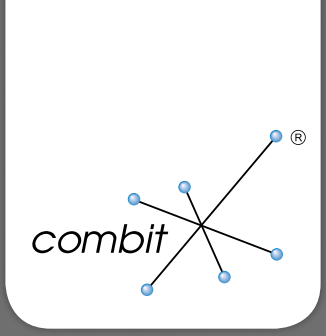


Fit im Datenschutz

Überblick über die DSGVO,

Checklisten zur Bestandsaufnahme und

für erste Maßnahmen

Im Mai 2018 begann ein neues Datenschutz-Zeitalter

Jede Person hinterlässt heutzutage digitale Fußabdrücke. Viele Menschen haben aber inzwischen keinen Überblick mehr darüber, wo und was über sie gespeichert wird. Möglicherweise sind sie auch nicht damit einverstanden und fühlen sich ausgeliefert. Zum Schutz der Privatsphäre gibt es bereits seit Jahren diverse Gesetze, doch mit dem 25. Mai 2018 brachen für die meisten Unternehmen, die mit personenbezogenen Daten von Menschen, die sich in der EU befinden, arbeiten, wie bspw. Kunden-, Interessenten-, Lieferanten- oder Personaldaten, neue Zeiten an. In diesem Whitepaper wird deshalb kurz erklärt, was die neuen Gesetze zum Datenschutz mit sich bringen und es gibt erste Anleitungen zur Umsetzung.

DSGVO – kurz erklärt

Das europäische Datenschutzrecht kann inzwischen auf eine mehr als zwanzigjährige Geschichte zurückblicken. Die heterogene Auslegung der bisher gültigen Richtlinien führte zur Idee für ein EU-weit einheitliches Datenschutzrecht. Ziel war auch, den Datenschutz an die neuen Anforderungen des Internets und der Globalisierung anzupassen. Für die Umsetzung der neuen EU-Datenschutz-Grundverordnung (EU-DSGVO) bestand eine zweijährige Übergangsfrist, die es den Ländern ermöglicht hat, bisher geltende Gesetze wie das Bundesdatenschutzgesetz (BDSG) anzupassen. Seit dem 25. Mai 2018 gilt die DSGVO EU-weit. Neu ist vor allem, dass die DSGVO Bußgelder bis zu 20 Mio. Euro oder 4% des Jahresumsatzes bei Verstößen vorsieht. Neu ist auch, dass Aufsichtsbehörden und Landesdatenschutzbeauftragte jetzt nicht erst bei Beschwerden reagieren, sondern aktiv die Umsetzung kontrollieren werden. Neben der Kontrolle zunächst vermutlich größerer Firmen sollen auch kleinere Unternehmen per Fragebogen untersucht werden. Zusätzlich können unzufriedene Mitarbeiter oder Kunden Unternehmen bei den Behörden melden, wenn Verstöße gegen den Datenschutz vermutet werden, und dann auch Schmerzensgeld einklagen. Unternehmen sehen sich deshalb vor die große Herausforderung gestellt, ihren Umgang mit personenbezogenen Daten neu zu regeln. Dabei ist es hilfreich, die neuen Chancen für Ihre Kundenbeziehungen zu erkennen: Wer sich vom Datenwolf zum Datenhirten entwickelt, der verantwortungsvoll und transparent mit den Daten seiner Kunden umgeht, kann eine ganz neue Qualität der Kundenbindung erreichen.

Neue Rechte für Ihre Kunden

Die DSGVO gilt für jedes Unternehmen, das mit personenbezogenen Daten von Menschen, die sich in der EU befinden, arbeitet. Das Unternehmen muss nachweisen können, dass jeder Geschäftsprozess nur die dafür unbedingt nötigen Daten verwendet, diese nur für den Bearbeitungszeitraum gespeichert werden und so wenig Mitarbeitern wie möglich zugänglich sind.

Die DSGVO verleiht Ihren Kunden und sonstigen Kontakten zum Teil neue Rechte, auf die Sie als Unternehmen jetzt eingehen müssen. Dies sind die wichtigsten Neuerungen:

1) Recht auf Datenübertragbarkeit
Unternehmen müssen Daten in elektronischem Format zur Verfügung stellen, damit sie auf einen anderen Anbieter übertragen werden können.

2) Zugangsrecht
Unternehmen müssen auf Anfrage innerhalb eines Monats eine Kopie aller gespeicherten Daten kostenlos und in elektronischem Format zur Verfügung stellen.

3) Löschungsrecht
Unternehmen müssen Daten löschen, wenn der Zweck, zu dem die Daten erhoben wurden, erfüllt ist oder entfällt, oder wenn die betroffene Person es dazu konkret auffordert. Das Löschungsrecht beinhaltet auch das "Recht auf Vergessenwerden", was bedeutet, dass ein Unternehmen bei bereits veröffentlichten personenbezogenen Daten dafür sorgen muss, dass diese auch auf anderen Plattformen oder bei anderen Unternehmen gelöscht werden.

4) Benachrichtigungsrecht
Unternehmen müssen sowohl Personen als auch die Datenschutzbehörden innerhalb von 72 Stunden informieren, wenn es zu einer Verletzung der Datensicherheit kam, die ein Risiko für die betroffene Person mit sich bringt.

5) Auskunftssrecht
Unternehmen müssen Verbraucher ausdrücklich informieren, welche Daten sie zu welchem Zweck verarbeiten. Die Zustimmung muss ausdrücklich erfolgen und darf nicht stillschweigend vorausgesetzt werden.

6) Widerspruchsrecht
Dem Widerspruch einer Person zu einer bestimmten Verarbeitung Ihrer personenbezogenen Daten müssen Unternehmen – von Ausnahmen abgesehen – schnellstmöglich Folge leisten. Dieses Recht muss von vorneherein mitgeteilt werden.

DSGVO-Fahrplan

Geschäftsleitung informieren und Bewusstsein für anstehendes Projekt schaffen.

Datenschutzprojekte planen, Zeitraum und Ziele festlegen.

Für Bestandsaufnahme Liste zu allen verarbeiteten Daten anlegen.

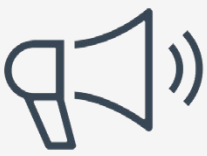
Bei bestimmten Voraussetzungen Datenschutzbeauftragten benennen.

Rechte Betroffener absichern (Auskunft, Korrekturen, Widerruf, etc.).

Prozesse zur Datenverarbeitung überprüfen. Gesetzeswidrige Prozesse abschaffen oder überarbeiten.

Bisherige Datenspeicherung überprüfen. Gesetzeswidrige Daten löschen.

Mittel bereitstellen, finanzielle und zeitliche Ressourcen planen.



Informationspflicht umsetzen (z. B. Datenschutzerklärungen aktualisieren).

Mitarbeiter und Geschäftspartner zum Einhalten der neuen Konventionen verpflichten.

Mitarbeiter zu neuen Regelungen schulen.

Workflows für Kontrolle, Updates und Reaktion bei Datenschutznotfällen einrichten.

Fit für den neuen Datenschutz

Teil 1: Checkliste zur Bestandsaufnahme

Legen Sie sich eine Liste an, in der Sie alle personenbezogenen Daten dokumentieren, die in Ihrem Unternehmen erfasst und verarbeitet wurden und werden. Das betrifft sowohl digital gespeicherte als auch gedruckte und handschriftlich notierte Daten.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse von natürlichen Personen wie z. B. Name, Geburtsdatum, Familienstand, geschäftliche oder private Beziehungen, Bilder, Beiträge in sozialen Netzwerken, Adresse, Telefonnummern, eMail-Adresse, Kontonummer, Mitgliedschaften, Urkunden, Zeugnisse, Kundennummern, Rechnungsnummern, Arbeitgeber, Konfession und Weltanschauung, Gesundheitsstatus, IP-Adresse, Standortdaten, biometrische Daten oder Einkünfte. Die personenbezogenen Daten können sich z. B. auch auf Ihrer Firmenwebsite (evtl. auch in vergessenen Bereichen/Subdomains) in vor langer Zeit hochgeladenen PDFs, Bild-Dateien, Excel- und Word-Dokumenten sowie deren Metadaten und in Tracking-Daten der Besucher (z. B. von Google Analytics) verstecken.

Für jede einzelne Datenart in Ihrer Liste müssen Sie sich alle unten aufgeführten Fragen stellen. Erst im Anschluss überprüfen Sie, inwiefern einzelne Punkte mit der DSGVO konform sind, und ob Änderungsbedarf besteht. Ihre Liste ist Bestandteil der Dokumentations-Anforderungen der DSGVO – als erster Schritt ist sie also unerlässlich.

Tipp: Arbeiten Sie hier so sorgfältig wie möglich und beziehen Sie alle Abteilungsverantwortlichen mit ein. Mit Einführung der DSGVO liegt die Beweislast des datenschutzkonformen Arbeitens nun beim Unternehmen.

1) **Angaben zur Quelle**
   Woher haben Sie die Daten bekommen? Mögliche Quellen sind Webformulare, Visitenkarten, Integration von anderen Systemen und Datenlisten. Wurde die Person bei der Erfassung über Verarbeitungszweck, Speicherdauer und Widerrufsmöglichkeit informiert? Das kann z. B. durch eine Einwilligungserklärung oder Datenschutzerklärung auf Ihrer Website geschehen sein.

2) **Zu welchem Zweck werden diese Daten erhoben?**
   Wenn z. B. das Geburtsdatum erhoben wird, muss man begründen, wozu es gebraucht wird. Das Geburtsdatum wäre bei einem Kunden wichtig, um die Geschäftsfähigkeit zu verifizieren.

3) **Was ist die rechtliche Grundlage?**
   Wurde bei der Erfassung bereits vorhandener Daten eine Einwilligung gegeben, oder ist die Erfassung Teil eines Vertrages? Bei Empfängern eines Newsletters muss z. B. der entsprechende Einwilligungstext oder die bestehende Datenschutzerklärung dokumentiert werden.

4) **Handelt es sich um besonders sensible Daten?**
   Besonders sensible Daten sind z. B. biometrische Daten, Krankendaten, Daten von Kindern und genetische Daten. Beschreiben Sie, welche Daten bei Ihnen darunter fallen, sowie Besonderheiten in der Handhabung, Archivierung und bei den Zugriffsrechten.

5) **Wie lange werden die Daten aufbewahrt?**
Gibt es aktuell eine Löschregelung in Ihrem Unternehmen? Ein Beispiel wäre, wenn Sie aktuell Gehaltsinformationen so lange aufbewahren, wie die Vorschriften zur Buchführung es vorschreiben.

6) **Wer kann auf die Daten zugreifen?**
Beschreiben Sie vorhandene Zugriffsbeschränkungen für unterschiedliche Datenarten. Haben beispielsweise nur Mitarbeiter aus der Buchhaltung Zugriff auf das Gehaltszahlungssystem? Oder sind Kundendaten nicht nur für Geschäftsleitung und Vertriebsteam, sondern auch für die Personalabteilung zugänglich? Beschreiben Sie die Sicherheitsvorkehrungen, die für die lokalen PCs der Mitarbeiter getroffen wurden, und wenn Mitarbeiter mit Firmenhandys oder ihrem eigenen Smartphone (Bring your own device) auf Firmendaten zugreifen.

   Dokumentieren Sie Geheimhaltungsvereinbarungen mit externen Dienstleistern. Bestehen Datenschutzvereinbarungen mit dem Dienstleister, der die Konfektionierung von Briefmailings vornimmt und dem dazu Etiketten mit Kundenadressen ausgehändigt werden? Möglich wäre auch eine On-Demand-Druckerei, welche die Empfängerdaten in die Drucksache integriert, z. B. Postkarten mit eingedruckter Anrede und Adresse.

   Die Weitergabe von personenbezogenen Daten kann auch ungewollt passieren, z. B. durch die Übergabe dieser Adressen an einen Webdienst (Routenplaner, Online-Landkarte, eMail Versand über ein externes Newsletter-Tool) oder die Übermittlung der Daten an einen Webdienst zur Validierung.

7) **In welchen Systemen werden die Daten aufbewahrt?**
Speichert Ihr Unternehmen Daten lokal oder in der Cloud? Wenn Sie Ihre Daten auf einem externen Server hosten, müssen Sie beschreiben, welche Datenschutzvorkehrungen der Anbieter trifft und die entsprechenden Verträge dokumentieren. Gleiches gilt z. B. für den Hoster Ihrer Website und den eMail-Versandservice. Bei Aufbewahrung in Papierform in Aktenschränken ist relevant, für wen diese zugänglich sind.

Teil 2: Erste Maßnahmen

Nach der Bestandsaufnahme beginnen Sie, die neuen Vorgaben umzusetzen.

1) **Datenschutz zur Chefsache machen**
   Schaffen Sie ein Bewusstsein für Datenschutz in Ihrem Unternehmen, vor allem in der Geschäftsführung. Machen Sie allen bewusst, dass es hier vor allem um die Vertrauensbeziehung zu Ihren Kunden, Geschäftspartnern und Mitarbeitern geht. Beschreiben Sie Ihre Ziele und informieren Sie sich über vorhandene Risiken. Der Geschäftsführung sollte außerdem bewusst sein, dass sie bei Datenpannen haftet. Erstellen Sie einen Projektplan, z. B. auf Basis dieser Checkliste.

   Tipp: Hilfreich für die Selbsteinschätzung ist der Prüffragebogen des Bayerischen Landesamtes für Datenschutzaufsicht. Solche oder ähnliche Fragebögen werden ab Mai 2018 von den Behörden der einzelnen Bundesländer zur Kontrolle eingesetzt:
   www.lda.bayern.de/media/dsgvo_fragebogen.pdf

2) **Datenschutzbeauftragten anmelden**
   Bei bestimmten Voraussetzungen müssen Sie einen Datenschutzbeauftragten haben und diesen namentlich bei Ihrer Datenschutzbehörde melden. Derzeit wird dafür noch ein einheitliches Musterformular entwickelt. Es ist also ratsam, hier noch abzuwarten.

   Datenschutzbehörden:
   www.bfdi.bund.de/DE/Infothek/Anschriften_Links/AnschriftenUndLink.html

   Je nach Größe des Unternehmens kann es sinnvoll sein, in den verschiedenen Abteilungen einen Verantwortlichen für den Datenschutz zu benennen, der als Vermittler zwischen dem Datenschutzbeauftragten und den Mitarbeitern dient. Der Datenschutzbeauftragte führt ggf. die Datenschutz-Folgeabschätzung durch.

3) **Erfüllen der neuen Dokumentationspflichten**
   Nach der neuen Verordnung muss jedes Unternehmen ein Verzeichnis aller Verarbeitungstätigkeiten im Bezug auf personenbezogene Daten führen. Darin dokumentieren Sie alle Abwägungen, Entscheidungen und Prozesse. Wenn Sie die Checkliste zur Bestandsaufnahme ausgefüllt haben, haben Sie einen großen Teil der Aufgabe schon erledigt. In Ihrer Liste muss dann nur noch ergänzt werden, wie und auf welcher rechtlichen Grundlage in Zukunft mit den Daten verfahren wird.

4) **Datenbestand hinterfragen**
   Sie sollten nicht mehr personenbezogene Informationen als unbedingt erforderlich speichern. Überlegen Sie, welche Daten aus Ihrer Bestandsaufnahme unnötig sind und welche Sie unbedingt zur Geschäftsabwicklung brauchen. Verzichten Sie in Zukunft auf die Erhebung dieser Daten und löschen Sie den nicht benötigten Datenbestand.

5) Festlegung der Rechtsgrundlagen und des Zwecks der Datenverarbeitung
Ergänzen Sie in Ihrer Dokumentation, auf welcher Rechtsgrundlage und zu welchem Zweck Sie die Daten verarbeiten. Datenverarbeitung ist laut DSGVO nur erlaubt, wenn einer der folgenden Erlaubnisvorbehalte erfüllt ist:

- Einwilligung der betroffenen Person.
- Die Person hat ein berechtigtes Interesse an der Datenverarbeitung.
- Die Datenverarbeitung ist erforderlich zur Erfüllung eines Vertrages oder für vorvertragliche Maßnahmen auf eine Anfrage hin.
- Zur Erfüllung der rechtlichen Verpflichtungen des Verantwortlichen.
- Zum Schutz lebenswichtiger Interessen.
- Im Interesse oder in Ausübung öffentlicher Gewalt.

Wir empfehlen Ihnen, die Rechtsgrundlagen mit Ihrem Anwalt passend festzulegen.

6) Informationspflichten erfüllen
Überarbeiten Sie Ihre AGBs, Datenschutzbestimmungen und die Informationstexte, z. B. bei Web-Formularen. Beraten Sie sich hierzu gegebenenfalls mit Ihrem Anwalt.

Tipp: Eine DSGVO-konforme Datenschutzerklärung können Sie sich zum Beispiel hier generieren: www.dg-datenschutz.de/muster-datenschutzerklarung/#loaded

7) Dienstleistungsbeziehungen anpassen
Passen Sie bestehende Verträge mit allen Kooperationspartnern, die in irgendeiner Form Zugriff auf personenbezogene Daten Ihrer Firma haben oder hatten, an. Beraten Sie sich mit Ihrem Anwalt, ob diese Verträge neu abgeschlossen werden müssen. Falls Sie bisher Daten an Dritte in Länder außerhalb der EU weitergegeben haben, ist zu prüfen, mit welcher Rechtsgrundlage dies in Zukunft noch zulässig ist. Eventuell greifen hier neue Einwilligungs- und Informationspflichten oder die Übertragung muss unter angemessenen Schutzvorkehrungen stattfinden.

Tipp: Fragen Sie Dienstleister rechtzeitig nach einem DSGVO-konformen Standard-Auftragsverarbeitungsvertrag.

8) IT Sicherheit überarbeiten
Stellen Sie durch strenges Rechtemanagement auf allen Ebenen sicher, dass personenbezogene Daten nur für die definierten Zwecke verwendet werden. Überprüfen Sie, ob regelmäßige Backups oder Hardware nötig sind. Prüfen Sie außerdem, auf welchem Wege personenbezogene Daten mit Kooperationspartnern ausgetauscht werden. Bei Cloud Anbietern ist unter anderem wichtig, in welchem Land die Datensicherung abgelegt ist und wo der Fail-Over Server steht. Auch wenn Ihr Anbieter mit einem „deutschen Rechenzentrum" wirbt, kann es sein, dass der Sicherungsserver bzw. der Speicher für die Sicherungen doch außerhalb der EU liegt.

Tipp: Wählen Sie einen Cloud-Anbieter, der die DSGVO vollständig umgesetzt hat.

9) **Implementierung von Betroffenenrechten**
Richten Sie Mechanismen ein, z. B. in Ihrer CRM Software, um die verschiedenen Stufen eines Widerrufs der Verarbeitung bearbeiten zu können. Zusätzlich müssen Sie sicher stellen, dass danach wirklich keine weitere Verarbeitung der jeweils betroffenen Datenfelder (z. B. Zusendung von Werbung per eMail) mehr erfolgt. Gleiches gilt für den Antrag auf Auskunft und den Antrag auf Datenportabilität. Richten Sie einen entsprechenden Report ein, mit dem die Daten ausgegeben werden können, den Sie dann per eMail verschicken.

10) **Umsetzung von Löschkonzepten**
Stellen Sie durch entsprechende Arbeitsabläufe sicher, dass alle bei der Bestandsaufnahme ermittelten personenbezogenen Daten tatsächlich nur so lange gespeichert werden, wie unbedingt notwendig. Gleiches gilt auch für PDFs, Excel-Listen und andere Speicherorte und Systeme.

11) **Umgang mit Bestandsdaten**
Überprüfen Sie, ggf. mit Beratung Ihres Anwalts, ob Sie Ihre alten Daten überhaupt weiterhin verwenden dürfen. Wurde von der betroffenen Person eine entsprechende Einwilligung erteilt? Falls ja, ist diese noch rechtskonform oder muss sie erneuert werden? Falls die betroffene Person keine weitere Einwilligung erteilt, und keine gesetzliche Aufbewahrungspflicht besteht, müssen die Daten umgehend gelöscht werden.

12) **Reaktionsmechanismen auf Datenpannen**
Jeder unberechtigte Zugriff auf personenbezogene Daten, von dem jemand innerhalb oder außerhalb des Unternehmens Kenntnis erlangt, ist eine Datenschutzpanne. Dazu zählen der Verlust eines unverschlüsselten USB-Sticks / Laptops / Aktenordners mit personenbezogenen Daten, versehentliche Löschung von Daten durch eine nicht autorisierte Person, Verlust des Schlüssels zur Entschlüsselung der Daten oder der versehentliche Versand einer eMail an einen größeren eMail-Verteiler im CC: statt im BCC:. Bei einer Datenschutzpanne sind Sie verpflichtet, die betroffene Person und die Behörde innerhalb von 72 Stunden darüber zu informieren, falls ein Risiko für die persönlichen Rechte und Freiheiten der Person besteht. Richten Sie entsprechende Mechanismen ein, z. B. eine standardmäßig verwendete eMail oder eine Anrufliste, um dieser Informationspflicht nachkommen zu können.

13) **Schulung der Mitarbeiter**
Auch die beste Datenschutzrichtlinie ist nicht sinnvoll, wenn sie nicht gelebt wird. Deswegen sollte Ihr Management und der Datenschutzbeauftragte alle Mitarbeiter für das Thema Datenschutz sensibilisieren und sie mit den zugehörigen Arbeitsabläufen und Konventionen vertraut machen.

14) **Langfristige Überwachung und Aktualisierung**
Überprüfen Sie oder Ihr Datenschutzbeauftragter fortlaufend, ob das Unternehmen konform zur DSGVO arbeitet. Richten Sie regelmäßige Termine zum Check ein und informieren Sie auch Ihre Kollegen über die Auswirkungen der neuen Verordnung auf die Branchenpraxis, ggf. mit Beratung Ihres Anwalts.

Fazit

Fakt ist, die neue Datenschutzverordnung kommt, und die Schonfrist für die Umsetzung läuft aus. Deshalb sollten Sie sich jetzt schnellstmöglich an die Umsetzung der Vorgaben machen, um Bußgelder zu vermeiden. Fakt ist aber auch, dass die Auslegung der Vorgaben zum Teil noch recht unklar ist. Hier werden einschlägige Urteile höchster Instanzen erst in den kommenden Jahren für Rechtssicherheit sorgen können. Bei allem möglichen Unmut über die zusätzliche Arbeitsbelastung sollten Sie aber immer die Auswirkungen der neuen Verordnung auf Ihre Kundenbeziehungen bedenken. Wenn Sie sich als datenschutzkonform arbeitendes Unternehmen präsentieren können, untermauert das langfristig Ihr gutes Image. Umgekehrt werden Datenschutzpannen, Abmahnungen oder gar Gerichtsverhandlungen Ihren Ruf schädigen. Es lohnt sich also, sich schnell und gründlich ans Werk zu machen!

Links zu weiterführenden Themen

DSGVO-Gesetz mit Erwägungsgründen und dem BDSG-neu

FAQ zur Verordnung von der Anwaltskanzlei RESMEDIA

Orientierungshilfe der Bundesbeauftragten für den Datenschutz

Liste der Datenschutzbeauftragten in Deutschland

Berufsverband der Datenschutzbeauftragten Deutschlands

Auslegungshilfen und Kurzpapiere der Datenschutzkonferenz

Leitlinien & Kurzpapiere der Datenschutzbehörden

Forum: DSGVO Datenschutzgrundverordnung

Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine, 2017. C.H.BECK ISBN 978-3-406-71662-1

combit CRM Software

Die combit CRM Software ist eine sehr flexible Lösung, die umfangreiche individuelle Anpassungen und eine nahezu grenzenlose Erweiterung des Datenmodells erlaubt. Damit übertrifft unsere Software die branchenüblichen Möglichkeiten bei weitem. Die Bandbreite der Einsatzmöglichkeiten ist dadurch enorm und individuell. Aktuell erstellen wir einen Leitfaden mit Customizing-Vorschlägen, die unseren Kunden bei der Umsetzung der DSGVO helfen. Entsprechende Solution-Dateien werden ebenfalls zur Verfügung gestellt. Da jede Firma letztlich andere personenbezogene Daten sammelt und verwaltet, unterstützen wir unsere Kunden außerdem gerne bei deren Umsetzung jeglicher Anforderungen. Typischerweise ist der Anpassungsaufwand gering, da die nötigen Grundfunktionalitäten in unserer Software bereits vorhanden sind. Im Wesentlichen müssen die verwendeten Workflows entsprechend umgestaltet werden.

Wir verfolgen aktiv die Entwicklungen im Zusammenhang mit den verschiedenen Datenschutzgesetzen (DSGVO, BDSG-neu, ePrivVO usw.) und verbessern unsere Software fortlaufend, um allen combit-Kunden ein erstklassiges Produkt zu bieten.

Sie haben Fragen zu combit CRM?

Ein Gespräch mit uns schafft schnell Klarheit:
+49 (0) 7531 90 60 10 | service@combit.net

Tipp: Abonnieren Sie unseren Newsletter und verpassen Sie keine Neuigkeit zu combit CRM.
www.combit.net/newsletter

Disclaimer

Dieses Whitepaper kann nicht als rechtliche Beratung für Ihr Unternehmen dienen, auf die Sie sich bei der Einhaltung der Datenschutzgesetze der EU – wie der DSGVO – stützen können. Wir weisen Sie deshalb darauf hin, dass Sie bei Beratungsbedarf über Ihre Auslegung dieser Informationen oder über deren Richtigkeit und Vollständigkeit einen Anwalt hinzuziehen sollten.

combit GmbH | Untere Laube 30 | 78462 Konstanz | Deutschland

combit.net