Michael Rohrlich

Datenschutz einfach umsetzen

Der Praxisratgeber zur DSGVO für Selbstständige und kleine Unternehmen

Wolters Kluwer | Steuertipps

Datenschutz einfach umsetzen

Der Praxisratgeber zur DSGVO für Selbstständige und kleine Unternehmen

Michael Rohrlich

Akademische Arbeitsgemeinschaft | Mannheim

Postfach 10 01 61 · 68001 Mannheim
Telefon 0621/8626262
Telefax 0621/8626263
www.akademische.de

1. Auflage

Stand: Januar 2023

Zum Zwecke der besseren Lesbarkeit verwenden wir allgemein die grammatisch männliche Form. Selbstverständlich meinen wir aber bei Personenbezeichnungen immer alle Menschen unabhängig von ihrer jeweiligen geschlechtlichen Identität.

Redaktion: Dr. Torsten Hahn, Benedikt Naglik, Annette Winkler

Geschäftsführer: Christoph Schmidt, Stefan Wahle

Layout und Umschlaggestaltung: futurweiss kommunikationen, Wiesbaden

Bildquelle: ©lassedesignen – stock.adobe.com

Printed in Poland

ISBN 978-3-96533-286-7

Alternative Streitbeilegung (Online-Streitbeilegung und Verbraucherschlichtungsstelle)
Die Europäische Kommission hat eine Plattform zur Online-Streitbeilegung eingerichtet, die unter folgendem Link abgerufen werden kann: www.ec.europa.eu/consumers/odr.
Wolters Kluwer ist nicht bereit und nicht verpflichtet, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen.

Vorwort

Mit dem Thema Datenschutz müssen sich alle Unternehmen auseinandersetzen, vom Solo-Selbstständigen über kleine und mittlere Betriebe bis zum Großunternehmen.

Und trotzdem ist Datenschutz und vor allem die EU-Datenschutzgrundverordnung (DSGVO) auch im sechsten Jahr ihrer Anwendbarkeit für viele noch ein rotes Tuch. Denn aus Unternehmenssicht hat dieses Gesetz eine Vielzahl von neuen Dokumentationspflichten sowie bürokratischer Hürden mit sich gebracht. Außerdem sieht sich der Datenschutz häufig dem Ruf ausgesetzt, ein »Verhinderer« von innovativen Technologien zu sein.

Datenschutz sollte jedoch nicht nur als unausweichliche Pflicht im Betriebsalltag sondern auch als Chance eines jeden Unternehmers verstanden werden!

Ihre Kunden, Mitarbeiter und Vertragspartner müssen darauf vertrauen können, dass die zur Verfügung gestellten personenbezogenen Daten bei Ihnen in guten Händen und geschützt sind. Nur so ist ein erfolgreiches Miteinander gewährleistet. Die Umsetzung der Datenschutzvorgaben im eigenen Betrieb schützt auf der einen Seite vor kostspieligen Fehlern - umgekehrt werden aber auch die Daten des eigenen Betriebs geschützt.

Im Bereich Datenschutzrecht gibt es seit Einführung der DSGVO immer wieder Neuerungen, etwa durch neue Gesetze oder Gerichtsentscheidungen.

Der Inhalt dieses Ratgebers erfasst die Rechtslage bis einschließlich Januar 2023. Sie sollten sich regelmäßig über zukünftige Entwicklungen informieren.

In diesem Ratgeber finden Sie einen fundierten Überblick über die verschiedenen Pflichten, welche die DSGVO Ihnen als Unternehmer auferlegt. Praxistipps, Checklisten, Musterformulierungen und weiter Arbeitshilfen, die wir Ihnen auch als Download zur Verfügung stellen, unterstützen Sie, das Thema Datenschutz im eigenen Unternehmen erfolgreich anzugehen.

Rechtsanwalt Michael Rohrlich, Würselen

Alle **Checklisten, Muster und Musterformulierungen** stehen Ihnen auch als Download im Servicebereich des Ratgebers im Internet zur Verfügung.
Hier finden Sie auch alle **weiterführenden Links**.
Der Link zum Servicebereich befindet sich am Ende des Praxisratgebers.

Inhalt

1 Erster Überblick: Worum geht es?

1.1 Weshalb der Datenschutz für Sie wichtig ist

Was ist eigentlich Datenschutz? Warum geht mich Datenschutz als Selbstständiger oder kleines Unternehmen überhaupt etwas an? Müssen sich um Datenschutz nicht nur die großen Unternehmen wie Siemens, Google & Co. kümmern?!

Solche oder ähnliche Fragen werden immer wieder gestellt, wenn es um das Thema Datenschutzrecht geht. Und tatsächlich ist es so, dass das zentrale Gesetz, die **EU-Datenschutzgrundverordnung (DSGVO),** ursprünglich dazu gedacht war, große internationale Unternehmen und deren Umgang mit den persönlichen Daten ihrer Kunden bzw. Nutzer zu regulieren. Sowohl Personen, deren Daten verarbeitet werden, als auch die zuständigen Datenschutzaufsichtsbehörden sollten durch die DSGVO gesetzlich verankerte Möglichkeiten bekommen, um sich gegen rechtswidrige Datenverarbeitung zur Wehr zu setzen und die Entscheidungsbefugnis über ihre persönlichen Daten zu behalten und zu verteidigen.

Und doch ist das Thema Schutz von personenbezogenen Daten auch für Solo-Selbstständige sowie kleine und mittlere Unternehmen immens wichtig. Zum einen, weil es ganz klare gesetzliche Pflichten gibt, die bei Verstößen Sanktionen nach sich ziehen können. Sie können also sich und Ihr Unternehmen vor kostspieligen Fehlern bewahren. Zum anderen können Sie durch eine gute Datenschutzorganisation in Ihrem Unternehmen sehr viel für die Sicherheit Ihrer Daten tun, sodass beispielsweise auch Geschäftsgeheimnisse besser geschützt werden. Und nicht zu vergessen: Mit der Umsetzung von Datenschutzmaßnahmen sollten Sie offensiv umgehen, indem Sie diese z.B. im Rahmen von Kundengesprächen hervorheben. Das ist umso wichtiger, wenn Sie Produkte oder Dienstleistungen anbieten, die ein gewisses Vertrauensverhältnis zwischen Ihnen und Ihren Kunden voraussetzen (z.B. bei Steuerberatern und Unternehmensberatern, bei Anbietern von Coachings, aber auch bei einem Piercing- oder Tattoo-Studio).

1.2 Ziel und Zielgruppe des Ratgebers

Dieser Ratgeber wendet sich nicht nur, aber insbesondere an **kleinere Betriebe, Freiberufler** und **Einzelunternehmer.** Denn im Unterschied zu mittleren oder großen Unternehmen gibt es bei kleineren Unternehmen oder Solo-Selbstständigen in aller Regel keine eigene Rechts-, Datenschutz- oder Compliance-Abteilung, die sich mit den Themen Datenschutz und IT-Sicherheit befasst. Die gesetzlichen Regelungen in diesen Bereichen gelten aber grundsätzlich für alle gleichermaßen, sodass deren Umsetzung zu den Hauptaufgaben des Selbstständigen, des Inhabers bzw. des Geschäftsführers gehört. Bei nur wenigen oder gar keinen Angestellten kommt oft niemand infrage, der offiziell als Datenschutzbeauftragter benannt oder zumindest in diesem Bereich weitergebildet werden kann. Zudem fehlt häufig das Budget, um auf externes Know-how zurückzugreifen.

Wie dem auch sei – die gesetzlichen Verpflichtungen bleiben und müssen umgesetzt werden. Es ist nachvollziehbar, wenn die immens gestiegenen Dokumentationspflichten als lästig und als weitere bürokratische Hürde empfunden werden. Aber hier ist es im Grunde genauso wie mit der Steuererklärung – auch diese ist lästig, muss aber erledigt werden. Es gehört zu den unternehmerischen Pflichten, sich an Recht und Gesetz zu halten. Drohen bei Nichtabgabe einer Steuererklärung Nachzahlungen oder Steuerprüfungen, so droht im Bereich des Datenschutzes gleich von mehreren Seiten Ungemach. Die zuständige Datenschutzaufsichtsbehörde kann prüfen und ggf. Sanktionen erlassen, u.a. auch eine Geldbuße verhängen. Mitbewerber oder Verbraucherinstitutionen können abmahnen und Personen, deren Daten verarbeitet werden, können unter Umständen Schadensersatz bzw. Schmerzensgeld fordern. Die Beachtung und Umsetzung der datenschutzrechtlichen Vorgaben ist insofern zugleich die Erfüllung der Verpflichtung, dem eigenen Unternehmen keinen Schaden zuzufügen. Das gilt umso mehr, wenn das Unternehmen bei Kleinbetrieben und Selbstständigen häufig deckungsgleich mit dem Gründer und Eigentümer ist.

Daher ist es Ziel dieses Ratgebers, Ihnen als selbstständigem Unternehmer das erforderliche Grundwissen im Datenschutz zu vermitteln und Ihnen zugleich **praktische Hilfestellungen und Anleitungen** in Form von Checklisten, Mustern, Vorlagen an die Hand zu geben, die Ihnen die Umsetzung des Datenschutzes in Ihrem Unternehmen erleichtern. Auch unterstützt Sie der Ratgeber mit zahlreichen Verweisen auf Quellen mit weiterführenden Informationen bzw. Materialien – so haben Sie alle notwendigen Ansprechpartner, Anlaufstellen und Tools auf einen Blick zur Verfügung.

Mithilfe dieses Ratgebers erhalten Sie den passenden »Werkzeugkasten«, um im Dschungel des Datenschutzrechts nicht die Orientierung zu verlieren und sich weitgehend selbst »hindurchzukämpfen«. Es gibt sicherlich ein paar Aspekte, die Sie nicht ganz alleine bewältigen können. Aber auch hier erhalten Sie das notwendige Fachwissen, um sich qualifizierte Hilfe zu holen und dann gemeinsam eine passende Lösung zu finden.

1.3 Die Datenschutzgrundverordnung gilt für alle

Nach Maßgabe der im Mai 2016 in Kraft getretenen und 2018 wirksam gewordenen DSGVO müssen **alle Unternehmen, Behörden und Vereine in der Europäischen Union** das Datenschutzrecht beachten. Das bedeutet, sie müssen sich um den sicheren Umgang mit den Daten ihrer Kunden, ihrer Vertragspartner und auch ihrer Mitarbeiter kümmern.

Ziel ist der Schutz von natürlichen Personen bei der Verarbeitung ihrer personenbezogenen Daten in allen Mitgliedstaaten der EU.

Daten von juristischen Personen, also etwa einer GmbH oder einer AG, sind hingegen ausgenommen.

Die Vorgaben der DSGVO gelten nach einer zweijährigen Übergangsphase seit dem 25.5.2018 grundsätzlich für alle gleich, vom Selbstständigen bzw. Einzelunternehmer über mittelständische Betriebe bis hin zu internationalen Großkonzernen. Nur an wenigen Stellen im Gesetz sind Ausnahmen für kleinere Betriebe vorgesehen.

Es kommt also nicht darauf an, wie viele Mitarbeiter Sie haben, in welcher Branche Sie tätig sind, wie Ihre Umsatzzahlen aussehen oder in welcher Unternehmensform Sie organisiert sind. An die Vorschriften der DSGVO müssen sich alle halten, die von Kunden, Mitarbeitern, Vertragspartnern, Bürgern oder Mitgliedern personenbezogene Daten verarbeiten, also erheben, speichern, ordnen, nutzen bzw. auswerten, übermitteln oder löschen.

Erfasst wird somit jeder Selbstständige und jedes Unternehmen mit Kunden und/oder Mitarbeitern.

DSGVO gilt vor nationalem Recht

Die DSGVO regelt den Bereich Datenschutz und geht nationalen Vorschriften, wie etwa dem deutschen Bundesdatenschutzgesetz (BDSG), vor. In speziellen Bereichen und Branchen wird die DSGVO teilweise durch Spezialgesetze ergänzt.

Beispiele:

- Online-Bereich: Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)
- Bereich der Sozialhilfe etc.: Sozialgesetzbücher
- Medizinischer Bereich: u.a. Transplantationsgesetz (TPG)
- Bereich des Steuerrechts: Steuerberatergesetz (StBG)
- Bereich des Arbeitsrechts: Betriebsverfassungsgesetz (BetrVG)

1.4 Weshalb die Relevanz des Datenschutzes steigt

Obwohl die DSGVO bereits seit Mai 2018 in Kraft ist, fällt auf, dass der Datenschutz immer häufiger in den Medien präsent ist und mehr darüber diskutiert wird. Es gibt verschiedene Gründe, weshalb die Relevanz des Datenschutzes gestiegen ist.

Erhöhter Druck durch das Accountability-Prinzip (Nachweisprinzip)

Ein Grund für die zunehmende Relevanz und Wichtigkeit des Datenschutzes ist das mit der DSGVO neu eingeführte sogenannte **Accountability-Prinzip (Nachweisprinzip).** Aufgrund dieses Nachweisprinzips muss Ihnen ein etwaiger Datenschutzverstoß nicht mehr von der Aufsichtsbehörde nachgewiesen werden – vielmehr ist es an Ihnen zu belegen, dass Sie rechtskonform handeln. Dies kommt fast schon einer Beweislastumkehr gleich und hat in der Praxis gravierende Auswirkungen.

Achtung: Es reicht nicht mehr aus, sich datenschutzkonform zu verhalten. Im Zweifel müssen Sie es auch nachweisen können.

Und das wiederum führt zu einem nicht zu unterschätzenden Dokumentationsaufwand. Das mag lästig oder gar überflüssig erscheinen, ist aber nun einmal leider unbedingt notwendig, um Sanktionen zu vermeiden.

Durch Corona hat der Datenschutz an Bedeutung gewonnen

Nicht nur, aber gerade auch aufgrund der Corona-Pandemie hat der Datenschutz mehr und mehr an Bedeutung gewonnen. Viele Unternehmer mit Ladenlokal bieten seit der Pandemie und den verschiedenen Lockdowns verstärkt **Online-Vertrieb, »Click & Collect«**

oder **Lieferservice** an – und behalten dieses Standbein auch ohne Corona-Beschränkungen bei. Aber egal, ob Ihre Kunden die nächste Übergangsjacke, ein Schnitzel oder Bücher online bzw. telefonisch ordern – in jedem Fall müssen Sie als Unternehmer spezielle datenschutzrechtliche Pflichten beachten.

Und auch das Home-Office ist für viele zur Gewohnheit und zu einer nicht mehr wegzudenkenden Arbeitsform geworden. Wenn Ihre Angestellten aber mehr im **Home-Office** arbeiten, hat dies nicht nur arbeits-, sondern vor allem auch datenschutzrechtliche Auswirkungen. Denn der Arbeitnehmer verarbeitet dann die Daten der Kunden, Mitarbeiter oder Vertragspartner des Unternehmens nicht mehr in der geschützten Büro-Umgebung, sondern in seinen Privaträumlichkeiten. Dort ist in der Regel kein allzu hohes IT-Sicherheitsniveau vorhanden. Zudem halten sich im Home-Office, also zu Hause, auch andere Familienmitglieder auf.

2 Diese Grundlagen des Datenschutzes müssen Sie kennen

2.1 Anwendbarkeit des Datenschutzrechts

Die DSGVO sieht vor, dass ihre Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten dienen. Es geht also um **Daten von Menschen,** hingegen werden Daten von Unternehmen genauso wie reine Maschinen- oder Statistikdaten ohne jeden Personenbezug nicht erfasst.

2.1.1 Welche Daten werden von der DSGVO geschützt?

Gemäß Art. 2 Abs. 1 DSGVO gilt die Verordnung

- für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie
- für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder dort gespeichert werden sollen.

In Zeiten immer stärker voranschreitender Digitalisierung geht es in erster Linie um die automatisierte Datenverarbeitung, die mithilfe von Computertechnik im weitesten Sinne erfolgt – unabhängig davon, ob dies mittels Computer, Tablet, Smartphone oder anderen technischen Datenverarbeitungsgeräten geschieht. Außerdem werden auch solche Datenverarbeitungen von der DSGVO erfasst, bei denen Daten zwar nicht automatisiert verarbeitet werden, aber in einem Dateisystem gespeichert werden bzw. werden sollen. Der Begriff »**Dateisystem**« umfasst nicht, wie man vielleicht denken könnte, eine elektronische Datenstruktur in Form von Dateien und Ordnern auf einem Computer. Ein Dateisystem im Sinne der DSGVO meint auch Daten in herkömmlicher Weise, zumeist also in Papierform, die in bestimmter Art und Weise angeordnet sind. Soweit diese Daten,

egal ob handschriftlich oder als Computerausdruck, mithilfe von zumindest zwei Kriterien geordnet werden, gilt dies bereits als Dateisystem.

» Die DSGVO-Vorschriften gelten beispielsweise auch

- bei Papier-Rechnungen, die chronologisch und nach Absendern sortiert in Aktenordnern abgeheftet sind oder
- bei Visitenkarten, die nach Namen und Unternehmen geordnet werden.

Es gibt auch Ausnahmen

Datenverarbeitungen, die den Bereich der EU-Außen- und Sicherheitspolitik betreffen oder solche, die außerhalb des EU-Rechts angesiedelt sind, unterfallen ebenso wenig der DSGVO wie Verarbeitungstätigkeiten der Strafverfolgungs- und Ordnungsbehörden.

Praktisch bedeutsamer als diese Ausnahmen ist jedoch das sogenannte **Haushaltsprivileg.** Wer für rein private Zwecke etwa eine Geburtstagsliste führt, der fällt nicht in den Anwendungsbereich der DSGVO. Wird diese Geburtstagsliste allerdings online offen, z.B. in den sozialen Medien, geführt, greift das Haushaltsprivileg nicht. Denn die konkrete Datenverarbeitung muss nicht nur privaten Zwecken dienen, sondern auch mit privaten Mitteln erfolgen. Wer die Geburtstagsliste also online bereitstellt, sodass sie nicht nur für einen eng begrenzten Personenkreis wie z.B. Familienangehörige, sondern für jedermann frei zugänglich ist, verlässt den rein privaten Bereich und muss sich an alle datenschutzrechtlichen Vorschriften halten.

! Die DSGVO findet bei nahezu allen Datenverarbeitungen Anwendung, die mit der Kerntätigkeit von Unternehmen, Behörden und Vereinen zu tun haben. Insgesamt ist der Anwendungsbereich der DSGVO sehr weit gefasst. In Zweifelsfällen sollten deren Vorgaben also befolgt werden.

2.1.2 Wo gilt die DSGVO überall?

Auch der räumliche Anwendungsbereich der DSVGO ist sehr weit gezogen. Sie findet Anwendung, wenn die verantwortliche Stelle und/oder die betroffene Person ihren Sitz in der Europäischen Union haben.

Es werden somit alle Unternehmen, Behörden und Vereine mit Sitz in der EU erfasst. Zusätzlich gilt die DSGVO beispielsweise auch noch für Unternehmen aus China, Indien, Russland oder den USA, sofern sie Daten von in der EU ansässigen Personen verarbeiten oder diese beobachten. Letzteres kann schon dadurch erfüllt sein, dass auf einer Internetseite eine Analysesoftware, wie z.B. Google Analytics, Matomo oder Etracker, eingesetzt wird. Auch solche Unternehmen, die gegenüber EU-Bürgern Waren bzw. Dienstleistungen anbieten, die an europäischen Konzernen beteiligt sind oder die Mitarbeiter aus EU-Staaten beschäftigen, haben sich an die DSGVO zu halten.

Auch hier gilt die Faustregel: Im Zweifel muss die DSGVO beachtet werden.

2.2 Die zentralen Begriffe müssen Sie kennen

Leider lässt sich das Datenschutzrecht nicht verstehen und folglich auch nicht korrekt in die Praxis umsetzen, ohne die zentralen Begriffe zu kennen. Auch wenn manches ziemlich theoretisch klingt, führt an diesen Begriffen kein Weg vorbei.

2.2.1 Von zentraler Bedeutung: »personenbezogene Daten« und »betroffene Person«

»Personenbezogene Daten« – das ist der zentrale Begriff im Datenschutzrecht.

Personenbezogene Daten sind definiert als Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (den sog. »Betroffenen«) beziehen. Bei dem Betroffenen (oder auch der »betroffenen Person«) handelt es sich um den Menschen, dessen Daten verarbeitet werden.

Der Begriff der personenbezogenen Daten soll nach dem Willen des Gesetzgebers sehr weit zu verstehen sein. Nur reine Unternehmensdaten, wie etwa Bilanzen oder auch Maschinendaten ohne jeglichen Bezug zu einem Menschen, sind davon ausgeschlossen.

Über den Familiennamen wird eine Person beispielsweise problemlos identifiziert. Schwieriger ist die Einordnung der Formulierung »identifizierbar«. Identifizierbar ist eine natürliche Person dann, wenn sie direkt oder indirekt identifiziert werden kann. Die Identifizierung kann dabei mittels Zuordnung zu einer Kennung erfolgen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person ist. An diesen Merkmalen wird schnell deutlich, wie weitreichend das Verständnis von personenbezogenen Daten in der DSGVO ist.

Kundennummern werden in einem Unternehmen mittels eines internen Zahlencodes erstellt. Mithilfe interner Systeme des Unternehmens können diese Zahlencodes einzelnen Kunden, also konkreten Menschen, zugeordnet werden. Somit handelt es sich bei den Zahlencodes um personenbezogene Daten einer identifizierbaren Person.

Wenn Sie sich nicht sicher sind, sollten Sie in Ihrem beruflichen Alltag im Zweifel davon ausgehen, dass Sie es mit personenbezogenen Daten zu tun haben.

Um den Begriff mit etwas mehr Leben zu füllen, hier einige Beispiele typischer Kategorien von Daten mit Personenbezug:

Persönliche Daten	Name, Anschrift, Geburtsdatum
Kontaktdaten	Telefonnummer, Faxnummer, E-Mail-Adresse
Finanzdaten	Bankverbindung, Gehaltsabrechnung
Allgemeine äußere Merkmale	Größe, Gewicht, Haar- oder Augenfarbe
Biometrische Daten	Fingerabdruck, Iris-Scan, DNA-Probe
Fotos/Videos	Digital-Aufnahmen mit erkennbarer Darstellung von Personen
Gesundheitsdaten	Krankmeldung, Diagnose, Überweisung, Rezept
Kfz-Kennzeichen	
IP-Adressen	Kombination aus Zahlen bzw. Buchstaben, »Anschrift« eines Endgeräts, z.B. eines Laptops, in einem Netzwerk

Am Beispiel des Kfz-Kennzeichens wird deutlich, wie weit der Begriff der personenbezogenen Daten zu verstehen ist. Wenn ein fremdes Auto an Ihnen vorbeifährt, können Sie normalerweise nicht anhand des Nummernschilds auf den Halter schließen. Allerdings ist dies mithilfe der Zulassungsbehörde möglich, was für den Personenbezug im Sinne der DSGVO ausreicht. Aber natürlich kommt es immer auf den Kontext an: Wenn Sie nur ein Geburtsdatum vorliegen haben, werden Sie dadurch noch keinen Bezug zu einer bestimmten Person herstellen können. Wenn jetzt aber noch ein Nachname oder vielleicht der Hinweis, dass es sich um einen Bekannten von Ihnen handelt, hinzukommt, ist die Identifizierung der betreffenden Person schon naheliegender. Prinzipiell werden die in der Tabelle aufgeführten Datenkategorien als solche mit Personenbezug eingestuft.

Wichtig: Es spielt keine Rolle, ob die Daten auf einem Computer elektronisch gespeichert oder in Papierform in Ordnern oder Karteikästen abgelegt sind. Den Datenschutz müssen Sie in jedem Fall beachten.

Besonders sensible Daten

Neben »normalen« personenbezogenen Daten gibt es auch noch »besondere« Datenkategorien, die der Gesetzgeber als besonders sensibel ansieht (Art. 9 Abs. 1 DSGVO). Hierunter fallen:

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- genetische Daten
- biometrische Daten
- Gesundheitsdaten
- Daten zum Sexualleben bzw. zur sexuellen Orientierung

Diese Datenarten dürfen nur unter bestimmten, engen Voraussetzungen verarbeitet werden, etwa im Rahmen der Personalakte (z.B. die Angabe der Religion zur Abfuhr von Kirchensteuer) oder von einem Arzt bei der Behandlung.

Eine weitere Kategorie von sensiblen Daten wird in Art. 10 DSGVO genannt. Dabei handelt es sich um personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen. Solche dürfen nur unter behördlicher Aufsicht verarbeitet werden oder dann, wenn es ausnahmsweise per Gesetz ausdrücklich zugelassen ist.

Dies ist im Unternehmen beispielsweise der Fall, wenn Sie als Arbeitgeber von Bewerbern ein Führungszeugnis verlangen. Im Regelfall ist dies nicht zulässig, in manchen Fällen aber verpflichtend, z.B. wenn es um den Job als Kundenberater in einer Bank oder um die Arbeit mit Kindern geht.

Auf den Homepages der verschiedenen Datenschutz-Aufsichtsbehörden der Länder so wie bei den Industrie- und Handelskammern, Handwerkskammern und Branchenverbänden finden Sie diverse Orientierungshilfen, welche personenbezogenen Daten von der jeweiligen Berufsgruppe und Branche eingeholt werden dürfen.

Welche persönlichen Daten dürfen Immobilienmakler von Mietinteressenten einholen? Hier gibt es eine Orientierungshilfe der Landesbeauftragten für Datenschutz von NRW: www.ldi.nrw.de (dort in der Suchfunktion den Begriff »Mietinteressent« eingeben).

2.2.2 Die »verantwortliche Stelle« sind Sie!

Wer muss nun eigentlich das Datenschutzrecht beachten? Die DSGVO nennt denjenigen »**Verantwortlichen«,** in diesem Ratgeber auch als »verantwortliche Stelle« bezeichnet. Hierbei handelt es sich um eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Neben Behörden und Vereinen sind damit folglich auch alle Unternehmen gemeint: vom Solo-Selbstständigen über den unternehmerischen Mittelstand bis hin zum Großkonzern – also auch Sie als selbstständiger Unternehmer.

2.2.3 Die »Verarbeitung« von Daten steht im Mittelpunkt

Bei welchen Datenverarbeitungen sind die Vorgaben der DSGVO nun zu beachten? Das Gesetz spricht von einer Verarbeitung bei jedem mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten. Auch dies ist sehr weitgehend zu verstehen.

Im Grunde fällt jeder Einzelvorgang darunter, von der ersten **Erhebung** von Daten über das **Speichern, Organisieren, Auswerten** oder **Übertragen** bis hin zum **Löschen** bzw. **Vernichten.**

Im Zweifel sollten Sie davon ausgehen, dass eine Verarbeitung im Sinne der DSGVO vorliegt. Es macht keinen Unterschied, ob Sie die Daten als Datei auf einem Computer, über Ihr Smartphone oder als handschriftliche Notizen auf Papier verarbeiten. Denn der Datenschutz ist nicht nur digital oder online, sondern auch analog und offline zu beachten.

Sie stecken die Kopie des Angebots, das Sie an einen Kunden verschickt haben, dieser jedoch nicht angenommen hat, in den Reißwolf. Das Vernichten dieser Unterlagen ist eine **Verarbeitung** im Sinne der DSGVO.

2.3 Diese Regeln müssen Sie einhalten

Neben den nötigen Grundbegriffen ist es entscheidend, dass Sie auch die grundlegenden Regeln im Datenschutzrecht kennen. Das ist nicht bloße Theorie, sondern führt zum besseren Verständnis und dadurch zur erleichterten Umsetzung im Alltag.

2.3.1 Der Rechtmäßigkeitsgrundsatz: ein Verbot unter Vorbehalt

Die wichtigste Regel ist das Rechtmäßigkeitsprinzip. Juristisch handelt es sich hier um ein »Verbot mit Erlaubnisvorbehalt«. Das bedeutet: Jede Verarbeitung personenbezogener Daten ist grundsätzlich untersagt, soweit keine Ausnahme vorliegt. Dies ist ein sehr restriktiver Ansatz, verdeutlicht aber einmal mehr den Stellenwert des Datenschutzrechts. Das Berufsleben wäre aber in der heutigen Form so nicht denkbar, wenn es nicht diverse Ausnahmen gäbe, die eine Verarbeitung von personenbezogenen Daten doch zulassen.

Index