonders problematisch wird es, wenn beide Wünsche zusammentreffen:

„*Ich möchte nie mehr von Ihnen kontaktiert werden, bitte löschen Sie zudem alle meine Daten.*“

Wie gehe ich damit um?

Bestätigen Sie dem Kunden, dass Sie seinen Wunsch nach Datenlöschung erhalten haben und ernst nehmen. Erklären Sie dem Kunden, dass die Löschung und Sperrung einen formalen Prozess auslöst. Dieser sollte im ganzen Unternehmen einheitlich angestoßen werden, entweder über einen Button im CRM-System oder einfach per Mail an den Datenschutzbeauftragten. Verlangen Sie auch zur Identifikation immer eine schriftliche Löschanfrage des Betroffenen. Nur in Einzelfällen kann diese auch telefonisch angenommen werden, nämlich wenn Sie ihn dadurch zweifelsfrei identifizieren können.

- **Formaler Löschprozess im Einzelnen:**

- **Daten ermitteln:**
  Der Datenschutzbeauftragten ermittelt anhand der schriftlichen Anfrage alle Daten in den vorhandenen Systemen im Unternehmen, die betroffen sein könnten (z.B. anhand der E-Mail-Adresse). Nicht vergessen: Auch Gesprächsverläufe und automatisierte Prozesse, wie Support-Ticketsysteme oder Ihre Marketing-Automation zählen dazu.

- **Aufbewahrungsfristen beachten:**
  Der Datenschutzbeauftragte prüft, ob es nicht entgegenstehende Rechte gibt, die Ihnen erlauben, die Daten weiterhin aufzubewahren (siehe Aufbewahrungsfristen in diesem Kapitel im Abschnitt „Speicherdauer und regelmäßiges Löschen“). Gleichen Sie diese mit den vorhandenen Daten ab.

- **Nicht eindeutige Daten zuordnen:**
  Möglicherweise treffen Sie auf Daten, die Sie nicht eindeutig dem Anfragenden zuordnen können z.B. eine zweite E-Mail-Adresse. Falls es sich dabei ohnehin um „Karteileichen“ handelt, ist es am einfachsten diese auch gleich mit zu löschen. Andernfalls entsteht zusätzlicher Aufwand für eine genaue Prüfung.

- **Daten löschen:**
  Sie haben nun bis zu 30 Tage Zeit die Löschung der Daten vorzunehmen. Backups sind übrigens in der Regel nicht betroffen (vgl. dazu Kapitel 5).

- **Dokumentation:**
  Vermerken Sie anschließend auch im zugehörigen Firmendatensatz, dass eine Löschanfrage bearbeitet wurde und beziehen Sie sich auf die Vorgangsnummer. So können Sie gewährleisten, dass jede Anfrage auch beantwortet wird (Art. 24 Abs. 1 DSGVO).

- **Bestätigung der Löschung:**
  Bestätigen Sie dem Betroffenen nur, dass die Löschung erfolgt ist. Eine Auskunft, welche Daten Sie überhaupt gespeichert hatten, hätte zuvor erfolgen müssen.

Vorsicht Widersprüche:

Ironischerweise darf man nach einem Löschbegehren die Daten des Kunden nicht mehr speichern, ist jedoch gleichzeitig verpflichtet den Löschvorgang an sich sauber zu dokumentieren. In Kapitel 5 im Bereich CRM-Systeme zeigen wir Ihnen eine technische Lösung auf, wie Sie diesen Spagat mittels Hash-Funktionen dennoch schaffen können.

DAZU RECHTSANWALT DR. CARSTEN ULBRICHT:

„Gemäß Art. 17 Abs. 3 lit. e DSGVO besteht der Anspruch auf Löschung nicht, soweit die Verarbeitung erforderlich ist zur Verteidigung gegen Rechtsansprüche. Das bedeutet, dass die Datenverarbeitung in dem Maße, wie es zur Dokumentation der Umsetzung des Löschanspruchs erforderlich ist, erfolgen darf. Was dies in der technischen Umsetzung bedeutet, ist leider noch nicht geklärt.

Ebenso problematisch ist der Wunsch des Betroffenen, er möchte „nie wieder" kontaktiert werden. Denn wenn man nicht speichern darf, dass eine betroffene Person keinen Kontakt wünscht (Stichwort „Blacklist"), so lassen sich auch keine technischen Schranken und Sicherheitshinweise verwalten.

In einem solchen Fall sollten Sie den Betroffenen also immer fragen, ob er einer Speicherung seiner Daten auf einer „Blacklist" zustimmt, um damit eine erneute Erfassung und ggf. Kontaktaufnahme sicher auszuschließen.

KOMMENTAR RECHTSANWALT DR. CARSTEN ULBRICHT:

„Jedes Löschbegehren betrifft immer nur die Datenverarbeitung der Vergangenheit bis zum aktuellen Zeitpunkt. Jede neue Verarbeitung in der Zukunft ist somit zunächst nicht betroffen, sofern die erneute Erfassung und Verarbeitung mit neuer Legitimationsgrundlage erfolgt ist.

Wird eine Blacklist geführt, so sollte die Einwilligung des Betroffenen in die Aufnahme unter Berücksichtigung der Informationspflichten des Art. 13 DSGVO eingeholt werden. Es sollte in diesem Zusammenhang dann auch präzise geregelt werden, welche Sachverhalte von der Blacklist abgedeckt werden."

d) Recht auf Widerruf der Einwilligung

Falls der Betroffene eine einmal erteilte Einwilligung zur Datenspeicherung gegeben hat, so kann er diese jederzeit widerrufen.

e) Beschwerderecht bei Aufsichtsbehörde

Wenn der Kunde sich über Sie beschweren möchte, so kann er das bei der zuständigen Aufsichtsbehörde des Bundeslandes tun. Die meisten Behörden bieten dafür bereits Online-Formulare an.

Wie gehe ich damit um?

Es reicht aus, wenn Sie den Link zu diesen Behörden sowie deren Anschrift in Ihrer Datenschutzerklärung aufführen und diesen auf Anfrage an den Kunden weitergeben.

Weitere Rechte sind das Recht auf Einschränkung der Verarbeitung, auf Widerspruch und auf Datenübertragbarkeit. Diese werden in diesem Leitfaden nicht thematisiert, da sie für den Vertrieb weniger relevant sind.

Speicherdauer und regelmäßiges Löschen

Der Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e) verlangt, dass jeder, der Daten erhebt und speichert, regelmäßig prüft, ob diese noch aktuell und relevant sind oder ganz oder teilweise entfernt werden müssen. Das muss auch geschehen, sobald der Zweck der Speicherung erloschen ist. Auch Daten, bei denen die Herkunft unklar ist oder die nicht nachträglich legitimiert werden können, müssen Sie demnach aus Ihrem Bestand entfernen.

Dabei liegt es in Ihrer Verantwortung als Verwalter, regelmäßig zu prüfen, ob einer der genannten Gründe vorliegt. Sobald das der Fall ist, sollten Sie „ohne schuldhaftes Zögern" handeln. Konkret meint der Gesetzgeber damit, dass Sie die Informationen nicht länger als notwendig in Ihrer Datenbank behalten und es vermieden werden soll, diese noch in irgendeiner Art und Weise zu verwenden.

Wie bei dem Löschbegehren des Betroffenen, gibt es auch der regelmäßigen Löschung entgegenstehende Aufbewahrungspflichten. Neben steuer- und handelsrechtlichen Vorgaben können dies z.B. auch Daten sein, die Rechtsstreitigkeiten betreffen. Die folgende Tabelle gibt Ihnen eine kleine Orientierung:

Gesetzliche Aufbewahrungsfristen		
6 Jahre	10 Jahre	30+ Jahre
• Geschäftsbriefe und Schriftwechsel (auch E-Mails, insbesondere in Zusammenhang mit einem Geschäftsabschluss) • Angebot und Auftragsbestätigung (sofern erfolgreich) • Preisvereinbarungen & Preislisten • Kaufverträge • Mahnungen & Mahnbescheide • Protokolle	• Andere handels- sowie steuerrechtliche Unterlagen, wie z.B. Rechnungen, Buchungsbelege • Debitorenkonten & -listen • Inkassobücher	• Gesetzliche Urteile und Prozessakten • Akten und Bücher, wie die Bau-beschreibung oder Kostennachweise für die gesamte Lebensdauer des Bauwerks

Im Rahmen Ihrer vertrieblichen Arbeit empfehlen wir folgendes:

PRAXISTIPPS zur Datenbereinigung im Vertrieb

- Löschen Sie alle E-Mail-Adressen, bei denen die Mails nicht mehr beim Empfänger ankommen („Hard-Bounces“).
- Entfernen Sie Benutzer- und Personendaten, die seit mehr als drei Jahren keine Aktivität (Login / Bestellung / Kontakt) hatten, sofern kein laufender Vertrag besteht (Orientierung an der regelmäßigen Verjährungsfrist nach §195 BGB).
- Entfernen Sie quartalsweise personenbezogene Daten von Potentiallisten, wenn diese für Ihre Vertriebsarbeit nicht mehr relevant sind.
- Prüfen Sie mindestens jährlich Ihre Ordner und Cloudspeicher auf nicht mehr genutzte Dateien.
- Verkürzen Sie die Laufzeit von Retargeting- / Tracking-Cookies auf maximal 14 Tage.
- Löschen Sie am Jahresende alle E-Mails und Protokolle, die sechs Jahre oder älter sind und nicht mehr benötigt werden.

Datensicherheit

So schnell wie sich die erfolgsversprechenden Seiten der Digitalisierung entwickeln, so schnell wächst auch die Bedrohungslage, die sich durch die Vernetzung ergibt. Cyberattacken gehören mittlerweile zur Kriminalitätsstatistik und treffen immer häufiger auch Unternehmen und deren Daten. Das ist einer der Gründe, weshalb der Gesetzgeber nicht erst seit der DSGVO von Ihnen erwartet, dass Sie Ihre Daten entsprechend schützen.

Art. 32 schreibt vor, wie Sie technische und organisatorische Maßnahmen umzusetzen haben, um Ihr Risiko bestmöglich zu minimieren. Dabei soll der Kostenaufwand im Verhältnis zum Schutzzweck stehen, d.h. zum Beispiel zur Menge und Sensibilität der Daten, die Sie verarbeiten. Zudem sollen Sie sich am Stand der Technik orientieren. Was genau darunter zu verstehen ist, bleibt zwar im Detail offen, lässt aber vermuten, dass damit marktübliche Sicherheitsstandards und aktuelle Technologien gemeint sind.

Da das Thema Datensicherheit – abgesehen vom Gesetz – auch im Interesse Ihres Unternehmens ist, sollten Sie einige Maßnahmen unbedingt umsetzen, falls das nicht schon geschehen ist:

PRAXISTIPPS Datensicherheit

- Legen Sie Zugriffsregeln auf Ihre Daten in einem Konzept fest. Nicht jeder Vertriebler oder Praktikant sollte alle Kundendaten einsehen oder bearbeiten können.
- Mit unterschiedlichen Nutzerprofilen für Ihre Datenbanken und Systeme regeln Sie nicht nur die Rechteverteilung, sondern können auch gleich nachvollziehen, wer welche Datensätze geändert hat.
- Stellen Sie auch sicher, dass Änderungen rückgängig gemacht werden können.
- Sofern möglich, sollten Sie Daten an geeigneten Stellen pseudonymisieren, zumindest verschlüsselt ablegen und insbesondere auch Zugangspasswörter nur verschlüsselt speichern.

- Schulen Sie Ihre Mitarbeiter im sicheren Umgang mit Daten und Passwörtern
- Helfen Sie Ihren Mitarbeitern über Schablonen und Vorlagen, bei der Datenerfassung und Bearbeitung die oben beschriebenen Grundsätze einzuhalten.

Zu diesen Grundregeln in Ihren technischen und organisatorischen Maßnahmen sollten Sie auch regelmäßig Backups erstellen, um die Daten nicht nur vor dem Zugriff Unbefugter zu schützen, sondern auch vor deren Verlust.

4. DIE DATENHERKUNFT SPIELT EINE ROLLE!

Gemäß den Grundsätzen in Art. 5 Abs. 1 lit. a DSGVO müssen Daten rechtmäßig erhoben und transparent verarbeitet werden. Nach Abs. 2 sind Sie zudem verpflichtet diese und weitere Anforderungen nachweisen zu können.

Gerade deswegen ist es entscheidend, dass Sie zu jedem Datum und Merkmal, das Sie zu einer Person speichern und verarbeiten, die Herkunft dokumentieren können.

Abhängig von der Quelle der Daten, sind neben der Dokumentation noch weitere Besonderheiten zu beachten. Zunächst möchten wir Ihnen mit folgendem Schaubild einen Überblick verschaffen, welche Datenquellen Sie in Ihrem eigenen Unternehmen berücksichtigen müssen:

a) Daten entstehen automatisch	**b) Daten werden vom Betroffenen selbst bereitgestellt**	**c) Daten werden von Ihnen recherchiert oder ergänzt**	**d) Sie haben die Daten von Dritten erworben oder erfassen lassen**	**e) Altbestände existierender Daten Ihrer Systeme**
z.B. durch Tracking der Klicks auf der eigenen Webseite	z.B. bei Registrierung als Kunde / Übergabe Visitenkarte oder Kontaktaufnahme	z.B. durch Recherche bei Google, XING oder dem Bundesanzeiger	z.B. durch Kauf einer Fach-besucherliste oder Adress-CD	z.B. Daten aus Ihren CRM-Systemen

a) Automatische Datenerhebung

In fast jeder modernen Webseite oder Software werden mittels verschiedener technischer Methoden, wie zum Beispiel Cookies, automatisiert Nutzerdaten gesammelt. Das ist zum Beispiel der Fall, wenn Sie die Zugriffe mit Google Analytics zählen oder Marketing-Tools, wie Hubspot, einsetzen. Dabei werden das Nutzerverhalten des Betroffenen, seine Klicks, Browserversion, Gerätetyp, Betriebssystem, Referrer, Datum und die Uhrzeit der Zugriffe gespeichert. Wenn hierbei auch die IP-Adresse abgelegt wird, gelten diese Informationen als personenbezogen, da darüber eine betroffene Person „identifizierbar“ ist.

Das müssen Sie beachten:

Es ist nicht grundsätzlich ausgeschlossen, Ihre Webseite mit Hilfe solcher Software auf Benutzerfreundlichkeit und Conversion-Rate zu optimieren. Dennoch müssen Sie darauf achten, dass die Datenverarbeitung über Art. 6 DSGVO legitimiert werden kann und der User über die Datenerhebung gemäß Art. 13 DSGVO in der Datenschutzerklärung informiert wird. Es wird weiterhin empfohlen, die gesammelten IP-Adressen zu anonymisieren. Gerade da viele Toolanbieter ihre Server in den USA betreiben, kommt es sonst zu einer automatischen Übermittlung von Daten in ein (Nicht-EU) Drittland, wofür wieder strengere Vorschriften gelten (vgl. Art. 44 DSGVO).

Ein weiteres Beispiel im Vertrieb sind E-Mail Klicktracking-Tools oder die Auswertung von Verbindungsdaten in automatisch erstellten Telefonprotokollen, wobei Betroffene möglicherweise über ihre Telefonnummer identifizierbar sind. Diese Auswertungen sind insbesondere nach der Stellungnahme der Datenschutzkonferenz mit erhöhtem Risiko verbunden.

Achtung: Der Hinweis auf die Datenschutzerklärung muss gerade im Online-Marketing immer gut sichtbar und getrennt von anderen Einwilligungen erfasst werden. Arbeiten Sie hier eng mit Ihrer technischen Abteilung und Ihrem Datenschutzbeauftragten zusammen, um Prozesse und Tools zu identifizieren, in denen automatisiert personenbezogene Daten erhoben werden. Oft ist das nicht auf den ersten Blick erkennbar.

RECHTSANWALT DR. CARSTEN ULBRICHT:

„Kurz vor dem 25. Mai 2018 sorgte die Datenschutzkonferenz (gemeinsames Gremium der Datenschutzbehörden der Bundesländer) für Aufruhr:

In einer Stellungnahme legte sie fest, dass es nicht mehr ausreicht, dem Nutzer beim automatisierten Tracking Widerspruchsmöglichkeiten aufzuzeigen (z.B. über Opt-Out-Links). Auch könne das Webtracking nicht mehr über berechtigtes Interesse begründet werden, sondern es bedürfe immer der vorherigen informierten Einwilligung des Nutzers. Das bedeutet, dass Unternehmen in kürzester Zeit gezwungen waren, ihre Prozesse auf eine „Opt-In-Möglichkeit“ umzustellen. Dass das nahezu unmöglich ist, stellt auch der Branchenverband bitkom in einer Stellungnahme heraus. Als Website-Betreiber können Sie also nur auf erste Urteile und eine künftige Lockerung dieser Regelungen hoffen, wenn wir in Zukunft nicht alle von „Cookie-Opt-In Pop-Ups“ beim Besuch einer Seite konfrontiert werden möchten. Bis dahin bleibt das Risiko beim Webtracking erhöht.

Es sprechen aus juristischer Sicht gute Gründe gegen die Stellungnahme der Datenschutzkonferenz. So besagt Erwägungsgrund 47 der DSGVO, dass Direktwerbung ein berechtigtes Interesse sein kann. Dann muss aber auch der weniger weitreichende Eingriff des Trackings, der eine Vorstufe der Direktwerbung sein kann, grundsätzlich über das berechtigte Interesse gerechtfertigt werden können. Darüber hinaus ist in Art. 21 Abs. 1 Sa. 1 DSGVO geregelt, dass ein Widerspruchsrecht bei Profiling besteht. Dieses impliziert aber, dass Profiling (und als Vorstufe damit auch Tracking) über berechtigte Interessen legitimiert werden kann, da nur dann ein Widerspruchrecht bestehen kann bzw. erforderlich ist.

Es ist gut möglich, dass in Zukunft zwischen verschiedenen Arten von Tracking-Tools zu unterscheiden ist. So spricht bei pseudonymisiertem, üblichem Tracking (z.B. Google Analytics) einiges für eine Zulässigkeit über die Abwägung im Bereich der berechtigten Interessen. In anderen Fällen kann sich durchaus eine strengere Handhabung durchsetzen.“

b) Personenbezogene Daten werden vom Betroffenen selbst bereitgestellt

Ein deutlich transparenterer Vorgang ist es, wenn der Betroffene Ihnen seine Daten selbst bereitstellt. Dabei gibt es verschiedene Wege, wie Sie diese Daten übermittelt bekommen können. Die häufigsten Fälle sind:

- Der Betroffene füllt ein Formular aus (physisch oder auf Ihrer Webseite)
- Der Betroffene übermittelt Ihnen seine Daten per Fax oder per E-Mail (Briefkopf, Signatur)
- Sie erhalten die Daten über eine Kontaktanfrage (Visitenkarte oder XING-Einladung)
- Er teilt Ihnen seine Daten persönlich mit (z.B. direkt oder am Telefon)

Das müssen Sie beachten:

Übertragen Sie die bereitgestellten Daten in Ihre Systeme. Das Gesetz unterscheidet nicht, wie Sie die erhobenen Daten digitalisieren und abspeichern. Ob Sie händisch abtippen oder die Visitenkarte scannen, ist für das weitere Vorgehen irrelevant. Viel wichtiger ist, dass Sie die Herkunft direkt im Datensatz dokumentieren, d.h. auf welchem Weg die persönliche Erhebung stattgefunden hat. Gleiches gilt für den Zweck, zu dem Sie die Daten erheben – auch dieser muss dokumentiert werden.

Bei der Erhebung der Daten bei dem Betroffenen gilt die Informationspflicht nach Art. 13. Das heißt, dass Sie zum Zeitpunkt der Erhebung in schriftlicher oder elektronischer Form die Informationen bereitstellen müssen. Wie Sie das am besten umsetzen, hängt von der Art ab, in der Sie der Betroffene kontaktiert. Stehen Sie sich persönlich auf einer Messe oder in einem Ladenlokal gegenüber, könnten Sie zum Beispiel über einen Aushang informieren und ggf. Handzettel auslegen oder ihm bei Bedarf aushändigen. Zugunsten der Übersichtlichkeit empfiehlt es sich die Inhalte in zwei Stufen zu gliedern, indem Sie die Inhalte aus Art. 13 Abs. 1 gleich direkt übermitteln (per Aushang) und auf die weiteren Inhalte aus Abs. 2 in Ihrer Datenschutzerklärung verweisen.

Sich im persönlichen Kontakt nur auf die URL der Datenschutzerklärung zu stützen, erfüllt an dieser Stelle nicht die Anforderungen, da das Gesetz einen sofortigen und leichten Zugang verlangt. Erhalten Sie die Daten des Betroffenen jedoch per Formular direkt auf der Website, sieht das anders aus: Dann genügt der Verweis mit direkter Verlinkung.

Bei telefonischem Kontakt wird die Informationspflicht umständlicher. Es kursieren schon diverse Empfehlungen, von der jeder die praktikabelste für sich finden muss. Entweder Sie entscheiden sich dafür, den Betroffenen selbst aufzuklären, was jedes Telefonat deutlich in die Länge zieht oder sie schalten eine Bandansage direkt vor das Telefonat. Eine etwas angenehmere Möglichkeit, welche das Gesetz freier interpretiert, ist, alle wichtigen Informationen online unter einer leicht zu merkenden URL zusammen zu fassen und darauf telefonisch und anschließend per E-Mail zu verweisen.

Da eine mündlich erteilte Auskunft nur schwer nachweisbar ist, kann dieses Vorgehen helfen Ihre Dokumentationspflichten zu erfüllen.

c) Daten werden selbst recherchiert oder digitalisiert

Diese Art der Datenerhebung kommt in der Kaltakquise relativ häufig vor. Wenn Sie also z.B. über Suchmaschinen (Google), Soziale Netzwerke (Xing/LinkedIN) oder auch Datenbanken und Anbieter wie Echobot aktiv recherchieren, dann erheben Sie die Daten selbst. Gerade im Vertrieb benötigen Sie einige grundlegende Informationen zum Unternehmen, den Ansprechpartner mit Namen, zumindest eine Telefonnummer oder andere Kontaktmöglichkeit.

Falls keine oder nur teilweise Informationen zu einem Interessenten vorhanden sind, ist das der gängige Weg, an diese zu gelangen. Um eine solche Erhebung und Verarbeitung zu rechtfertigen, müssen Sie in jedem Einzelfall eine Interessensabwägung durchführen, welche Daten Sie guten Gewissens verarbeiten können (Wie das funktioniert erklären wir in Kapitel 7).

Wann genau beginnt die „Verarbeitung" der Daten?

Das Gesetz definiert den Begriff der Verarbeitung in Art. 4 Abs. 2 und meint damit wörtlich „das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung,…" .

Das müssen Sie beachten:

Was bei dieser Abgrenzung auffällt ist, dass die reine Recherche der Daten (z.B. das Nachschauen/ Lesen einer persönlichen E-Mail-Adresse auf einer Webseite oder aus der Echobot CONNECT Datenbank), noch kein Verarbeitungsvorgang im oben beschriebenen Sinne ist. Erst wenn Sie die personenbezogenen Daten in die „Sphäre Ihres Einflussgebietes" übertragen greift die DSGVO. Insofern sollten Sie im Vertrieb z.B. erst Daten in Ihr System überführen, wenn Sie von der Rechtmäßigkeit der Verarbeitung ausgehen können (wann dies der Fall ist beschreiben wir in Kapitel 6).

> Vorsicht!
> An dieser Stelle schon ein Vorgriff auf Kapitel 8: Nur weil Sie die Daten ggf. rechtmäßig verarbeiten dürfen, heißt dies nicht automatisch, dass Sie auch zur Kontaktaufnahme berechtigt sind. Hierfür sind weitere Vorschriften z.B. aus dem UWG zu berücksichtigen.

Auch bei der Eigenrecherche gilt für Sie die Informationspflicht nach Art. 14, die Sie beim ersten Kontakt, spätestens aber nach einem Monat nach Erhebung der Daten erfüllen sollten. In den meisten Fällen werden Sie die Daten vermutlich dann recherchieren, wenn Sie unmittelbar mit dem Kunden oder Interessenten Kontakt aufnehmen möchten: informieren Sie ihn dann in der ersten E-Mail oder im Telefonat (Inhalte vgl. Kapitel 3).

Um auch Ihrer Nachweispflicht nachzukommen, speichern Sie die Quellen sorgfältig ab. Bei einer Internetrecherche empfiehlt sich der Link der Ursprungsseite mit Datumsangabe, da sich Seiteninhalte von Zeit zu Zeit ändern können. Da auch alle öffentlichen Register, wie Handelsregister und Bundesanzeiger, heute online verfügbar sind, können Sie darauf per Link verweisen, bzw. falls das auf die jeweilige Unterseite nicht möglich ist, das Register und das Recherchedatum angeben.

d) Daten über Drittanbieter beziehen

Eine andere Form der Herkunft liegt vor, wenn Sie die Daten durch einen Dritten, zum Beispiel ein Call-Center, erheben lassen, wenn Sie Daten und Adresslisten mieten oder fertige Adresslisten einkaufen und zusätzlich zu Firmenadressen auch konkrete Ansprechpartner benötigen.

In der Vergangenheit galt für diese Fälle das sogenannte „Listenprivileg". Hierdurch war es gemäß §28/29 BDSG (alt) erlaubt, personenbezogene Daten z.B. von bestimmten Berufsgruppen für Zwecke der Werbung selbst und sogar für die geschäftsmäßige Übermittlung zu erheben, wenn es sich um listenmäßig zusammengefasste Daten handelte und keine schutzwürdigen Interessen der Betroffenen entgegenstanden. Diese Regelungen sind mit der Einführung der DSGVO weggefallen.

Stattdessen setzt die DSGVO solche Aktivitäten, und damit auch den Adresshandel mit personenbezogenen Daten, unter die Voraussetzung, dass in jedem Einzelfall ein überwiegend berechtigtes Interesse des Verarbeiters vorliegen muss. Zwar schließt der Erwägungsgrund 47 die „Direktwerbung" explizit als ein solches mit ein, jedoch bietet das Gesetz dem Anwender keinerlei weitere Orientierung, wie solche Abwägungen auch für größere Listen im Rahmen eines Geschäftsprozesses strukturiert durchgeführt werden sollen.

> KOMMENTAR
>
> Der Gesetzgeber hat durch die Abschaffung des Listenprivilegs eine fatale Entscheidung getroffen, die nicht nur nach Meinung von Branchenverbänden schwerwiegende Folgen für die deutsche Wirtschaft haben wird. Gerade die wichtige Neukundengewinnung wird durch das Versäumnis, dafür geeignete Möglichkeiten und klare Regelungen zu schaffen, stark beeinträchtigt. Auch eine Differenzierung von B2B- und B2C-Anwendungen wäre dringend nötig gewesen. Stattdessen flieht der Gesetzgeber wieder in die faule Form der pauschalen Einzelfallbetrachtung und bürdet somit den Gerichten und Marktteilnehmern die eigentliche Arbeit einer Ausdifferenzierung über langwierige Verfahren und Urteile auf. Leider eine in den letzten Jahren häufig gesehene Praxis.
>
> Im Effekt wird es eine noch stärkere Verschiebung vertrieblicher Maßnahmen von Outbound- zu Inbound-Methoden geben, wodurch Versandhändler, Katalogversender, Direktmarketing-Anbieter, Verlage und die Werbewirtschaft leiden und die Budgets noch stärker den großen Werbe-Plattformen wie Google, Facebook und Co. zufließen.

PRAXISTIPP:

<u>Was Sie bei der Nutzung von Drittanbietern beachten sollten:</u>

- Klären Sie im Vorfeld, dass der Anbieter rechtskonform arbeitet und jeder Betroffene der Erhebung, Verarbeitung und Weitergabe seiner Daten zugestimmt hat.
- Prüfen Sie die Einhaltung des sog. „Koppelungsverbots", also z.B., dass die Teilnahme an einem Gewinnspiel nicht von der Zustimmung der Datenweitergabe abhängt.

- Wenn Sie Adressen oder Verteiler mieten, verwenden Sie den Absender, dem der Betroffene seine Zustimmung erteilt hat, sonst kann es zu Verwirrung kommen.
- Fragen Sie den Anbieter nach einer Freistellung, wenn sich im Fall der Nutzung gekaufter Daten herausstellen sollte, dass er unsauber gearbeitet hat.

Auftragsverarbeitungsvertrag bei Nutzung externer Daten?

In allen drei oben genannten Fällen (Datenbeschaffung, -miete und -kauf) benötigen Sie keinen Auftragsverarbeitungsvertrag. Da Sie selbst keine eigenen Daten an den Dritten weiterleiten, ist dies nicht nötig. Auch kommt ein AVV nur dann zum Tragen, wenn ein Dritter nach Ihrer Weisung Daten verarbeitet. Adresshändler, Listbroker und Datenbank-Betreiber entscheiden jedoch in der Regel selbst über den Umgang mit den angebotenen Daten.

KOMMENTAR RECHTSANWALT DR. CARSTEN ULBRICHT:

Das Thema Adresshandel und der Datenkauf sind im Rahmen der DSGVO leider rechtlich noch weitgehend ungeklärt. Die Absicht Direktwerbung als berechtigtes Interesse nach Art. 6 Abs. 1 lit. f rechtssicher zu legitimieren wird noch einige Diskussionen und Urteile benötigen. Beachten Sie in jedem Fall, dass Sie unabhängig von der Datenverarbeitung auch prüfen müssen, ob und auf welchem Weg Sie zur Kontaktaufnahme berechtigt sind (vgl. Kapitel 8).

e) Altbestände existierender Daten

In vielen Kundendatenbanken befinden sich noch nicht-DSGVO-konforme “Altlasten“. Das bedeutet für Sie nicht nur viel Aufwand, sondern auch ein großes Risiko Daten zu verlieren. Sie fragen sich jetzt:

„*Muss ich meine Personendatenbank löschen?*“

Pauschal kann man zunächst vorwegschicken, dass Datenverarbeitungsvorgänge vor dem 25.05.2018, die den Vorgaben des Bundesdatenschutzgesetzes entsprochen haben, grundsätzlich auch den Anforderungen der DSGVO genügen. So haben die Datenschutzbehörden mitgeteilt, dass bestehende BDSG-konforme Einwilligungen, die vor Geltung der DSGVO eingeholt worden sind, auch nach dem 25.05.2018 fortwirken.

Altbestände sollten folglich daraufhin geprüft werden, ob diese BDSG-konform erhoben worden sind, bzw. ob dies nachgewiesen werden kann. Wenn das nicht der Fall ist, stellt sich die Frage, ob Sie die Daten auch nachträglich legitimieren können und falls ja, wie?

Das müssen Sie beachten:

Grundsätzlich spricht nichts gegen eine nachträgliche Legitimation Ihrer Altbestände. Solange Sie den Zweck und die Herkunft nachweisen können, falsche Daten berichtigen und den Betroffenen über die Eintragung in Ihre Systemen informieren, dürfen Sie die Daten auch weiterhin speichern und verarbeiten.

PRAXISTIPP:

Greifen Sie auf externe Hilfe zurück, um größere Mengen zu legitimieren. Indem Sie mithilfe von Google oder Echobot öffentliche Quellen recherchieren, können Sie die Herkunft belegen und die Aktualität und Richtigkeit prüfen. Echobot ermöglicht Ihnen bei Bedarf sogar eine CRM-Integration von Echtzeit-Daten. Wenn Sie jetzt noch den Zweck ergänzen und sicherstellen, dass Sie alle vorhandenen Daten benötigen, sind Sie auf gutem Weg Ihren Altbestand rechtskonform zu halten.

Ob Sie bei der Änderung des Datensatzes auch den Betroffenen informieren müssen, hängt davon ab, wie ausführlich Sie ergänzen und ob Sie grundlegende Änderungen vornehmen (vgl. Kapitel 3).

Falls der Betroffene bisher gar nicht wusste, dass Sie Daten über ihn gespeichert haben, wie das oft bei Interessenten, mit denen Sie noch nicht in Kontakt standen, vorkommen kann, sollten Sie schleunigst handeln und ihn informieren. Aus diesem Grund wurden auch um den 25. Mai zahlreiche E-Mails von Unternehmen verschickt, in denen sie ihre Informationspflicht erfüllten.

5. WELCHE SYSTEME SIND BETROFFEN?

Im Vertrieb kommen die unterschiedlichsten Systeme zum Einsatz, in denen personenbezogene Daten gespeichert sein können. In diesem Abschnitt möchten wir Ihnen eine kleine Übersicht geben, wo typischerweise personenbezogene Daten anfallen, damit Sie bei der Umsetzung der Empfehlungen schneller die richtigen Stellen in Ihren Prozessen identifizieren können.

a) Dateien

Wenn Sie …

… Namen, E-Mail-Adressen und Telefonnummern in Excel-Listen abspeichern;
… Formulare oder Visitenkarten abtippen oder mit Texterkennung einscannen;
… Gesprächsprotokolle oder Projektpläne als Word-Dokument ablegen;
… E-Mail-Korrespondenzen lokal abspeichern;
… oder Profilbilder und erhaltene Bewerbungsunterlagen speichern;

dann liegen in diesen Dateien in der Regel personenbezogene Daten vor.

➔ Achten Sie darauf, dass Mitarbeiter und Kollegen nach Möglichkeit nicht lokal, sondern immer an einem zentralen Ort, z.B. einem Netzlaufwerk, ablegen. Sonst ist es für Sie später nicht möglich herauszufinden, auf welchen PCs noch welche Dateien und Daten abgelegt sind.

➔ Für bestimmte Dateien gelten gesetzliche Aufbewahrungspflichten von teilweise bis zu 10 Jahren. Andere Dateien wie z.B. Bewerbungsunterlagen müssen Sie nach einer Absage in angemessener Frist löschen. Ein zentrales Dokumentenmanagement-System (DMS) kann helfen, hier nicht den Überblick zu verlieren.

➔ Vorsicht, wenn Sie Dateien bei einem Cloud-Storage Anbieter wie Google Drive / Dropbox oder Microsoft OneDrive speichern. In den meisten Fällen stehen deren Server im Ausland, wodurch eine Übermittlung in ein Drittland erfolgt. Darüber müssen Sie betroffene Personen aufklären. Ergänzen Sie einen entsprechenden Hinweis in Ihrer Datenschutzerklärung und binden Sie diese wirksam in Ihre Kommunikation mit dem Betroffenen ein (vgl. Kapitel 4). Dank dem EU-US Privacy Shield Abkommen finden Sie einige Anbieter aus den USA, die zumindest selbstverpflichtend Datenschutzprinzipien einhalten und Ihnen eine DSGVO-konforme Übermittlung von Daten garantieren: https://www.privacyshield.gov/list

b) CRM-Systeme und Kundendatenbanken

Wenn Sie Ihren Vertrieb professionell aufgestellt haben, verwenden Sie vermutlich eine zentrale Kundendatenbank oder ein CRM-System (selbiges gilt analog auf für ERP- oder Warenwirtschafts-systeme, und selbst entwickelte Datenbanken, sofern Sie darin Personendaten speichern).

Es ist nicht notwendig, dass Sie alle Daten in diesen Systemen löschen oder neu aufbauen. Bestimmte Datensatztypen sollten Sie jedoch noch einmal genau unter die Lupe nehmen:

- Tabellen mit Namen wie „Ansprechpartner“, „Kontakte“ oder „Personen“
- Felder mit Namen wie „Ansprechpartner“ oder „Kontaktperson“ z.B. am Firmendatensatz
- Text-, Notizfelder oder Protokolle, in denen Personen namentlich erwähnt werden
- Tabellen wie „Leads“ oder „Anfragen“, bei denen Personendaten für eine Auskunft angegeben werden
- Logs und Protokolldateien, in denen z.B. Gesprächs-, Verbindungsdaten oder Klickpfade zu Identifikationsmerkmalen wie Telefonnummern oder IP-Adressen abgelegt werden

Erinnern Sie sich an die Grundsätze der „Datenminimierung“, „Zweckbindung“, „Speicherbegrenzung“ und „Richtigkeit“ (vgl. Art. 5 DSGVO). Unsere Empfehlung bei deren Umsetzung im Rahmen Ihres CRM-Systems lauten daher wie folgt:

- Entfernen Sie alle Personeneinträge, die Sie nicht mehr benötigen.
- Entfernen Sie Personendaten, von denen Sie wissen, dass diese falsch sind (z.B. Person arbeitet dort nicht mehr).
- Entfernen Sie Einträge, deren Herkunft Sie nicht mehr nachvollziehen können und für die Sie keine nachträgliche Legitimation haben,
    - z.B. würde eine aktive Vertragsbeziehung eine weitere Speicherung legitimieren
    - oder Sie können mittels Echobot eine Datenquelle z.B. als Link ergänzen, auf der die gespeicherten Daten offensichtlich öffentlich einsehbar sind.
- Auch wenn Sie bestimmte Personendatensätze weiterhin speichern wollen, entfernen Sie aus den Einträgen Feldwerte, die Sie für den angedachten Zweck nicht mehr benötigen.
    - Löschen Sie z.B. Werte wie „Alter“ oder „Name der Ehefrau“, wenn Sie hierfür keinen direkten Zweck vorweisen können.

Speichern Sie an jedem Eintrag das Erstellungs- und Änderungsdatum sowie die Person, welche den Eintrag angelegt oder editiert hat. So erhalten Sie künftig die vom Gesetz geforderte Transparenz.

PRAXISTIPP zum richtigen Entfernen der personenbezogenen Daten:

Gerade in Datenbanken werden Objekte häufig relational verknüpft. Das bedeutet, dass sich z.B. ein altes Angebot auf den Personendatensatz mit ID-Nummer 435 bezieht. Wenn Sie jetzt besagten Personendatensatz komplett löschen, entsteht im System ein fehlender Verweis, da das Bezugsobjekt nicht mehr existiert. Dies kann in einigen Systemen zu Fehlern führen. Besser ist es, den Datensatz zu behalten und nur die Feldwerte (Daten) zu überschreiben.

Eine Variante wäre z.B. alle entfernten Datensätze „Gelöschte Person“ zu nennen. Eine bessere Idee ist es jedoch die Werte mit einer irreversiblen Hash-Funktion zu verschlüsseln. Beispiel:

Die Funktionen MD5 oder SHA1 machen aus einem beliebigen Textfeld einen HASH-Wert:

peter@firma.de -> abf53829e7af66722f5936906f5e9638

Diese Transformation ist nicht mehr umkehrbar, außer man berechnet eine große Tabelle aller möglichen Texte und vergleicht die Hash-Werte. Dies ist aber leicht mit einem sogenannten „Salt“ zu umgehen. Ergänzen Sie z.B. am Anfang „#123#“ und es entsteht ein anderer Hash:

#123#peter@firma.de -> 5612fa9df1c5130eee7b20273f7aeb31

➔ Achtung, eine Verschlüsselung der Werte mit einem Passwort ist nicht dasselbe, da diese Transformationen mit dem bekannten Passwort umkehrbar sind.

Wiederholen Sie den Prozess mit allen Datenfeldern, die Sie sicher löschen möchten.

Die so veränderten Datensätze sind in Ihrem CRM sehr leicht als gelöschte Werte zu erkennen. Der Vorteil dieses Vorgehens ist, dass Sie später einem Betroffenen Auskunft erteilen können, ob ein Datensatz in Ihrem CRM tatsächlich gelöscht wurde, indem Sie bei einer Anfrage den Anfragewert nehmen und dieselbe Transformation wie oben durchführen. Anschließend können Sie über einen Hash-Vergleich feststellen, ob es den Wert schon einmal gab und belegen, dass dieser nicht mehr im System im Klartext existiert.

c) E-Mail-Programme (Outlook), Apps und Handy-Adressbücher

In nahezu allen Software-Systemen zur Kommunikation, wie E-Mail-Programmen, Chat-Apps oder in Geräten, wie Smartphones, gibt es heutzutage eine Adressbuch-Funktion. Dies ist letztlich nichts anderes als eine Art Mini-CRM. Daher gelten im Prinzip die gleichen Grundsätze wie oben beschrieben.

➔ Da diese Adressbücher jedoch häufig auf die Arbeitsstationen oder mobilen Geräte der Mitarbeiter verteilt sind, empfiehlt es sich auf ein System zurückzugreifen, welches die Datensätze regelmäßig synchronisiert. So können Löschungen auch an allen verteilten Stellen automatisch umgesetzt werden und es existiert eine einheitliche Sicht auf den relevanten Datenbestand.

➔ Für Potential-Adressen und Kaltakquise empfehlen wir, komplett auf die Adressbuch-Funktion zu verzichten und stattdessen die Daten von der Firmenwebseite oder direkt aus einem Echtzeit-System wie Echobot CONNECT zu verwenden. Erst, wenn der Potentialkunde sein Interesse bekundet hat, z.B. indem er ein Angebot anfragt, können Sie die Speicherung im Rahmen einer Vertragsanbahnung legitimieren. Dann macht das Anlegen des Eintrags Sinn.

➔ Auch E-Mail-Inhalte und Korrespondenzen können personenbezogene Daten, z.B. in Signaturen, beinhalten. Da diese Informationen jedoch wichtige Dialoge Ihrer Geschäftsbeziehung mit der betroffenen Person darstellen, würde man im Rahmen einer Interessenabwägung das Interesse des Unternehmens an einer sauberen Dokumentation sehr hoch gewichten. Unsere Empfehlung ist deswegen, nicht pauschal alle Korrespondenzen zu löschen, zumindest solange nicht, bis es gerichtliche Urteile gibt, welche sich hierzu entsprechend geäußert haben.

➔ Achtung: E-Mails, Adressbücher und Kontaktinhalte sind in der Regel nicht nur auf den Clients, sondern auch auf Servern gespeichert. Falls Sie etwas löschen wollen, denken Sie daran, dies an beiden Stellen zu tun. Falls Ihr Mail-Server in den USA steht (z.B. im Fall von GoogleMail) denken Sie an Ihre Hinweispflicht. Ein Link in Ihrer E-Mail-Signatur auf die aktuelle Datenschutzerklärung kann hier helfen.

d) Kundenakten, Karteien und Ordner

Gerade im Rechnungswesen wird häufig noch viel Papier produziert. Seien Sie sich darüber im Klaren, dass auch Daten in Papierform entsprechend den oben dargestellten Grundprinzipien zu behandeln sind. Alte Umfrage- oder Anmeldeformulare sollten Sie nicht pauschal archivieren, sondern nach angemessener Zeit entsorgen. Für Rechnungen und die darauf vermerkten Rechnungs-Empfängerdaten gilt die gesetzliche Aufbewahrungspflicht von 10 Jahren.

Bei sensiblen Daten, wie medizinische Fragebögen über Vorerkrankungen, Beratungs-dokumentationen im Finanzbereich, Bewertungen von Arbeitnehmern oder Gehaltsinformationen, sollten Sie besondere Vorsicht walten lassen und ganz klare Prozesse für den Umgang mit solchen Dokumenten etablieren. Dies kann schon daher erforderlich sein, wenn Sie gemäß Art. 35 verpflichtet sind eine Datenschutz-Folgenabschätzung anzufertigen.

In jedem Fall sollten Sie sogenannte technische und organisatorische Maßnahmen (TOM) definiert haben, die den Umgang mit Dokumenten regeln. Hier helfen Ihnen die Regelungen aus Art. 25 DSGVO.

e) Backups

Egal, welche Tools Sie einsetzen, in der Regel werden die Daten aller Systeme über Backups vor Datenverlust gesichert. Die Verfügbarkeit der personenbezogenen Daten sicherzustellen und den Zugang zu ihnen rasch wiederherzustellen, wenn es zu einem physischen oder technischen Zwischenfall kommt, ist sogar eine zentrale Forderung der DSGVO.

Jedoch gilt natürlich auch für Backups, dass die dortige Speicherung von personenbezogenen Daten von Löschpflichten betroffen sein kann. Da gerade Backup-Systeme häufig mit anderen Zugriffsrechten versehen sind und an anderen Orten liegen, kommt es an dieser Stelle immer wieder zu Zwischenfällen. In jedem Fall sollten Sie Backups nur in verschlüsselter Form ablegen.

Aktuell wird von Experten jedoch die Meinung vertreten, dass eine Löschung von Einzeldaten aus Backups in der Regel nicht erfolgen muss, weil dies entweder unmöglich oder mit unverhältnismäßig hohem Aufwand verbunden ist. Jedoch sollten Sie beim Wiederherstellen von Daten aus einem Backup genau aufpassen, dass nicht bereits gelöschte Datensätze auch wiederhergestellt werden.

Weitere Informationen im Fachartikel von RA Dr. Jens Bücking:

► **Fachartikel auf https://www.kanzlei.de**

f) Auskunft in maschinenlesbarem Format

Behalten Sie immer im Hinterkopf, dass jeder Betroffene auch Anspruch darauf hat, Auskunft über die in Ihren Systemen zu ihm gespeicherten Daten zu erhalten. Diese Daten müssen Sie ihm auf Anfrage sogar in einem geeigneten maschinenlesbaren Format bereitstellen. Je komplizierter Ihre eigenen Datenstrukturen sind und je mehr Systeme Sie verwenden, umso schwieriger wird es, diesem Anspruch gerecht zu werden. Der Betroffene wird in der Regel z.B. eine Excel Datei erwarten.

6. WANN IST DIE DATENVERARBEITUNG RECHTMÄSSIG?

Nach Erklärung der Datentypen und Erklärung der verschiedenen Vorgaben zur Datenherkunft, kommen wir nun nochmal zu den rechtlichen Anspruchsgrundlagen.

Die DSGVO sieht vor, dass es „rechtmäßig" ist Daten zu verarbeiten, wenn mindestens eine der in Art. 6 genannten Voraussetzungen existiert. Die drei relevantesten Punkte sind Abs. 1 lit. a, b und f. Angewendet auf den Vertrieb ergeben sich folgende Legitimationsgrundsätze:

Art. 6 Abs. 1 lit. a – mit Einwilligung bei Bestandskunden

Am eindeutigsten können Sie die Rechtmäßigkeit der Datenverarbeitung begründen, wenn Ihnen die Einwilligung des Betroffenen vorliegt. Das kommt in der Regel dann vor, wenn Sie mit einer Firma und deren Ansprechpartner schon eine aktive Geschäftsbeziehung haben und sich diese in Ihrem Bestand befindet. Falls Sie nicht sicher sind, ob eine Einwilligung vorliegt, sollte es kein Problem sein, diese bei aktiven Geschäftsbeziehungen auch nachträglich noch einzuholen. Die Einwilligung kann dabei für einen oder gleich für mehrere Zwecke erfolgen. Darunter können Serviceleistungen aber auch der Versand des Newsletters oder weiterer Mailings fallen. Hier sind Sie auf der sicheren Seite.

So holen Sie wirksam eine Einwilligung ein:

Jegliche Verarbeitung, die zur Erfüllung eines vereinbarten Vertrags notwendig ist, wie z.B. das Erstellen von Rechnungen, dürfen Sie ohne explizite Genehmigung durchführen (siehe nächster Abschnitt). Alle anderen Zwecke, wie Kundenumfragen, Katalogversendung, etc., sollten im Rahmen der Zustimmung des Kunden bereits definiert sein. Wann eine erteilte Einwilligung tatsächlich wirksam ist, regelt Art. 7 der DSGVO:

- **Nachweisbar**
  Lassen Sie sich Einwilligungen bestenfalls in Schriftform geben, z.B. per Unterschrift oder E-Mail. Bei Online-Formularen mit ankreuzbaren Kästchen speichern Sie die IP-Adresse und den Zeitpunkt der Zustimmung ab.
- **Unmissverständlich, zweckbezogen & ausdrücklich**
  Machen Sie dem Betroffenen klar, dass und zu welchem Zweck Sie seine Daten verarbeiten. Er selbst muss die Möglichkeit haben, sich aktiv *dafür* zu entscheiden. Ein bereits angekreuztes Kästchen oder ein aktives Widersprechen (Opt-Out) ist nicht rechtskonform.
- **Kopplungsverbot**
  Die Zustimmung muss unabhängig und freiwillig erfolgen. Machen Sie es also nicht zur Voraussetzung, dass ein Betroffener sich für Ihren Newsletter anmeldet, damit er an Ihrem Gewinnspiel teilnehmen kann, sondern stellen Sie ihm beide Optionen unabhängig dar.
- **Vor Beginn der Datenverarbeitung**
  Sofern Sie die Datenverarbeitung auf die Einwilligung des Betroffenen stützen, beginnen Sie erst damit, wenn Ihnen diese vorliegt.

- **Hinweis auf Widerrufsrecht**
  Sie müssen dem Betroffenen jederzeit das Recht auf Widerruf der Einwilligung einräumen und ihn auch darauf hinweisen.

Bei Kindern gelten strengere Vorschriften, bzw. ist die Einwilligung der Erziehungsberechtigten erforderlich. In diesem Dokument gehen wir darauf nicht ein, da unsere Zielpersonen im Vertrieb ausschließlich Geschäftskunden sind.

Art. 6 Abs. 1 lit. b – zur Vertragsanbahnung bei Interessenten

Abs. 1 lit. b erlaubt die Verarbeitung personenbezogener Daten, sofern jemand Interesse bekundet für sogenannte „vorvertragliche Maßnahmen" oder wenn es für die „…Erfüllung eines Vertrags…" notwendig ist. Diesen Fall finden Sie im Vertrieb immer dann vor, wenn der Betroffene eine aktive Anfrage (einen „Lead") an Sie stellt. Egal ob die Anfrage per eingehendem Telefonanruf oder über die Abgabe einer Visitenkarte auf einer Messe erfolgt, es handelt sich hierbei immer um Interessensbekundungen, auf die Sie sich stützen können, um die hierfür notwendigen Daten auch zu verarbeiten.

Ab wann beginnt die Vertragsanbahnung?

Aus rechtlicher Sicht geht die Tendenz dazu, den Zeitpunkt der Vertragsanbahnung über den §311 Abs. 2 BGB zu begründen. Dieser besagt, dass Sie schon während der Vertragsanbahnung in einem rechtsgeschäftsähnlichen Schuldverhältnis mit dem Interessenten stehen. Ganz eindeutig ist das, sobald Sie über Leistungsinhalte oder Preise sprechen. Zudem beschreibt der Gesetzgeber den Fall, wenn die „Möglichkeit zur Einwirkung auf Rechte, Rechtsgüter und Interessen…" des anderen gewährt wird. Dies kommt zum Beispiel vor, wenn Sie Ihre Leistungen zum Test anbieten (Einrichten eines Test-Accounts, Überlassung eines Fahrzeuges zur Probefahrt, etc.), aber auch ein detailliertes Gespräch (Erstberatung im Finanzbereich) kann schon ausreichen.

Ziffer 3 von §311 Abs. 2 BGB geht sogar noch einen Schritt weiter und legitimiert die Vertragsanbahnung mit „ähnlichen geschäftlichen Kontakten". Dies können Sie sich insbesondere dann zu Nutze machen, wenn Sie eine für bestimmte Anwendungsfälle passende Success-Story erstellt haben oder in einer Branche einen besonderen Referenzkunden nutzen können. Eine Datenverarbeitung ähnlicher geschäftlicher Kontakte könnte dann zulässig sein. Diese sehr weite Auslegung der Rechtsnormen ist jedoch noch nicht Gegenstand gerichtlicher Klärungen gewesen, weswegen ein Restrisiko besteht.

Denken Sie in jedem Fall daran, sehr sauber zu dokumentieren, wann wer auf welchem Wege Informationen angefordert hat oder warum Sie von einer Vertragsanbahnung ausgehen. Haben Sie zum Beispiel eine ausführlich dokumentierte Telefonnotiz, stehen Sie zunächst auf der sicheren Seite. Der Betroffene müsste dies erst glaubhaft widerlegen.

Art. 6 Abs. 1 lit. f - mit berechtigtem Interesse bei Kaltakquise

Der bei Unternehmen ohne Frage beliebteste Absatz in der ganzen DSGVO ist der Art. 6 Abs. 1 lit. f. In diesem wird den datenverarbeitenden Firmen nach all den Verboten und Vorschriften nämlich erstmals ein sogenanntes „berechtigtes Interesse“ zugestanden.

Ein berechtigtes Interesse entsteht dabei grundsätzlich aus jeder üblichen Geschäftstätigkeit, die in einem Unternehmen ausgeführt wird, sofern diese zum Unternehmenszweck und somit z.B. auch zur Gewinnerzielungsabsicht beiträgt.

Klar ausgedrückt liegt im Vertrieb, im Marketing und gerade auch in der Kaltakquise ein berechtigtes Interesse des Unternehmens vor. Und da man ganz ohne Datenverarbeitung keine Werbung und auch keinen Vertrieb machen kann, ist die Verarbeitung gerade auch personenbezogener Daten hier „erforderlich“, wie es auch vom Gesetz verlangt wird. In der Vergangenheit war hier nur eine „Zweckmäßigkeit“ gefordert, dies wurde im Rahmen der DSGVO verschärft.

Zu einfach macht es der Gesetzgeber einem dann aber auch wieder nicht und schränkt den beliebten Absatz gleich mit einem weiteren Nebensatz dahingehend ein, dass die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person einer Verarbeitung nicht entgegenstehen dürfen. Kinder genießen hier nochmals einen besonders strengen Schutz.

Vereinfacht gesagt bedeutet dieser Zusatz, dass es keine pauschale Erlaubnis gibt, sondern die Rechtmäßigkeit der Datenverarbeitung nach Art. 6 Abs. 1 lit. f immer die einzelnen Umstände betrachtet und die Interessen jeder Person im Einzelfall mit den Interessen des Unternehmens abwägt.

Solche mitunter doch sehr schwammigen Regelungen sind in den letzten Jahren leider häufig in der Rechtsprechung aufgetaucht. Im stark umstrittenen Leistungsschutzrecht etwa heißt es, dass die Verwendung „kurzer Textauszüge“ erlaubt sei, es wird aber nirgendwo definiert wie kurz „kurz“ ist.

Dieses Vorgehen des Gesetzgebers sorgt dafür, dass niemand mit Sicherheit sagen kann in welchen Fällen Sie als Verarbeiter oder als Betroffener ein überwiegendes Interesse haben. Eine annähernde Klärung entsteht erst durch höchstrichterliche Rechtsprechung von BGH oder EuGH, was mitunter Jahre dauern kann.

Solange Sie sich als Unternehmen auf eine solide Annahme stützen können, dass Ihre berechtigten Interessen für bestimmte Datenverarbeitungen überwiegen, ist eine Nutzung der Daten zumindest nicht verboten. Im Zweifelsfall muss man sich mit dem Betroffenen darüber streiten. Damit Sie schon von vornherein genügend Belege für Ihr Vorgehen erstellen, wollen wir Ihnen im Folgenden ein besseres Verständnis vermitteln, wie die Sache mit dem „berechtigten Interesse“ genau funktioniert und wie man solche Interessen gegeneinander abwägt:

So weisen Sie berechtigtes Interesse nach

Zunächst müssen Sie sauber dokumentieren, wie Ihre Entscheidung, die personenbezogenen Daten für einen bestimmten Geschäftszweck zu verwenden, zustande gekommen ist. Legen Sie ferner für jeden Verarbeitungsvorgang fest, warum dieser notwendig ist und was Ihr berechtigtes Interesse ist.

Beispiel:

Projekt:	Gewinnspiel zur Neukundengewinnung
Prozess:	Bewerbung und Anmeldung über die Webseite; Speicherung der Daten im CRM; zusätzlich freiwillige Erfassung von Newsletter-Opt-Ins; spätere Bewerbung der eigenen Leistungen an eine größere Zielgruppe per E-Mail.
Erforderlichkeit:	Datenverarbeitung / gewählter Datenumfang notwendig
Berechtigtes Interesse:	Werbung / Marketing zur Absatzförderung

Wenn Sie bestehende Prozesse haben, hilft Ihnen eventuell auch folgendes Prüfschema:

1. Kann ich zur Verarbeitung berechtigte Interessen vorlegen?
2. Sind die verarbeiteten Daten erforderlich, um diese Interessen zu wahren?
3. Liegen beim Betroffenen keine entgegenstehenden Interessen vor, die überwiegen?

PRAXISTIPP

Was den Vertrieb angeht, beachten Sie bitte auch unbedingt folgende Punkte:

- ✓ Passenden Ansprechpartner gezielt auswählen:

  Wenn Sie in der Rolle als Vertriebler einen Einkäufer oder Geschäftsführer ansprechen, so berufen Sie sich auf Ihr Interesse an einer Geschäftsanbahnung. Dokumentieren Sie, warum Sie die spezielle Kontaktperson ausgewählt haben, z.B. aufgrund von deren Funktion im Unternehmen oder weil diese nach außen hin als Ansprechpartner für Anfragen auftritt. Auch ein öffentliches geschäftliches Social-Media-Profil, etwa bei XING oder LINKEDIN, kann ein Indikator für ein berechtigtes Interesse sein. Gerade dann, wenn in der Rubrik „Ich suche" Schlagworte, wie „Interessante Kontakte" oder „Neue Geschäftspartner", angegeben sind.

- ✓ Passenden Angebotsinhalt wählen:

  Natürlich sollte Ihr Angebot auch zur Zielgruppe passen. Niemand möchte mit Dingen belästigt werden, die ihn nicht interessieren. Eine gute Referenz aus derselben Branche kann helfen, den Bedarf beim Gegenüber zu wecken und Ihre Vermutung zu untermauern.

- ✓ Passenden Zeitpunkt anhand von Signalen auswählen:

  Ideal ist es, wenn Sie sich auf einen konkreten Anlass oder Grund beziehen können, warum gerade jetzt Ihre Ansprache legitim ist. Hier helfen Ihnen die von Echobot gelieferten Business-Signale:

Anhand einer aktuellen Meldung, eines Artikels oder Weblinks können Sie damit akute Gesprächsanlässe, wie z.B. Neubauten, Managementwechsel oder Stellenausschreibungen, finden. Dies hilft nicht nur der Dokumentation, sondern garantiert auch, dass Sie sich zum richtigen Zeitpunkt reinmelden. Denn durch den so erkannten Bedarf und die zielgerichtete Ansprache steigern Sie deutlich Ihre Erfolgschancen.

Beispiele:

Messebesuch Ereignis am: 01.01.2018 | 7 weitere

08.08.2018 Echobot auf der dmexco 2018: Highlights und Termine ... Auch auf der dmexco 2018 erweitern wir die Kernkompetenzen an unserem Stand durch Partner. Tauschen Sie sich mit der B2B Sales & Marketing Intelligence Agentur Phocus Direct Communication darüber aus, wie Sie traditionelle Marketing- und Vert... - https://www.echobot.de (Weniger)

Managementwechsel | 3 weitere

04.09.2018 Grass hat Geschäftsführung auf vier Mitglieder erweitert 04.09.2018 – Der zur Würth-Gruppe gehörende österreichische Funktionsbeschlägehersteller Grass hat Albert Trebo mit Wirkung zum 1. September zum neuen Geschäftsführer Marketing und Vertrieb ernannt. - https://www.euwid-holz.de ... (Mehr)

Neubauten & Erweiterungen | 1 weitere

03.09.2018 Filigraner Bau wird Blickfang - Fränkische Nachrichten Unternehmen Würth investiert rund 7,1 Millionen Euro in Hochregallager am Standort Künzelsau-Gaisbach Filigraner Bau wird Blickfang Von der B 19 aus ist zu sehen, wie das Stahlgerippe für die Erweiterung des Würth-Palettenhoch - https://www.fnweb.de ... (Mehr)

7. INTERESSENSABWÄGUNG

Eine Interessensabwägung sieht der Gesetzgeber immer dann vor, wenn es widersprüchliche Interessen gibt, die nicht durch einfache Vorschriften klar geregelt werden können, sondern bei denen es auf die Umstände oder die Gesamtschau der konkreten Situation ankommt.

Leider führen gerade solche Fälle häufig zu Rechtsstreitigkeiten, da natürlich jede der Parteien sich im Recht sieht. Eine Klarstellung erfolgt in Fällen der Interessensabwägung immer erst durch mehrere aufeinanderfolgende Urteile möglichst hoher Instanzen, die sich einem gleichen Grundtenor anschließen. Man nennt dies dann „herrschende Rechtsmeinung". Durch die veröffentlichten Urteile und die darin dargelegten Entscheidungsgründe wird dann erst klar, wie die Jurisdiktion solche Grenzfälle einschätzt und worauf es ankommt. Es kann helfen, wenn Sie sich am oben dargestellten Prüfschema orientieren und zusätzlich den Erwägungsgrund Nr. 47 heranziehen. Darin heißt es zum Thema des berechtigten Interesses auszugsweise:

> Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z.B. wenn die betroffene Person ein Kunde des Verantwortlichen ist…

Hat jemand in der Vergangenheit bei Ihnen etwas bestellt oder eine angemessene Beziehung aufgebaut, z.B. sich ein Angebot kalkulieren lassen, stehen die Chancen gut, dass für eine Weiterverarbeitung der Daten ein berechtigtes Interesse vorliegt. Eine angemessene Beziehung kann aber auch bedeuten, dass eine Verbindung zwischen den Parteien besteht, zum Beispiel über gemeinsame Kontakte, wie Sie in XING oder LinkedIN dargestellt werden. Wird der Kontakt dann sogar über eine Empfehlung der verbindenden Person aufgebaut, ist dies ein deutlich positiver Hinweis.

> Auf jeden Fall wäre das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird.

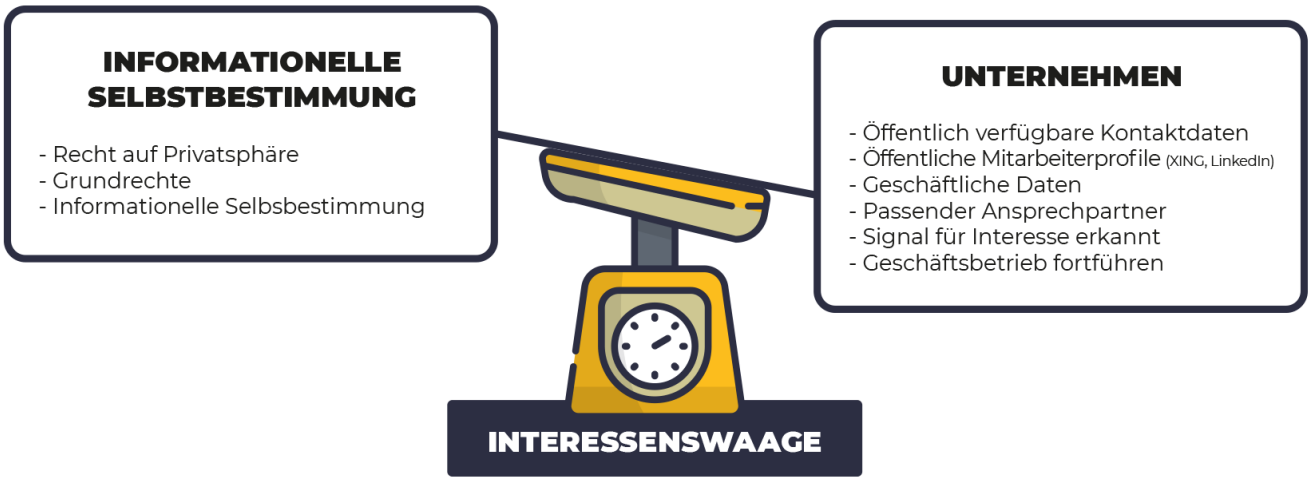
Dieser Satz ist deswegen interessant, da sich über ihn diverse Vorgehensweisen legitimieren lassen: Schreibt jemand beispielsweise seine geschäftliche Telefonnummer oder E-Mail-Adresse öffentlich auf seine Webseite, so kann er vernünftigerweise absehen, dass diese auch verwendet wird. Vorsicht jedoch, wenn auf der Webseite auf eine Zweckbindung hingewiesen wird (z.B. technische Kundenhotline). In einem solchen Falle wäre die Nutzung eines solchen Kanals gerade nicht im Interesse des Betroffenen, da Ihre Anfrage seine Erreichbarkeit für Kunden einschränkt. Solange aber kein Zweck genannt wird, kommt es auf die „Üblichkeiten" an, die der Betroffene erwarten muss. Was üblich ist liegt jedoch nicht im Ermessen eines Beschwerdeführers, sondern hängt davon ab, was ein Gericht als „üblich" ansieht. Konkret heißt das, dass es im Falle der Telefonnummer von der Webseite auf die Auslegung des jeweiligen Gerichts ankommt.

Betreibt eine Person jedoch ein öffentlich einsehbares Profil in einem geschäftlichen Social-Media-Netzwerk, wie Xing oder LinkedIN, so kann jeder mittels Kontaktanfrage eine Geschäftsanbahnung

starten. Da solche Netzwerke explizit für diesen Zweck existieren, ist dies für den Betroffenen eindeutig absehbar.

> Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.

Sehr zur Freude von Mitarbeitern in Vertrieb und Marketing steht hier noch einmal explizit, dass auch Direktwerbung gerade als berechtigtes Interesse für eine Datenverarbeitung gelten kann. Ob und über welchen Kanal Sie dann aber zur Kontaktaufnahme berechtigt sind, regelt allerdings nicht die DSGVO im Allgemeinen. Mehr dazu lesen Sie in Kapitel 8.



Ob man die Personendaten eines potentiellen Kunden für die Kaltakquise nutzen darf oder nicht, hängt also davon ab, welche Situation vorliegt und ob das Interesse des Unternehmens oder das Interesse der Person höher zu bewerten ist.

Auf der Ebene der Grundrechte treffen hier einerseits das Recht auf informationelle Selbstbestimmung (also die Hoheit über seine eigenen Daten zu behalten) und das Recht auf den eingerichteten und ausgeübten Geschäftsbetrieb (also die Gewinnerzielungsabsicht der Unternehmen) andererseits aufeinander.

Aber nicht nur rechtliche, sondern auch tatsächliche, wirtschaftliche oder ideelle Interessen werden vom entscheidenden Richter hier im Zweifelsfall berücksichtigt. In der folgenden tabellarischen Gegenüberstellung versuchen wir Ihnen eine Orientierung und Hinweise zu geben, welche Abwägungsgründe berücksichtig werden können:

Erwägungsgründe, die für die betroffene Person sprechen:	Erwägungsgründe, die für das verarbeitende Unternehmen sprechen:
Der Betroffene muss mit der Datenverarbeitung vernünftigerweise rechnen.	Der Betroffene muss mit der Datenverarbeitung vernünftigerweise rechnen.
Es erfolgt ein umfassendes Profiling.	Der Betroffene erhält die Möglichkeit, der Datenverarbeitung zu widersprechen.
Die Datenverarbeitung hat relevante Nachteile für den Betroffenen (z.B. schlechteres Angebot).	Es gibt keine relevanten Nachteile für den Betroffenen aus der Datenverarbeitung.
Die betroffenen Daten sind privat und nicht öffentlich kommuniziert.	Die betroffenen Daten sind offensichtlich öffentlich einsehbar.
Die betroffenen Daten sind sensibel oder nicht allgemeiner Natur (besondere Kategorien).	Die betroffenen Daten sind unsensibel, allgemeiner Natur oder beziehen sich auf die geschäftliche Tätigkeit (z.B. Firmen-E-Mail)
Die Parteien standen vorher noch nie in Kontakt.	Es bestand oder besteht eine Beziehung zwischen Person und Unternehmen – oder es kam zu einer Empfehlung.
Die Datenverarbeitung und Ansprache erfolgt ohne ersichtlichen Anlass.	Es existiert eine Ausschreibung oder ein konkreter Anlass, auf die sich als Grund der Datenverarbeitung bezogen wird.
Die Person wird durch den Missbrauch ihrer Daten häufig (ggf. auch in ihrem eigenen Geschäftsbetrieb) gestört.	Die Ansprache erfolgt individuell und sorgfältig und nicht in Form einer Massenverarbeitung.
Die Person hat sich in eine öffentliche DoNotContact-Liste eintragen lassen.	Die Person kommuniziert ihre Daten öffentlich mit Hinweis zur Kontaktaufnahme.
Die Verantwortlichen sammeln Daten auf Vorrat, ohne diese konkret zu begründen.	Die Verantwortlichen können den Zweck jeder Datenverarbeitung genau nachweisen.
Der Zweck der Verarbeitung wurde verschleiert oder liegt in einem anderen als dem offensichtlichen Aspekt.	Der Kunde weiß genau, worauf er sich einlässt, wenn er der Verarbeitung seiner Daten zustimmt.

8. WIE KANN ICH DIE DATEN ZUR KONTAKTAUFNAHME NUTZEN?

WICHTIGE UNTERSCHEIDUNG:
Auch wenn Sie Daten DSGVO-konform gespeichert haben und verarbeiten, berechtigt dies nicht automatisch zur Ansprache / Kontaktaufnahme. An dieser Stelle kommt zusätzlich das Gesetz gegen unlauteren Wettbewerb (UWG) ins Spiel.

Diese Abgrenzung wird häufig nicht ganz klar vorgenommen, weshalb in der Praxis viele die Anforderungen durcheinanderwerfen. Hat ein Kunde zur Datenverarbeitung eingewilligt, heißt das aber nicht automatisch, dass Sie ihm jetzt E-Mails zusenden dürfen. Die Verarbeitung ist zwar die Grundlage, aber je nach Form des Kontaktkanals benötigen Sie noch zusätzliche Genehmigungen (Opt-Ins). Die Datenschutzgrundverordnung regelt nur Speicherung und Verarbeitung personenbezogener Daten. Rechtskonform erhobene Daten sind somit nur der erste Schritt auf dem Weg zum Vertriebserfolg.

Kontaktaufnahme – so geht´s

Um per E-Mail, Brief, Telefon oder auf sonstigem Weg mit den Personen in Kontakt zu treten, gelten weitere Voraussetzungen, wie sie z.B. im Gesetz gegen unlauteren Wettbewerb (UWG) geregelt sind.

Insbesondere betrifft Sie in diesem Fall die Regelung in §7, die bestimmt unter welchen Voraussetzungen Sie Kunden, Interessenten oder sonstige Marktteilnehmer ansprechen dürfen, damit keine unzumutbare Belästigung von deren eingerichtetem und ausgeübtem Geschäftsbetrieb vorliegt.

Hinweis: Die folgenden Abhandlungen beziehen sich insbesondere auf den Erstkontakt mit einer Person. Sobald Sie von dieser eine Antwort erhalten haben, können Sie erkennen, ob ein weiterer Kontakt legitimiert werden kann oder besser unterlassen werden sollte. Denn besteht kein Interesse an Ihrem Angebot oder verlangt der Betroffene nicht mehr kontaktiert zu werden, steigt die Gefahr für eine Abmahnung noch weiter.

Erhalten Sie beim Erstkontakt jedoch positive Rückmeldung oder sogar die Bitte nach weiteren Informationen, dann können Sie sich im Folgenden ggf. schon auf vorvertragliche Maßnahmen für die Datenverarbeitung stützen (vgl. Kapitel 6) und dem Kunden ein Opt-In zur Bestätigung zukommen lassen.

Bei der Auswahl des passenden Mediums sollten Sie auch die Dringlichkeit abwägen. Als Vertriebsmitarbeiter haben Sie es selbstverständlich eilig, neue Kunden zu finden. Wie zeitkritisch ist Ihr Anruf oder Ihre E-Mail aber für den Betroffenen? Würde im Zweifel auch der Postweg für Ihr Anliegen ausreichen? Um die Auswahl eines Telefonats zu begründen, kann es nützlich sein, sich auf einen aktuellen Anlass bei einem Unternehmen zu beziehen: Wird zum Beispiel händeringend ein qualifizierter Mitarbeiter gesucht, können für Sie als Personaldienstleister wenige Tage schon entscheidend sein.

Kontaktaufnahme per Post / Brief

Auch wenn er heute nahezu vergessen wird und in der Praxis nur vereinzelt, z.B. für die Versendung von Verträgen und Rechnungen, Verwendung findet – der Brief ist ein persönliches Kommunikationsmittel, das sogar nach UWG grundsätzlich zulässig ist. Es sei denn, der Empfänger widerspricht durch z.B. Aufkleber auf dem Briefkasten. Das gilt jedoch für alle auf dem Postweg versendeten Formate, wie Postkarten, Kataloge oder Wurfsendungen.

Letztendlich bleibt die postalische Kontaktaufnahme mehr dem Marketing überlassen und stellt den Vertrieb eher vor eine Kosten-, Zeit- und Nutzenabwägung. In den meisten Unternehmen zählt der Akquisebrief nicht mehr zu den gängigen Kontaktformen. Zudem ist er im Vergleich teurer und die Konversionsrate häufig schlecht. In manchen Branchen kann er aber durchaus Sinn machen, zumindest um die Hürde des Erstkontakts zu überwinden.

Beispiel: Sie bieten umfangreiche und personalisierte Leistungen an, wie die Erstellung von Geschäftsberichten für Unternehmen. Dann können Sie Ihre Leistungen über einen personalisierten Brief und ein individuelles Angebot samt hochwertig produzierter Broschüre herausstellen.

Zu beachten: Versuchen Sie nicht, den Empfänger in die Irre zu führen, z.B. mit einem Hinweis „vertraulich“. Verwenden Sie neutrale oder als Werbung gekennzeichnete Briefumschläge, d.h. marken- oder produktspezifisch bedruckt. Auch in Ihrem Interesse: Geben Sie immer Ihr Unternehmen mit vollständigen Kontaktdaten als Absender an.

Kontaktaufnahme per Telefon

Grundsätzlich fordert §7 Abs. 2 Nr. 2 UWG für die telefonische Kontaktaufnahme eine Einwilligung, lässt aber auch die Möglichkeit einer „mutmaßlichen Einwilligung“ offen, sofern es sich nicht um Verbraucher, sondern um geschäftliche Kontakte handelt.

Auf diesen Abschnitt stützt sich letztendlich jeder Kaltakquise-Anruf. Das Gesetz verlangt von Ihnen, dass Sie sich vorher mit den Bedürfnissen des potentiellen Interessenten auseinandersetzen. Sie sollen erkennen können, bei wem Ihr Angebot in Frage kommt und nicht eine willkürlich erstellte Liste abtelefonieren. Echobot kann Ihnen dabei helfen, konkrete Zielgruppen herauszuarbeiten.

Mutmaßliche Einwilligung erkennen

Diese Passage lässt natürlich wieder Spielraum offen und stellt Sie als Vertriebler vor die Frage: „Wann kann ich von einer mutmaßlichen Einwilligung ausgehen?“ Hierfür haben wir wieder einige Ansatzpunkte gesammelt, an denen Sie sich orientieren können:

- ✓ **Branchenbezug**: bei Produkten, die besonders für bestimmte Branchen in Frage kommen, z.B. landwirtschaftliche Nutzfahrzeuge an Landwirte vorstellen
- ✓ **Zeitbezug**: bei Angeboten, die Firmen in regelmäßigen Abständen nutzen, z.B. Steuerberater zur Erstellung des Jahresabschlusses

- ✓ **Personenbezug**: bei Produkten, die nur von bestimmten Personengruppen genutzt werden, z.B. Softwaretools für die Personalverwaltung an HR-Mitarbeiter bewerben
- ✓ **Anlassbezug**: bei Angeboten, die bei bestimmten Anlässen gefragt sind, z.B. Ausschreibungen oder Business Signale

PRAXISTIPP:

Es gibt noch einige mehr Hinweise, die Sie nutzen können, um potentielle Interessenten zu finden und einen Telefonanruf zu rechtfertigen. Bei Echobot werden solche Akquisegründe automatisch erkannt und bereitgestellt (Beispiel: Sie sind eine Webdesign-Agentur und adressieren Kunden, die ein bestimmtes CMS, wie z.B. Wordpress, einsetzen).

Wenn Sie sich an solchen Hinweisen orientieren, können Sie darauf schließen, wann Ihr Angebot im wirtschaftlichen Interesse einer Firma liegen kann. Das kann einerseits Ihre Erfolgsquote nach oben treiben, ganz nebenbei können Sie auch aus rechtlicher Sicht die mutmaßliche Einwilligung besser begründen.

Gleiches Recht für Call-Center?

Möchten Sie Call-Center oder externe Agenturen mit der telefonischen Akquise beauftragen, dann gelten aus UWG-Gesichtspunkten die gleichen Vorschriften. Wenn Sie allerdings personenbezogene Daten weitergeben oder sogar den Zugriff auf Ihre Kundendatenbank gewähren, müssen Sie unbedingt einen Auftragsverarbeitungsvertrag (AVV) abschließen. Wir empfehlen zudem eine Zusammenarbeit mit Anbietern aus der EU.

Darf man Gespräche aufzeichnen?

Wenn Sie künftig Gespräche zu Schulungszwecken oder aus Nachweisgründen aufzeichnen möchten, verlangt die DSGVO eine aktive Einwilligung. Ihre Ansage muss also lauten: „Wir möchten das Gespräch gerne zu Schulungszwecken aufzeichnen. Wenn Sie damit einverstanden sind, drücken Sie die Raute-Taste.“ **Wichtig**: Auch Ihr Mitarbeiter ist eine Person und muss hierzu einwilligen.

KOMMENTAR RECHTSANWALT DR. CARSTEN ULBRICHT:

„Die Rechtsprechung ist in Bezug auf die Voraussetzungen einer mutmaßlichen Einwilligung eher restriktiv. Der bloße Bedarf an einer Ware oder Dienstleistung soll also nicht ohne Weiteres genügen. Vielmehr muss hinzukommen, dass der Angerufene mutmaßlich zum aktuellen Zeitpunkt (Anlass) gerade auch mit einer telefonischen Werbung einverstanden sein wird. Das Risiko einer Fehleinschätzung trägt der Werbende.“

Kontaktaufnahme per E-Mail

Bei der Flut an E-Mails, die im Tagesgeschäft anfallen, scheinen die strengen Regelungen des UWG ein Segen zu sein. Das gilt aber nur für den vermeintlichen Empfänger. Für Sie im Vertrieb wird Ihre Arbeit durch harte Vorgaben stark erschwert, zumal sich Wettbewerber aus dem Ausland häufig gerade nicht an die für Deutschland geltenden Regelungen halten. Allgemein gilt, dass für E-Mails mit werblichem Charakter eine ausdrückliche Erlaubnis des Empfängers per Double-Opt-In vorliegen muss.

Wann gilt eine E-Mail als „Werbung“?

Der Werbebegriff wird vom Gesetz sehr weit ausgelegt. So kann schon ein Link auf Ihre Webseite in der Signatur ausschlaggebend sein, wenn auf der Homepage Ihre Leistungen und Angebote beschrieben werden. Auch die Aufmachung des Anschreibens und der Inhalt sind zu berücksichtigen, wenn diesen ein kommerzielles Interesse zu Grunde liegt, was in der Regel der Fall ist. Dass sich hier auch die Gerichte oft nicht einig sind, sieht man zum Beispiel an per E-Mail versendeten Bewertungsanfragen. Während das Landgericht Coburg 2012 und das LG Berlin 2013 die Bitte um Kundenbewertung als zulässig ansahen, hat das Amtsgericht Hannover und aktuell das Kammergericht Berlin dies auch als unzulässige Belästigung angesehen (Stand 09/2018).

Was bedeutet “Double-Opt-In”?

Dieses Verfahren wird in der Praxis zum Beispiel für Newsletter-Anmeldungen genutzt. Per Klick auf einen Bestätigungslink wird sichergestellt, dass kein Dritter beliebige E-Mail-Adressen für den Werbeversand anmeldet, sondern der tatsächliche Empfänger auch ausdrücklich eingewilligt hat. Für den Erstkontakt ist dieses Verfahren also nicht geeignet.

PRAXISTIPPS im Grenzbereich:

Besonders wenn Sie E-Mails im Erstkontakt trotzdem unbedingt verwenden wollen, müssen Sie immer mit Abmahnungen rechnen. Folgende Tipps können Ihr Abmahnrisiko eventuell reduzieren:

1. **Kollegentrick**
   Wenn Sie Ihren Ansprechpartner telefonisch nicht erreichen können, lassen Sie sich vom Sekretariat oder einem Kollegen dessen E-Mail-Adresse geben. Beziehen Sie sich gleich im ersten Satz namentlich auf den Kollegen/die Kollegin: „Hallo Herr X, Frau Y hat mich gebeten Ihnen eine E-Mail zu schreiben …“

2. **Textmail Dialog**
   Halten Sie Ihr Anschreiben individuell, persönlich und kurz. Verzichten Sie auf Bilder, Anlagen, Links und werblichen Inhalt. Sobald ein Dialog zustande gekommen ist, können Sie Ihr Anliegen vorsichtig vorbringen.

Allgemein gilt also: Je weniger werblich und je persönlicher eine E-Mail formuliert ist, desto geringer ist auch Ihr Abmahnrisiko. Verschleiern oder verbergen Sie auf keinen Fall den Absender, sondern fügen Sie immer korrekt Ihre Firmen- und Kontaktdaten ein.

Übrigens: Haben Sie eine E-Mail-Adresse im Zusammenhang mit einem vorherigen Vertragsabschluss erhalten, dürfen Sie diese auch für Cross- und Up-Selling nutzen, solange es sich um eigene ähnliche Produkte oder Dienstleistungen handelt und der Kunde dem nicht widersprochen hat.

Vorsicht bei gekauften E-Mail-Adressen mit Einwilligung: Wie das OLG Düsseldorf in seinem Urteil (Az. I-20 U 137/09) vom 24.11.2009 festgehalten hat, dürfen Sie sich nicht auf allgemein gehaltene Zusicherungen eines Verkäufers verlassen. Das Haftungsrisiko geht in diesem Fall auf Sie über.

Kontaktaufnahme per Social-Selling (XING, LinkedIn ...)

Man könnte fast meinen, dass sich mit Social Selling eine Art Schlupfloch gefunden hat, in dem die Kontaktaufnahme rechtlich noch nahezu ohne Einschränkungen möglich ist. Soziale Netzwerke bieten heute ganz neue Möglichkeiten Geschäftskontakte zu knüpfen und zu pflegen. Dabei gibt es neben Facebook und Twitter auch rein geschäftliche Netzwerke, wie XING oder LinkedIn, bei denen sich die Chance ergibt, eine Kontaktanfrage zu starten.

Kontaktaufnahme: Was darf ich?

Die meisten sozialen Netzwerke erlauben Ihnen erst dann einen anderen Nutzer mit persönlicher Nachricht zu kontaktieren, nachdem er Ihre Kontaktanfrage angenommen hat. Mit dieser Anfrage holen Sie sich sozusagen das Einverständnis, den Nutzer zu kontaktieren. In der Anfrage können Sie in der Regel bereits Ihr Anliegen kommunizieren, was es dem Betroffenen leichter macht eine Entscheidung zu treffen. Oftmals werden dadurch auch weitere Profilinformationen für Sie sichtbar.

Wir empfehlen Ihnen in Analogie des Erwägungsgrunds 47 jedoch darauf zu achten, womit der Betroffene typischerweise rechnen kann: Während man im Business-Netzwerken wie XING oder LinkedIN mit geschäftlichen Anfragen rechnen kann, ist bei eher privaten Anbietern wie Facebook größere Vorsicht geboten. Es sei denn, der Betroffene betreibt auf einer solchen Plattform auch ein klar als gewerblich gekennzeichnetes Profil mit Kontaktmöglichkeit.

Soziale Netzwerke als Datenlieferant?

Jeder Nutzer kann im Netzwerk selbst verwalten, welche Daten er preisgibt und für welchen Kreis sie verfügbar sind. Befinden Sie sich also in der Kontaktliste des Betroffenen, dann ist ihm bewusst, dass Sie seine Daten einsehen können. Jetzt stellt sich nur die Frage, ob Sie diese Daten auch in Ihre Datenbank übertragen dürfen. Da es auch zu diesem Thema bislang keinerlei Rechtsprechung gibt, empfehlen wir Folgendes:

Sobald der Betroffene seinen Profilstatus auf „öffentlich“ gestellt hat und die Daten für jeden einsehbar sind, gelten die gleichen Regeln, wie bei der Erhebung aus öffentlichen Quellen. Betreibt er aber ein privates Profil, das Sie nur einsehen können, weil Sie sich in seiner Kontaktliste befinden, sehen Sie von einer Übertragung ab. In gewisser Weise stellt er Ihnen die Daten zwar selbst zur Verfügung, jedoch zu dem Zweck, den er im Netzwerk angegeben hat. Denken Sie auch hier daran, den Betroffenen gegebenenfalls über die Datenverarbeitung zu informieren.

CHECKLISTE

9. ALLGEMEINE TIPPS ZUR RISIKOMINIMIERUNG

- ✓ **Art der Ansprache**
  Wählen Sie eine individuelle Einzelansprache mit korrekter persönlicher Anrede. Niemand möchte Teil eines Massenmailings sein.

- ✓ **Vorsicht vor Formatfehlern**
  Wenn Sie dennoch Serienbriefe oder Marketing-Automation einsetzen, achten Sie darauf, dass die Platzhaltertexte auch korrekt ausgefüllt werden und sich korrekte Sätze ergeben. Eine Anrede, wie „Sehr geehrter [Müller]“, sorgt bei vielen Empfängern direkt für Ärger.

- ✓ **Einwilligung** (vgl. Kapitel 8)
  Hat Ihr Interessent die Einwilligung zur Ansprache in der gewünschten Form gegeben oder können Sie diese zumindest glaubhaft und über dokumentierte Nachweise vermuten?

- ✓ **Adressat prüfen**
  Ist die angesprochene Person tatsächlich der designierte Empfänger oder kann es sein, dass die Ansprache bei einer anderen Person landet? In diesem Fall sollten Sie solche Datensätze lieber aussortieren.

- ✓ **Kanal** (vgl. Kapitel 8)
  Prüfen Sie, ob Ihr genutzter Kanal (Persönlich, Brief, Telefon, Business-Netzwerk, E-Mail) für die Ansprache zulässig ist.

- ✓ **Bestehender Bezug** (vgl. Kapitel 6)
  Prüfen Sie, ob eine vorvertragliche Maßnahme besteht, es sich um eine Empfehlung handelt oder berechtigtes Interesse vorliegt.

- ✓ **Relevanter Aufhänger / konkreter Bezug**
  Binden Sie ein aktuelles Signal, eine Neuigkeit oder einen Hinweis in die Ansprache mit ein: „Ich melde mich heute bei Ihnen, WEIL …“

- ✓ **Informationsminimierung** (vgl. Kapitel 3)
  Löschen Sie vor einer Ansprache Felder und Werte, die Sie nicht benötigen. Ihre Anfrage könnte ein Auskunftsbegehren auslösen.

- ✓ **Zweckgebundenheit** (vgl. Kapitel 3)
  Können Sie einen konkreten Zweck für jeden Datensatz und jede Verwendung angeben?

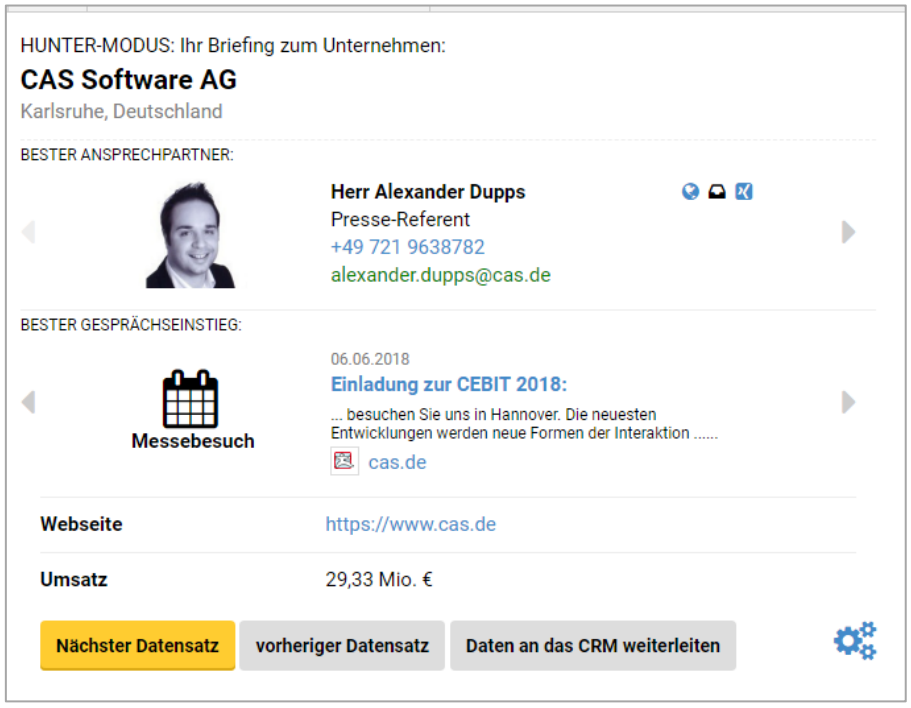
- ✓ **Informationspflicht** (vgl. Kapitel 3)
  Denken Sie daran, den Nutzer spätestens beim ersten Kontakt auf die Verarbeitung seiner Daten hinzuweisen und einen Link zu Ihrer aktuellen Datenschutzerklärung einzufügen.

- ✓ **Holen Sie sich rechtlichen Rat**
  Zwar werden Sie ernüchtert sein, was in Deutschland mittlerweile alles verboten ist, jedoch wissen Sie dann zumindest auf welche Risiken Sie sich ggf. einlassen.

BEST PRACTICE

10. DATEN-STREAMING MIT DEM ECHOBOT „HUNTER MODUS“

Wie Sie an Inhalt und Umfang dieses Dokuments erkennen können, ist es, gerade im Bereich der B2B-Kaltaquise, nicht ganz leicht ein DSGVO-konformes Vertriebsvorgehen umzusetzen. Daher haben wir eine Echobot-Lösung entwickelt, welche die oben genannten Grundprinzipien datenschutzkonformer Vertriebsarbeit berücksichtigt und zugleich darauf ausgelegt ist, die Vertriebseffizienz signifikant zu steigern. Das Ergebnis ist der sogenannte „Hunter Modus“ in Echobot CONNECT:



Der Hunter Modus basiert auf folgenden Überlegungen:

- ✓ Daten von Firmen und Personen Ihrer Zielgruppe werden gar nicht erst in Ihren Systemen gespeichert, sondern existieren in der Echobot-Cloud-Plattform.
- ✓ Der Zugriff darauf erfolgt in Echtzeit über eine „Streaming“-Lösung direkt im Browser.
- ✓ Zu jedem personenbezogenen Datum wird automatisch ein Link zu einer offensichtlich öffentlichen Quelle angezeigt, um auf Rückfragen des Kunden direkt reagieren zu können.
- ✓ Daten übertragen Sie per Download/Sync erst dann in Ihre eigenen Systeme, wenn Sie im selben Moment ein Interesse des Kunden nachweisen und dokumentieren können.
- ✓ Es werden zusätzlich weitere für den Pitch relevante Business-Signale angezeigt, damit Ihr Vertrieb einen konkreten Gesprächseinstieg, bzw. Verkaufsanlass erhält.
- ✓ Das System wählt mit Hilfe künstlicher Intelligenz automatisch den relevantesten Kontakt und geeignete Informationen aus, ohne Ihren Vertrieb zu überfordern.

So wird eine schnelle und effiziente Vertriebsarbeit mit hoher Schlagzahl möglich. Gerne können Sie den Echobot Hunter Modus testen. Eine Integration und Synchronisation ist dabei mit vielen CRM-Systemen möglich. Wenden Sie sich an unseren Vertrieb unter: +49 (721) 500 57 501.

HERAUSGEBER

ÜBER ECHOBOT

Das Technologieunternehmen Echobot Media Technologies GmbH aus Karlsruhe entwickelt Online-Software für die Informationsaggregation und Analyse externer Daten. Die Experten für Business Information Intelligence helfen über 1.000 Firmen aller Branchen und Größen, mehr über ihre Marken, Märkte und Zielgruppen zu erfahren. Milliarden digitaler Inhalte werden in Echtzeit analysiert und geschäftsrelevante Daten und Informationen für verschiedenste Unternehmensbereiche bereitgestellt. Weitere Informationen auf www.echobot.de

Über Dr. Carsten Ulbricht

Dr. Carsten Ulbricht ist ein auf Internet und die digitale Transformation spezialisierter Rechtsanwalt bei der Kanzlei Bartsch Rechtsanwälte (Standorte Karlsruhe, Frankfurt und Stuttgart) mit den Schwerpunkten IT-Recht, Marken-, Urheber- und Wettbewerbsrecht sowie Datenschutz. Im Rahmen seiner anwaltlichen Tätigkeit berät Dr. Ulbricht nationale und internationale Mandanten in allen Rechtsfragen des E- und Mobile-Commerce sowie zu allen Themen im Bereich Social Web. Seine Schwerpunkte liegen dabei auf der rechtlichen Prüfung internetbasierter Geschäftsmodelle und Vermeidung etwaiger Risiken bei Aktivitäten in und über die Sozialen Medien, datenschutzrechtlichen Themen aber auch dem Umgang mit nutzergenerierten Inhalten. Neben seiner Referententätigkeit berichtet er seit dem Jahr 2007 regelmäßig in seinem Weblog zum Thema „Web 2.0, Social Media & Recht“ unter www.rechtzweinull.de nicht nur über neueste Entwicklungen in Rechtsprechung, Diskussionen in der Literatur und über eigene Erfahrungen, sondern analysiert auch Internet-Geschäftsmodelle und -projekte auf ihre rechtlichen Erfolgs- und Risikofaktoren.

Noch Fragen?

Gerne unterstützen wir Sie auch über diesen Leitfaden hinaus, Ihren Vertrieb DSGVO-konform zu optimieren und praktisch auf Knopfdruck neue Kunden zu generieren. Wir freuen uns auf Ihren Anruf oder Ihre E-Mail.

Telefon: **+49 (0) 721 - 500 57 500**
E-Mail: service@echobot.de
Webseite: https://www.echobot.de/

Herausgeber:
Echobot Media Technologies GmbH
Südendstr.52
D-76135 Karlsruhe
Bastian Karweg (Geschäftsführer)

Kommentar von:
Kanzlei Bartsch Rechtsanwälte
Dr. Carsten Ulbricht
(Rechtsanwalt)