Wissen auf den Punkt gebracht.

DSGVO richtig umsetzen

Achim Barth

GABAL

30 Minuten

DSGVO richtig umsetzen

Achim Barth

Bibliografische Information der Deutschen Nationalbibliothek. Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-96739-121-3

Umschlaggestaltung: die imprimatur, Hainburg
Umschlagkonzept: Martin Zech Design, Bremen
Lektorat: Eva Gößwein, Berlin
Autorenfoto: Danijel Grbic, Schorndorf
Satz: Zerosoft, Timisoara (Rumänien)
Druck und Verarbeitung: Salzland Druck, Staßfurt

Wir drucken in Deutschland.

www.gabal-verlag.de
www.gabal-magazin.de
www.twitter.com/gabalbuecher
www.facebook.com/gabalbuecher
www.instagram.com/gabalbuecher

PEFC zertifiziert
Dieses Produkt stammt aus nachhaltig bewirtschafteten Wäldern und kontrollierten Quellen.
www.pefc.de

ÖKOLOGISCHE VERANTWORTUNG

Wir übernehmen Verantwortung! Ökologisch und sozial!

- Verzicht auf Plastik: kein Einschweißen der Bücher in Folie
- Nachhaltige Produktion: Verwendung von Papier aus nachhaltig bewirtschafteten Wäldern, PEFC-zertifiziert
- Stärkung des Wirtschaftsstandorts Deutschland: Herstellung und Druck in Deutschland

Wissen auf den Punkt gebracht

Dieses Buch ist so konzipiert, dass Sie in kurzer Zeit prägnante und fundierte Informationen aufnehmen können. Mithilfe eines Leitsystems werden Sie durch das Buch geführt. Es erlaubt Ihnen, innerhalb Ihres persönlichen Zeitkontingents (von 10 bis 30 Minuten) das Wesentliche zu erfassen.

Kurze Lesezeit

In 30 Minuten können Sie das ganze Buch lesen. Wenn Sie weniger Zeit haben, lesen Sie gezielt nur die Stellen, die für Sie wichtige Informationen beinhalten.

- Schlüsselfragen mit Seitenverweisen zu Beginn eines jeden Kapitels erlauben eine schnelle Orientierung: Sie blättern direkt zu dem Thema, das Sie besonders interessiert.
- **Zahlreiche Zusammenfassungen innerhalb der Kapitel erlauben das schnelle Querlesen.**
- Ein Fast Reader am Ende des Buches fasst alle wichtigen Aspekte zusammen.
- Ein Register erleichtert das Nachschlagen.

Inhalt

Vorwort 6

1. Einführung in die DSGVO 9
Begriffe und Grundsätze im Datenschutz 10
Der Datenschutzbeauftragte 16
Rechenschaftspflicht und Rechtmäßigkeit 20
Die Rechte der Betroffenen 28

2. Die Pflicht – alles, was getan werden muss 35
Sieben Schritte zum Projektstart 37
Das Verzeichnis von Verarbeitungstätigkeiten 52
Dokumentation der technischen und organisatorischen Maßnahmen 54

3. Die Kür – alles, was getan werden soll 61
Umgang mit Auftragsverarbeitern 62
Erfüllung der Informationspflichten 63
Der DSGVO-konforme Internetauftritt 65

4. Zugabe – für ein Topergebnis 71
Schutzeinstufung von Daten und Risikobewertung ... 72
Aufbau eines Datenmanagements 73
Kontinuierlich: Überwachung, Kontrolle, Verbesserung 76

5. Besondere Datenverarbeitungen 79
Datenschutz im Homeoffice 80
Bewerberauswahl und Onboarding 82

Fast Reader 87
Der Autor 93
Weiterführende Literatur 94
Register 95

Vorwort

Spätestens seit Einführung der Datenschutz-Grundverordnung (DSGVO) ist das Thema Datenschutz in den Köpfen der Verantwortlichen in Unternehmen, Vereinen und sonstigen Organisationen angekommen. Als die DSGVO im Mai 2018 kam, hatten viele vor allem Angst vor Bußgeldern und Abmahnungen. Die befürchtete Abmahnwelle blieb jedoch aus, und so trat Frust an die Stelle der Angst. Grund dafür waren schwammige Formulierungen im Gesetzestext, keine eindeutigen Vorgaben, wie Datenschutz nun konkret im Unternehmen umgesetzt werden muss, und sich ständig widersprechende Aussagen in Medien und von Experten. Dazu kamen noch nörgelnde Kollegen in Vertriebs- und Marketingabteilungen, die sich in ihrer Tätigkeit ausgebremst sahen.

Kurzum, der Datenschutz hat in so gut wie allen Organisationen für Unsicherheit und Unverständnis gesorgt. Dies führte teilweise zu teurem Aktionismus, teilweise dazu, dass Datenschutz völlig ausgeblendet wurde. Beide Verhaltensweisen sind nicht zielführend.

Große Unternehmen sind in der Lage, eigene Datenschutzabteilungen aufzubauen und das Thema professionell mit eigenen und externen Experten anzugehen und umzusetzen. Diese Ressourcen stehen kleinen Organisationen im Regelfall nicht zur Verfügung. Das vorliegende Buch richtet sich daher vor allem an Verantwortliche in KMU, an Soloselbstständige, an Menschen, die sich in Vereinen en-

gagieren, und solche, die in ihrer Firma die Rolle des Datenschutzkoordinators einnehmen. Ich stelle Ihnen eine Lösungsmöglichkeit vor, wie Sie das Thema Datenschutz Schritt für Schritt angehen können. Dabei berücksichtige ich die zeitlichen und finanziellen Ressourcen eines KMU genauso wie die praktische Umsetzung der Maßnahmen.

Nehmen Sie das Thema ernst, genießen Ihre Kunden mindestens drei Vorteile: mehr Transparenz, was mit den eigenen Daten passiert, weniger Bürokratie und mehr Sicherheit für die gespeicherten personenbezogenen Daten.

Und für alle Verantwortlichen gilt: Wer seine Pflicht erfüllt, muss sich weder um Bußgelder und Abmahnungen noch um persönliche Haftung sorgen.

Legen wir los.

Ich wünsche Ihnen viel Erfolg bei der Umsetzung.

Achim Barth

Was sind die Grundsätze der Datenverarbeitung?

Seite 10

Benötige ich einen Datenschutzbeauftragten?

Seite 16

Welche Rechte meiner Kunden und Mitarbeiter muss ich gewährleisten?

Seite 28

1. Einführung in die DSGVO

Wenn Sie mit Ihrem Auto auf der Straße fahren, dann kennen Sie die Verkehrsregeln. Sie wissen, auf welcher Seite Sie zu fahren haben, Sie können gut einschätzen, wie sich die anderen Verkehrsteilnehmer verhalten, und Sie können die Verkehrszeichen lesen. Dazu kommt, Sie beherrschen Ihr Fahrzeug und können es sicher durch den Verkehr lenken, und wenn es doch mal zu einem Unfall kommt, sind das Fahrzeug und Sie selbst abgesichert.

Wenn wir das Beispiel Autofahren und Verkehr mit der Situation im Hinblick auf den Datenschutz vergleichen, sieht es dort leider bei den meisten nicht so rosig aus. Alle stehen mit ihrem kleinen oder großen Auto auf derselben Straße, kennen aber die Regeln kaum und können auch die Verkehrsschilder nicht lesen. Manch einer fährt, bildlich gesprochen, mit 200 Stundenkilometern über die Autobahn, obwohl nur 80 erlaubt sind, und der nächste hätte freie Fahrt, steht aber auf dem Standstreifen. Daher beschäftigen wir uns in diesem Kapitel zuerst einmal mit den „Verkehrsregeln", damit Sie zukünftig die Schilder auch lesen können, die Ihnen auf der Datenautobahn entgegenkommen.

Sehr oft erlebe ich in der Praxis, dass Unternehmen zwar damit begonnen haben, etwas in Sachen Datenschutz in die Wege zu leiten, aber entweder schnell aufgegeben oder sich selbst mit unnötigen internen Regeln ausbremsen.

Datenschutz *richtig* umsetzen ist das Ziel. Allerdings hapert es genau daran in der Praxis leider sehr oft. Das soll nicht heißen, dass Datenschutz in den Unternehmen keine Rolle spielt. Vielmehr setzen unerfahrene eigene Mitarbeiter sehr oft irgendetwas um, ohne dass sie selbst oder die Geschäftsleitung wissen, warum überhaupt. Man hat eventuell gesehen, dass der Wettbewerber so verfährt, in einem Tagesseminar etwas aufgeschnappt oder vom Berufsverband wenig „Hilfreiche Tipps zur Umsetzung der DSGVO" erhalten. Oft fehlen auch zwei Zutaten: gesunder Menschenverstand und genaues Wissen, was die DSGVO überhaupt in der praktischen Umsetzung verlangt … und was nicht.

1.1 Begriffe und Grundsätze im Datenschutz

Das Ziel ist es, dieses Buch in einfacher, verständlicher Sprache zu schreiben und nicht in die „Expertensprache" abzudriften. Dennoch gibt es einige Begriffe, die ich direkt zu Beginn erläutern möchte. Grundsätzlich können Sie die 26 wichtigsten Begriffe in **Artikel 4 der DSGVO** direkt nachschlagen (folgen Sie dazu einfach dem QR-Code auf dieser Seite). Dort sind diese zwar definiert, aber leider nicht sonderlich verständlich für Laien.

Begriffe

Folgende Fachbegriffe sollten Sie kennen, um in Ihrem Betrieb datenschutzkonform zu arbeiten. Außerdem sollten Sie die Grundsätze der Datenverarbeitung gelesen und verstanden haben. Denn jegliche Verarbeitung von personenbezogenen Daten muss diesen Grundsätzen entsprechen. (Die Grundsätze zur Datenverarbeitung nach der DSGVO finden Sie direkt nach den Begriffsdefinitionen.)

Personenbezogene Daten

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

⇨ **In der Praxis:** Personenbezogene Daten sind neben Namen, Adresse, Geburtsdatum und allen Kontaktdaten auch Informationen über Vermögen, Besitz oder Gehalt sowie Fotos. Auch Angaben zum Arbeitsverhalten, die Personalnummer, die Arbeitsergebnisse, Benutzererkennungen und Nutzungszeiten zählen dazu.

Verantwortlicher

Ein „Verantwortlicher“ ist „die 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“.

⇨ **In der Praxis:** Verantwortliche sind die Inhaber, Geschäftsführer, CEOs oder (ehrenamtliche) Vorstände einer Organisation.

Gemeinsam Verantwortliche

Eine gemeinsame Verantwortlichkeit oder auch Joint Control liegt vor, wenn für die Datenverarbeitung zwei und mehr Verantwortliche gemeinsam tätig sind.

⇨ **In der Praxis:** Gemeinsam verantwortlich sind Sie zum Beispiel mit Facebook, wenn Sie eine Facebook-Unternehmensseite betreiben.

Auftragsverarbeiter

„Auftragsverarbeiter ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.“

⇨ **In der Praxis:** Ich vergleiche Auftragsverarbeiter gerne mit Sherpas bei einer Bergexpedition. Ein Auftragnehmer ist weisungsgebunden und verarbeitet die Daten ausschließlich im Sinne des Auftraggebers und explizit nicht für eigene Zwecke.

Besondere Kategorien personenbezogener Daten

Diese Daten stehen unter besonders hohem Schutz. Gemeint sind Informationen über die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten und Daten zum Sexualleben oder der sexuellen Orientierung.

⇨ **In der Praxis:** Wenn Sie solche besonderen Kategorien von personenbezogenen Daten regelmäßig verarbeiten, zum Beispiel als Gesundheitsdienstleister, sind höhere Schutzmaßnahmen für die Datensicherheit notwendig.

Grundsätze der Datenverarbeitung

Sobald Sie personenbezogene Daten verarbeiten, gelten die sieben Grundsätze der Verarbeitung. Diese können Sie in Artikel 5 der DSGVO nachlesen.

Auf die betriebliche Praxis übertragen müssen Sie bezüglich der Grundsätze Folgendes beachten:

Grundsatz 1: Rechtmäßigkeit

Um Daten aufzunehmen, zu nutzen und zu speichern, benötigen Sie immer eine Rechtsgrundlage. Grundsätzlich ist die Verarbeitung personenbezogener Daten nämlich verboten. Es sei denn, die DSGVO erlaubt dies ausdrücklich. Im Falle einer Kundenbeziehung zählt vor allem ein Vertrag, in Einzelfällen auch die Einwilligung oder ein berechtigtes Interesse, welches der Verantwortliche belegen kann.

Grundsatz 2: Transparenz

Zudem müssen Verantwortliche die Verarbeitung personenbezogener Daten so organisieren, dass es für den Betroffenen nachvollziehbar bleibt. Ein Anbieter darf seine Kunden nicht hinters Licht führen, zum Beispiel eine Einwilligung einfordern und, falls diese nicht kommt, sich auf einen bestehenden Vertrag beziehen.

Grundsatz 3: Zweckbindung

Betroffene müssen darauf vertrauen können, dass Sie ihre Daten nur für die Zwecke verarbeiten, die zum Beispiel in einem Vertrag eindeutig und legitim festgelegt wurden. Eine Änderung ist nur in ganz wenigen Ausnahmefällen erlaubt und muss dem Betroffenen sofort mitgeteilt werden.

Grundsatz 4: Datenminimierung

Verantwortliche dürfen nur die Daten verarbeiten, die für die Vertragserfüllung tatsächlich notwendig sind. Erheben Sie also zum Beispiel nicht das Geburtsdatum, wenn dies für die Durchführung Ihrer Leistung nicht erforderlich ist.

Grundsatz 5: Richtigkeit

Nur „sachlich richtige" Daten dürfen verarbeitet werden. Personenbezogene Angaben müssen daher immer auf dem neusten Stand sein. Sie sollten regelmäßig abfragen, ob ein gespeicherter Datensatz noch korrekt und der Zweck der Datenverarbeitung gegeben ist. Im Bedarfsfall löschen oder korrigieren Sie die Informationen.

Praxistipp!
Wer auf Nummer sicher gehen will, fragt seine Bestandskunden einmal jährlich, ob der gespeicherte Datensatz noch stimmt. Das fordert die DSGVO aber nicht.

Grundsatz 6: Speicherbegrenzung

Personenbezogene Daten müssen so abspeichert sein, dass sie nach Wegfall des Zwecks gelöscht oder anonymisiert werden können. Die Daten selbst müssen sicher gespeichert werden.

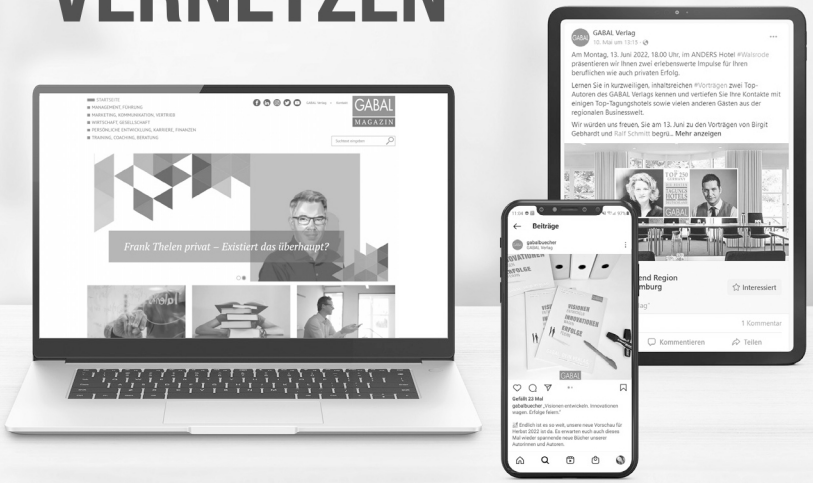
Grundsatz 7: Integrität und Vertraulichkeit

Alle Verantwortlichen haben die Aufgabe, die Sicherheit der Daten durch geeignete technische und organisatorische Maßnahmen zu gewährleisten. Die DSGVO nennt dabei konkret „angemessene Sicherheit" sowie Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, vor unbeabsichtigtem Verlust, vor unbeabsichtigter Zerstörung und Schädigung.

Praxistipp!
Im Betriebsalltag setzen Sie diese Prinzipien durch Richtlinien und Durchführungshinweise um. Dazu unterweisen Sie Ihre Beschäftigten auf geeignete Weise und führen eine umfassende Datenschutz-Dokumentation zur Erfüllung der Rechenschaftspflicht. Diesen Grundsatz und den Grundsatz der Rechtmäßigkeit beleuchten wir weiter unten im Detail. Ihre Kunden profitieren von einer geschützten Umgebung und einem zweckmäßigen Umgang mit ihren Daten.

GABAL

WISSEN TEILEN – MENSCHEN VERNETZEN



→ Im GABAL MAGAZIN

Aktuelle Themen und Trends aus Wirtschaft, Business & Karriere sowie persönliche Weiterentwicklung

Schauen Sie vorbei!
www.gabal-magazin.de

→ Auf Social Media

Alle Infos rund um unsere neuen Bücher und unsere AutorInnen sowie spannende Einblicke in das Verlagsleben

Folgen Sie uns auf unseren Social-Media-Kanälen!