CRM-Leitfaden

Datenschutz

EU-DSGVO
Chancen für Ihr Unternehmen

CAS SOFTWARE

CAS-Weg 1 - 5, 76131 Karlsruhe, www.cas.de

2. Auflage
Stand: April 2018

Inhalt

Einleitung 5

EU-DSGVO 7

- Was sind personenbezogene Daten? 8
- Welche Vorgänge sind betroffen? 9
- Grundsätze 10
- Rechtmäßigkeit 11
- Einwilligung 11
- Rechte der betroffenen Person 12

Datenschutz durch Technik und Organisation 15

- Verantwortlicher & Datenschutzbeauftragter 15
- Technische Maßnahmen 16
- Bei Verletzungen des Datenschutzes 17
- Datenschutz-Folgenabschätzung 17
- Datenübermittlung 17
- Haftung & Sanktionen 19

In der Praxis: Wie Sie Ihr Kundenbeziehungsmanagement datenschutzkonform gestalten 20

- Datenerhebung & -speicherung 20
- Verwendung personenbezogener Daten 24
- Gezielte Kundenansprache 24
- Was ist bei verschiedenen Werbeformen zu beachten? 27
- Rechte der Kunden 29
- Datensicherheit 30

Checkliste: Was Unternehmen jetzt tun sollten 33

Fazit 39

Einleitung

Willkommen in der digitalen Welt von heute. Das Internet bietet mit all seinen Daten, Informationen und Vernetzungen ungeahnte Chancen und Möglichkeiten. Fast selbstverständlich sammeln und teilen wir Informationen und Wissen, kommunizieren weltweit und in Sekundenschnelle, sind jederzeit erreichbar und wollen überall auf alle Daten zugreifen. Wir bestellen und bezahlen auf Knopfdruck, schließen online Geschäfte mit z. T. hoher Tragweite ab. Vieles läuft automatisiert und wie von Zauberhand.

Doch die Leichtigkeit hat auch ihre Risiken: Datendiebstahl und -missbrauch, Überwachung, der „gläserne Mensch" und Manipulation sind nur einige davon.

Um uns als Person, Verbraucher und Kunde vor den Risiken im Umgang mit personenbezogenen Daten zu schützen, wurden Gesetze und Regularien erarbeitet, die nun u. a. in der EU-Datenschutz-Grundverordnung (EU-DSGVO) europaweit einheitlich zusammengefasst und zu berücksichtigen sind.

Ab dem 25. Mai 2018 ist die EU-DSGVO anzuwenden und sorgt so für mehr Klarheit, Transparenz sowie Kontrollierbarkeit was den Schutz natürlicher Personen bei der Verarbeitung von deren personenbezogenen Daten angeht.

Vor allem die hohen Geldbußen von bis zu 20 Millionen Euro und viele offene Fragen haben die bisherigen Schlagzeilen dominiert.

Für Unternehmen ist die EU-DSGVO aber auch eine hervorragende Gelegenheit, gute und vertrauensvolle Kundenbeziehungen aufzubauen und diese mit gezielten, auf Kundenbedürfnisse ausgerichteten Marketing-, Vertriebs- und Serviceaktivitäten weiterzuentwickeln.

In diesem Leitfaden erklären wir allgemein, worum es in der EU-DSGVO geht und welche Auswirkungen sie auf das Kundenmanagement in Unternehmen hat. Außerdem erhalten Sie Tipps zur Umsetzung einzelner Vorgaben.

Bitte beachten Sie, dass diese Tipps nur sehr allgemein gehalten werden können. Auch kann nicht auf alle weiteren für Datenschutz und Datensicherheit zu berücksichtigenden Gesetze und Regularien eingegangen werden. Bei konkreten Fragen ziehen Sie daher Ihren Datenschutzbeauftragten oder einen Fachanwalt hinzu.

Machen Sie Ihr Kundenmanagement fit für den Datenschutz. Mit unseren CRM-Lösungen und unserem Know-how unterstützen wir Sie gerne!

Ihre
CAS Software AG
www.cas.de

in Kooperation mit:

Thomas Heimhalt
DATENSCHUTZ *perfect* GbR
Datenschutz-Berater, -Beauftragter und -Auditor (TÜV)
www.datenschutz-perfect.de

EU-DSGVO

Die Würde des Menschen ist unantastbar. Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht: Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.[1]

Zum Schutz dieser Grundrechte und im Hinblick auf eine europaweite Harmonisierung wurde eine neue europäische Datenschutz-Grundverordnung, die EU-DSGVO, erarbeitet. Sie ist ab dem **25. Mai 2018** anzuwenden.

Die neue Richtlinie gibt EU- und EWR-Bürgern mehr Kontrolle über ihre personenbezogenen Daten und stellt sicher, dass ihre Informationen europaweit geschützt sind. Damit wird der Spielraum geringer, personenbezogene Daten zu kommerziellen Zwecken zu erfassen und zu verwenden, wenngleich es nicht Ziel der Verordnung ist, Geschäfte zu unterbinden oder zu erschweren. Vielmehr soll die Aufbewahrung und Verwendung personenbezogener Daten transparenter werden.

Die EU-DSGVO gilt für alle Unternehmen, die Produkte an europäische Bürger verkaufen und deren personenbezogene Daten speichern bzw. verarbeiten – unabhängig dem eigenen Firmensitz („Marktortprinzip").

Weitere bisherige Regelungen – in Deutschland sind das u. a. die Datenschutzbestimmungen aus dem TKG (Telekommunikationsgesetz), dem TMG (Telemediengesetz) und dem Gesetz gegen den unlauteren Wettbewerb (UWG) – bleiben erhalten, müssen jedoch rechtskonform mit der EU-DSGVO sein.

Das sagt der Experte

Nehmen Sie die EU-DSGVO ernst und treffen Sie umgehend die notwendigen Maßnahmen zur Einhaltung der Bestimmungen, denn die **Sanktionen wurden deutlich angehoben:** Bei Verstößen gegen den Datenschutz drohen erhebliche Geldstrafen in Höhe von bis zu 20 Millionen Euro oder von bis zu vier Prozent des weltweiten Vorjahresumsatzes des Gesamtkonzerns – je nachdem, welcher Betrag der höhere ist. Für betroffene Personen, denen ein materieller oder immaterieller Schaden entstanden ist, besteht zudem ein Anspruch auf Schadenersatz.

[1] Gemäß Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta") sowie Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV).

Überblick über die wichtigsten Regelungen der EU-DSGVO

Die EU-DSGVO

- enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten und
- schützt die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten, wobei
- der freie Verkehr personenbezogener Daten in der EU aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden darf.

Was sind personenbezogene Daten?

Gemäß der EU-DSGVO sind personenbezogene Daten alle Informationen, die zur Identifizierbarkeit einer natürlichen Person beitragen, wie Namen, private und betriebliche Kontaktdaten (u. a. Anschrift, E-Mail-Adresse, Festnetz- oder Mobilnummern) ebenso wie Standortdaten, Bankdaten, Beiträge in den Social Media-Kanälen oder IP-Adressen – ohne Unterscheidung zwischen personenbezogenen Daten im privaten, öffentlichen oder arbeitsbezogenen Umfeld einer Person, denn Geschäftsbeziehungen werden immer von einzelnen (natürlichen) Personen[2] gepflegt.

Praxistipp

Im Rahmen einer Kundenbeziehung werden häufig auch private Informationen wie z. B. Geburtstag, Familie und Hobbys ausgetauscht. Prüfen Sie vor Speicherung solcher Daten im CRM, ob diese überhaupt gespeichert bzw. verarbeitet werden dürfen – idealerweise nur dann, wenn sie vertragsrelevant sind oder eine Einwilligung vorliegt.

[2] Art. 4 DSGVO

Welche Vorgänge sind betroffen?

Generell beinhaltet der Datenschutz alle Vorgänge mit personenbezogenen Daten.

Die Verordnung fasst dies unter „Verarbeitung“ zusammen[3], darunter versteht man:

- jeden ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten
- ausgeführt mit oder ohne die Hilfe automatisierter Verfahren.
- Betroffene Vorgänge:
  - das Erheben oder Erfassen,
  - die Organisation oder das Ordnen,
  - die Speicherung,
  - die Anpassung oder Veränderung,
  - das Auslesen, Abfragen oder die Verwendung,
  - die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung,
  - den Abgleich oder die Verknüpfung,
  - die Einschränkung,
  - das Löschen oder die Vernichtung.

[3] Art. 4 DSGVO

Grundsätze

Die EU-DSGVO schreibt die bisherigen datenschutzrechtlichen Grundsätze[4] fort und entwickelt sie weiter:

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben sowie in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

Zweckbindung

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Ändert sich der ursprüngliche Zweck, muss dies kommuniziert werden.

Datensparsamkeit/-minimierung

Weniger ist mehr: Es dürfen nur die personenbezogenen Daten in einem notwendigen Maß erhoben und verarbeitet werden, die für einen bestimmten Zweck angemessen und relevant sind.

Richtigkeit

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Speicherbegrenzung

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Danach sind die personenbezogenen Daten zu löschen oder zu anonymisieren. Ausnahmen der EU-DSGVO hierzu sind zu beachten.

Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Einhaltung der Grundsätze und Rechenschaftspflicht

Der Verantwortliche ist für die Einhaltung des Abs. 1 Art. 5 DSGVO verantwortlich und muss dessen Einhaltung nachweisen können.

[4] Art. 5 DSGVO

Rechtmäßigkeit

Allgemeiner Grundsatz für die Verarbeitung personenbezogener Daten ist ein sogenanntes Verbot mit Erlaubnisvorbehalt.[5] Die Verarbeitung von personenbezogenen Daten ist demnach nur dann zulässig, wenn eine Einwilligung des betroffenen Kunden (oder eine gültige Ausnahme nach Art. 6 DSGVO) vorliegt.

Einwilligung

Die Einwilligung unterliegt einigen Bedingungen[6], u. a.:

Nachweispflicht

Der Verantwortliche muss nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten für einen oder mehrere bestimmte Zwecke eingewilligt hat.

Klare Trennung

Erfolgt die schriftliche Einwilligung im Zusammenhang mit anderen Sachverhalten, so muss das Ersuchen um Einwilligung zur Datenverarbeitung so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Außerdem muss das Ersuchen in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen.

Hinweis auf Widerrufsrecht

Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

Freiwilligkeit

Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden.

Zweck- und Verarbeitungsbezug

Die betroffene Person ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

[5] Nach Art. 6 DSGVO,
[6] Art. 7 DSGVO und § 51 BDSG (neu). Für die Einwilligung eines Kindes sind weitere Bedingungen zu berücksichtigen (Art. 8 DSGVO)

Rechte der betroffenen Person

Mit der EU-DSGVO erhalten Einzelpersonen mehr Kontrolle über ihre Daten (Betroffenenrechte[7]) – dazu gehören u. a.:

Informationsrecht

Die betroffene Person muss vor dem Erheben und der Erfassung ihrer personenbezogenen Daten informiert werden. Sie muss explizit in die Erfassung der Daten einwilligen.

Recht auf Auskunft

Die betroffene Person hat das Recht, eine Auskunft darüber zu erhalten, ob und welche ihrer Daten verarbeitet werden, sowie weitere Auskunft/Informationen u. a. zu Verarbeitungszweck, Herkunft und Empfänger der Daten, Dauer der Speicherung und ihren Rechten.

Recht auf Berichtigung

Die betroffene Person kann verlangen, dass falsch oder unvollständig gespeicherte Daten berichtigt oder vervollständigt werden.

Recht auf Löschung („Recht auf Vergessenwerden“)

Die betroffene Person kann die unverzügliche Löschung ihrer Daten verlangen, wenn bspw. der ursprüngliche Zweck ihrer Verarbeitung nicht mehr besteht, die erteilte Einwilligung widerrufen wird, Widerspruch gegen die Verarbeitung eingelegt wird oder Daten unrechtmäßig verarbeitet wurden. In der EU-DSGVO aufgeführte Ausnahmen sind zu beachten.

Recht auf Einschränkung der Verarbeitung

Die betroffene Person kann die Einschränkung der Verarbeitung von Daten verlangen, wenn diese bspw. nicht korrekt sind, unrechtmäßig verwendet werden oder die Einwilligung zur Verarbeitung der Daten widerrufen wurde.

Recht auf Datenübertragbarkeit

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, welche sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und sie hat das Recht, diese Daten an einen anderen Verantwortlichen zu übermitteln oder übermitteln zu lassen.

Widerspruchsrecht

Die betroffene Person kann bezogen auf unterschiedliche Verwendungszwecke der Verarbeitung ihrer Daten jederzeit widersprechen. Bei der ersten Kommunikation muss auf das Widerspruchsrecht in einer verständlichen und von anderen Informationen getrennten Form hingewiesen werden.

[7] Art. 12ff DSGVO

Notizen

Datenschutz durch Technik und Organisation

Unter Berücksichtigung von u. a. Stand der Technik und Implementierungskosten sowie der Eintrittswahrscheinlichkeit und dem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen sind geeignete technische und organisatorische Maßnahmen (TOM) zur Datensicherheit umzusetzen.[8] Dabei muss das Sicherheitslevel der Höhe des Risikos entsprechen.

Die EU-DSGVO stellt die Bedeutung des technischen und organisatorischen Datenschutzes heraus und gibt den Verantwortlichen und den Auftragsverarbeitern gleichermaßen die Verantwortung dafür.

Verantwortlicher & Datenschutzbeauftragter

Der Verantwortliche und der Auftragsverarbeiter setzen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

Unternehmen, die personenbezogene Daten verarbeiten, müssen unter bestimmten Voraussetzungen einen eigenen Datenschutzbeauftragten benennen[9]. Dieser muss aufgrund beruflicher Qualifikationen oder umfassenden Fachwissens über eine hohe Kompetenz im Bereich des Datenschutzes verfügen. Kenntnisse in der praktischen Anwendung von Datenschutzregelungen sind unabdingbar.

Das sagt der Experte

Die Verantwortung für die Umsetzung von Datenschutz und Datensicherheit nach den gesetzlichen Vorgaben verbleibt trotz dem Einbinden kompetenter Personen weiterhin bei den Unternehmensverantwortlichen.

[8] Art. 5 Abs. 1 lit. f und Art. 32 DSGVO
[9] Art. 37 DSGVO

Technische Maßnahmen

Privacy by Design

Technische Maßnahmen zur Datensicherheit und -sparsamkeit

Datenschutz lässt sich am besten einhalten, wenn er bereits bei der Erarbeitung eines Datenverarbeitungsvorgangs technisch integriert ist. Dies hat Einfluss auf Auswahl und Entwicklung von Software und Systemen, die für die Datenverarbeitung genutzt werden.

Privacy by Default

Datenschutzfreundliche Voreinstellungen

Dadurch sollen möglichst wenig personenbezogene Daten verarbeitet werden können. Dies soll diejenigen Nutzer schützen, die weniger technikaffin sind und z. B. dadurch nicht geneigt sind, die datenschutzrechtlichen Einstellungen ihren Wünschen entsprechend anzupassen.

Praxistipps

- Achten Sie darauf, dass Hard- und Software immer dem Stand der Technik entsprechen. D. h. verwenden Sie möglichst aktuelle Produktversionen.
- Reichern Sie bei der Lead-Generierung bestehende Kundenprofile nicht immer nur weiter an, sondern überprüfen Sie stets in Bezug auf den Nutzungszweck, ob und welche Informationen wieder gelöscht werden können bzw. sogar gelöscht werden müssen.

Das sagt der Experte

Eine Verschlüsselung oder Pseudonymisierung von Daten, sowie die technische Fähigkeit, Vertraulichkeit, Integrität sowie Verfügbarkeit und Belastbarkeit der Systeme zu gewährleisten, kann von Vorteil oder gar erforderlich sein.

Bei Verletzungen des Datenschutzes

Meldung der Datenschutzverletzung

Verletzungen des Schutzes personenbezogener Daten müssen unverzüglich, nach Möglichkeit innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls, an die zuständige Aufsichtsbehörde gemeldet werden.[10] Eine Ausnahme besteht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen führt, z. B. durch geeignete Verschlüsselung personenbezogener Daten.

Benachrichtigung der betroffenen Person

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

Datenschutz-Folgenabschätzung

Birgt die Art der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten, muss der Verantwortliche bereits vorab eine Abschätzung der Folgen der Verarbeitung für den Schutz personenbezogener Daten durchführen.[11] Dies ist insbesondere der Fall bei neuen Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung. In Fällen wie u. a. der Verarbeitung besonders sensibler Daten sowie einer umfangreichen Videoüberwachung ist eine Datenschutz-Folgenabschätzung erforderlich.

[10] Art. 33f DSGVO
[11] Art. 35 DSGVO

Datenübermittlung

Besondere Aufmerksamkeit ist auf die Übermittlung von personenbezogenen Daten zu legen. Eine Übermittlung liegt dann vor, wenn Daten an Dritte weitergegeben werden. Dritte sind dabei Personen oder Stellen außerhalb des Verantwortlichen, davon ausgenommen sind die betroffenen Personen selbst sowie die Auftragsverarbeiter.

Eine Übermittlung liegt vor, wenn die Daten durch explizites Versenden oder eine gemeinsam genutzte Kundendatenbank nach Außen an einen Dritten weitergegeben werden. Das gilt auch, wenn es sich um ein Tochterunternehmen oder ein anderes Unternehmen der Gruppe oder des Konzerns handelt.

Eine Übermittlung personenbezogener Daten an ein Drittland ist nur unter bestimmten Voraussetzungen, wie u. a. der Einzelgenehmigung und Zustimmung der betroffenen Person zulässig. Damit soll sichergestellt werden, dass das durch die EU-DSGVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

Notizen

Haftung & Sanktionen

Hohe Geldstrafen

Es kann teuer werden, bis hin zur Existenzgefährdung: Nach den EU-DSGVO drohen bei Verstößen gegen den Datenschutz erhebliche Geldstrafen in Höhe von bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweiten Vorjahresumsatzes des Gesamtkonzerns – je nachdem, welcher Betrag der höhere ist.

Haftung für den Schaden

Jeder an einer Verarbeitung von personenbezogenen Daten beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht-datenschutzkonforme Verarbeitung verursacht wurde.[12]

Schadenersatz für betroffene Personen

Die EU-DSGVO führt außerdem für die betroffenen Personen einen Anspruch auf Schadenersatz bei materiellem oder immateriellem Schaden ein.

Praxistipps

- Dokumentieren Sie, was Sie in Ihrem CRM abbilden und für welchen Zweck.
- Speichern Sie nur die Daten, die Sie tatsächlich benötigen – weniger ist mehr!
- Definieren Sie eine klare Berechtigungsstruktur für den Zugriff auf die Daten.
- Dokumentieren Sie, woher Sie die Daten bzw. Informationen haben.
- Vermeiden Sie „doppelte" Datenhaltung, d. h. gleiche Daten an mehreren Stellen.

[12] Art. 82 DSGVO

In der Praxis: Wie Sie Ihr Kundenbeziehungsmanagement datenschutzkonform gestalten

Die Anforderungen an Unternehmen, die sich aus den Gesetzen und Regularien zum Datenschutz ergeben, lassen sich ohne Einsatz professioneller CRM-Systeme kaum mehr bewältigen. CRM-Lösungen bieten die technische Voraussetzung zur Umsetzung des Datenschutzes in Ihrem Unternehmen und unterstützen bei weiteren organisatorischen Maßnahmen.

Datenerhebung und -speicherung

Die Herausforderung beim Erstkontakt ist die rechtmäßige Erfassung der Interessenten- und Kundendaten:

- Wie kann ich Daten korrekt erfassen?
- Welche Daten darf ich speichern?
- Welche Daten muss ich speichern?
- Welche Daten darf ich gar nicht erst speichern?

Stichwörter sind **Einwilligung, Datensparsamkeit** und **Zweckbindung.**

Es dürfen nur die Daten erfasst und gespeichert werden, die zur korrekten Abwicklung eines Rechtsgeschäfts erforderlich sind.

Auch die Herkunft der Daten und ggf. deren Weitergabe müssen protokolliert und gespeichert werden, um Auskunft geben zu können.

Das sagt der Experte

CRM-Lösungen **unterstützen** bei der Umsetzung des Datenschutzes, ersetzen aber keineswegs weiter notwendige technische und insbesondere organisatorische Maßnahmen.

Die CRM-Lösungen der CAS Software AG bieten durch ihre technische Grundausstattung und benutzerdefinierte Anpassbarkeit wichtige Bausteine im Hinblick auf **Privacy by Design** und **Privacy by Default.**

Zum Einholen einer **Einwilligung** bietet sich ein Formular an. Achten Sie darauf, dass Sie eine klare und einfache Sprache verwenden und die Einwilligung freiwillig erteilt wird.

Das Formular sollte folgende Punkte enthalten:

- Welche Daten werden erfasst?
- Zu welchen Zwecken?
- Herkunft/Quelle des Kontaktes?
- Welche Kontaktart darf genutzt werden?
- Hinweis auf Datenschutzbestimmungen des Unternehmens mit Kontaktdaten des Verantwortlichen und ggf. Datenschutzbeauftragten

Das sagt der Experte

Bei elektronischen Formularen müssen Checkboxen zur Einwilligung leer, also nicht vorbelegt sein. Speichern Sie die Einwilligung mit Einwilligungstext im CRM, idealerweise in Verbindung (Verknüpfung) zur entsprechenden Adresse. Damit können Sie später aus der Kundenakte heraus die Einwilligung des Kunden zur Speicherung und Verarbeitung seiner Daten nachweisen.

Praxistipps zur Adress-Erfassung

- Nutzen Sie **Adress-Assistenten** zur einfachen und schnellen Adress-Erfassung per Copy & Paste – Tippfehler können so gar nicht erst entstehen.
- **Eingabehilfen,** die Vervollständigung und Konsistenzprüfung sorgen für vollständige sowie richtige Adressen.
- Legen Sie für alle nachzuweisenden Informationen **Felder an,** sofern diese in Ihrem CRM nicht bereits vorgesehen sind, z. B. für die Adressherkunft (Quelle des Kontaktes), Datum (Erstkontaktdatum), Erstkontakt durch (Mitarbeiter), Zweck (Zweckbindung), erlaubte Kontaktart (Kanal), Löschfrist/Löschdatum.
- Mit **Pflichtfeldern** stellen Sie sicher, dass Mitarbeiter auch alle relevanten und verpflichtenden Informationen zu einem Kunden oder Interessenten vollständig erfassen.
- Gemäß der Datensparsamkeit sollten nur die absolut notwendigen Daten erhoben und gespeichert werden. Definieren Sie keine Pflichtfelder für Daten, die nicht erforderlich sind.
- Nutzen Sie die Flexibilität Ihrer CRM-Lösung, um die Informationen zu einem Kontakt übersichtlich, ggf. auf verschiedenen Registern darzustellen und so eine einfache und schnelle Dateneingabe zu ermöglichen.
- Bei einer CRM-Lösung mit **Fragebogen-Modul** kann auch ein Fragebogen den Anwender beim Erfassen der Adresse oder beim Abklären von Kontaktwünschen (Zweck) leiten.
- Bietet das Fragebogen-Modul auch **Online-Fragebögen,** können Sie diesen auch vom Kunden eigenhändig ausfüllen lassen. So ist es ihm überlassen, welche Daten erfasst werden und zu welchem Zweck sie verwendet werden dürfen.
- Idealerweise können Antworten aus dem Fragebogen direkt mittels **Feldanbindung** in den Adressdatensatz übertragen werden. Damit werden unnötiger Arbeitsaufwand und eventuelle Übertragungsfehler vermieden.

Notizen

Verwendung personenbezogener Daten

Gezielte Kundenansprache

Nachdem eine Adresse korrekt erfasst und gespeichert wurde, wollen Sie den Kunden auch gezielt ansprechen.

Die Kundenansprache darf nur erfolgen:

- wenn eine Einwilligung vorliegt,
- nur über den erlaubten Informationskanal und
- nur zum zugestimmten Zweck.

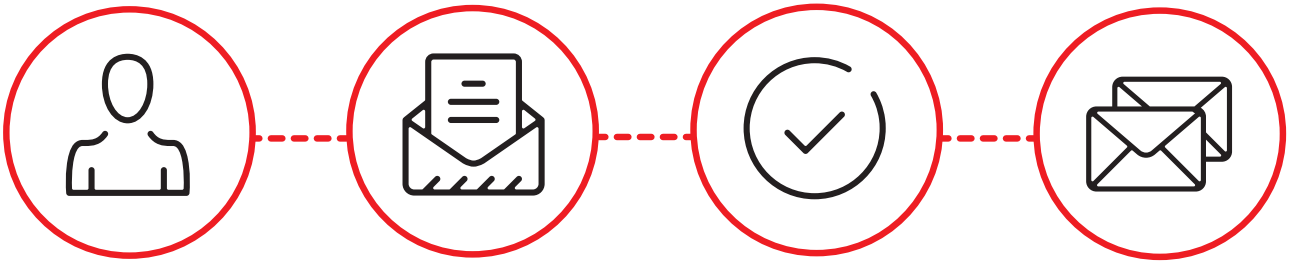
Für die Erlaubnis der passenden Kundenansprache ist eine **Einwilligung** (Opt-In) für die Zusendung insbesondere von Werbung vorgeschrieben.

Um Ärger und Missverständnisse zu vermeiden, wird das einfache **Opt-In** durch das **Double-Opt-In**-Verfahren ersetzt, bei dem der Interessent die Anmeldung z. B. zu einem Newsletter in einem zweiten Schritt bestätigen muss. Hierzu wird meist eine E-Mail mit der Bitte um Bestätigung an die eingetragene E-Mail-Kontaktadresse gesendet. Erst wenn die Bestätigung vorliegt, wird die Registrierung wirksam.

So holen Sie sich eine Einwilligung für das E-Mail-Marketing

Für eine datenschutzkonforme Einwilligung empfehlen wir das **Double-Opt-In**-Verfahren:

1. Formulieren Sie im Online-Formular eine Einwilligungserklärung.
   Sie sollte folgende Punkte enthalten:
   - Verwendungszweck, z. B. Themen, die im Newsletter behandelt werden
   - Informations-/Kommunikationskanal (E-Mail, Telefon, Fax, SMS, Brief)
     Feld/er für Kontaktdaten abhängig vom Kommunikationskanal – Pflichtfelder sollten nur für die absolut notwendigen Kontaktdaten definiert werden, z. B. Mail-Adresse für das E-Mail-Marketing
   - Datenschutzhinweis als Fließtext oder als Link zu den Datenschutzrichtlinien
   - Hinweis auf das Widerrufrecht für die allzeitliche Rücknahme der Einwilligung
   - Checkbox für die Einwilligung; markiert der Interessent diese Checkbox und schickt das Formular ab, willigt er der Werbung in einem ersten Schritt ein (Opt-In).
2. Im zweiten Schritt senden Sie dem Interessenten eine E-Mail an die angegebene E-Mailadresse, mit der er seine Einwilligung bestätigt. Am einfachsten geschieht das mit einem Bestätigungslink in der E-Mail.
   Zu beachten: Die Bestätigungs-E-Mail darf keine Werbung oder Angebote enthalten.
3. Betätigt der Interessent den Bestätigungslink, ist seine Einwilligung zum Erhalt von E-Mail-Werbung vollständig.



Was ist bei verschiedenen Werbeformen zu beachten?

Werbung per E-Mail

Die Einwilligung des Kunden durch das Opt-In-Verfahren ist mittlerweile generell erforderlich, im Unterschied zur früheren Opt-Out-Regelung.

Zu empfehlen ist das Double-Opt-In-Verfahren, das zusätzlichen Schutz vor Missbrauch bietet.

Der Adressat muss bei jedem Mailing auf sein Widerspruchsrecht aufmerksam gemacht werden und aufgezeigt bekommen, wie er seinen Widerspruch umsetzen kann.

Kurz gefasst: In jeder Werbemail muss eine Möglichkeit zur Abmeldung, idealerweise ein Abmelde-Link enthalten sein.

Werbung per Telefon

Im B2C-Bereich ist Werbung per Telefon nur mit Einwilligung gestattet. Im B2B-Bereich bleibt es bei der Regelung der konkludenten oder mutmaßlichen Einwilligung (vermutetes Interesse). Die Rufnummer muss immer übertragen werden.

Werbung per Telefax

Bei Werbung per Telefax gilt bei B2C und B2B die Notwendigkeit der Einwilligung gleichermaßen: eine Zustimmung ist immer erforderlich.

Printwerbung

Nicht- oder nur teiladressierte Prospektwerbung ist erlaubt, falls sich kein Aufkleber „Keine Werbung“ am Briefkasten befindet.

Bei adressierter Werbung gilt das Opt-In-Prinzip. Auch Kontakte ohne Opt-In können i. d. R. angeschrieben werden, sofern kein Widerspruch vorliegt:

- Bestandskunden
- Adressen aus allgemein zugänglichen Verzeichnissen (das Internet zählt allerdings nicht dazu)
- Spenden
- Transparente Übermittlung und Nutzung.
  Das bedeutet, dass die ursprüngliche Quelle der Adresse genannt wird. Übermittler und Empfänger müssen die Datenweitergabe protokollieren, u. a. wegen den Auskunftsansprüchen.

In jedem Fall ist die Robinsonliste zu beachten.

Das sagt der Experte

Fragen Sie Ihre Kunden und Interessenten am besten gleich beim Erstkontakt nach ihrer Einwilligung für den Erhalt von Mailings und Newslettern und lassen Sie sich diese z. B. nach dem Double-Opt-In-Verfahren bestätigen. Denken Sie auch an die Dokumentations- und Nachweispflicht aufgrund der EU-DSGVO.

Praxistipps für eine gezielte Kundensprache

- Mit einem **Fragebogen-Modul** Ihrer CRM-Lösung können Sie auf einfache Weise die Einwilligung einholen.
- Der positiv beantwortete Fragebogen dient als Legitimation für das Direktmarketing. Archivieren Sie diese Einwilligung im CRM, idealerweise in **Verbindung** (Verknüpfung) zur entsprechenden Adresse, damit Sie die Einwilligung jederzeit nachweisen können.
- Eigene Adressfelder für die Einwilligung und für die erlaubte/gewünschte Kontaktart erleichtern die Adressselektion und das Erstellen von Verteilern.
- Bei einer CRM-Lösung mit Marketing-Modul haben Sie i. d. R. umfangreiche Möglichkeiten um mehrstufige Kampagnen zu planen, durchzuführen und auszuwerten: Über Verteiler und Kampagnen können Sie Ihre Kunden gemäß ihren Wünschen ansprechen. Die Zuordnung der Kunden zu den einzelnen Kanälen Post, E Mail usw. erfolgt automatisch basierend auf **Feldern** wie „Bevorzugte Kontaktart" bzw. „Erlaubte Kontaktart". Wenn eine bestimmte Kontaktart nicht erlaubt ist, weist Sie das CRM idealerweise darauf hin.
- Auch externe E Mail-Marketing-Tools bieten komfortable und leistungsstarke Möglichkeiten der Kundenansprache. Gerade durch die Integration in die CRM-Lösung kommen die Adressen aus dem CRM und das personalisierte Mailing wird professionell umgesetzt. Anschließend werden An-/Abmeldungen sowie Bounces wieder ins CRM rückübertragen, so dass die Adressen mit ihren Einwilligungen und Verteiler entsprechend aktuell bleiben.
- Achten Sie darauf, dass in jedem E-Mailing ein **Abmeldelink** enthalten ist.
- Schaffen Sie die Rolle des Adress- bzw. Datenverantwortlichen in Ihrem Unternehmen.

Rechte der Kunden

Die Rechte der Kunden werden in der EU-DSGVO ausdrücklich gestärkt. Ein Kunde hat z. B. das Recht auf Berichtigung, Sperrung und Löschung seiner Daten. Außerdem hat er das Recht, unentgeltlich Informationen über alle gespeicherten personenbezogenen Daten zu erhalten – nach dem Recht auf Datenübertragbarkeit auch in einem strukturierten, gängigen und maschinenlesbaren Format.

Praxistipps um den Rechten der Kunden zu entsprechen

- CRM ist eine große, fast unverzichtbare Unterstützung, wenn es darum geht, Kundendaten, deren Erfassung, Bearbeitung und Verwendung zu dokumentieren. Eine **Journal-Funktion** kann sicherstellen, dass alle Änderungen am Adressdatensatz lückenlos protokolliert werden. In der Kundenakte lässt sich feststellen, wann die Adresse z. B. zu welchen Verteilern hinzugefügt wurde, welche Kontakte und Interaktionen stattgefunden haben und welche Informationen wann verschickt wurden.
- Hinterlegen Sie in der Akte auch, wann ggf. welche Daten an wen weitergegeben wurden und beachten Sie die zur Weitergabe nötige Erlaubnis.
- Mit **Reports und Berichten** lassen sich auf Knopfdruck Berichte erzeugen, die alle zur Person gespeicherten Daten auflisten. So können Sie dem Recht auf Auskunft lückenlos und ohne großen Aufwand nachkommen.
- Die meisten CRM-Lösungen bieten **Export-Funktionen,** idealerweise in verschiedenen Dateiformaten. Damit kommen Sie dem Recht auf Datenübertragbarkeit nach.
- Sind Daten zu berichtigen oder zu vervollständigen, kann sich ein **Fragebogen-Modul** mit Online Fragebogen als nützlich erweisen.
- Die betroffene Person hat das Recht, die Berichtigung, Löschung und/oder Sperrung ihrer Adresse zu verlangen. Auch kann sie die Weitergabe der eigenen Adresse untersagen. Kommen Sie diesem Kundenwunsch nach, indem Sie entsprechende **Kennzeichnungen** im CRM setzen.

Das sagt der Experte

Die Auskunftspflicht stellt Unternehmen vor große Herausforderungen, insbesondere wenn Daten verteilt vorliegen und erst zusammengesucht werden müssen. Hier ist effizientes Handeln unbedingt erforderlich, um schnell und einfach Auskunft geben zu können. Das gesteigerte Datenschutzbewusstsein bei den Verbrauchern kann die Anzahl der Anfragen steigern.

Datensicherheit

Zur Sicherheit von Kundendaten gehören:

- Schutz vor Datendiebstahl
- Schutz vor Missbrauch
- Schutz vor unberechtigtem Zugriff

Zu den Zielen einer Software gehört die Vereinfachung der Arbeit für Anwender. Eine Software bietet dafür viele nützliche Funktionen. Werden die Funktionen missbräuchlich eingesetzt, können sie aber auch Probleme bereiten.

Gerade in sensiblen Bereichen ist es wichtig, leistungsstarke und anpassbare Funktionen anzubieten.

Sicherheitsmechanismen von CRM-Lösungen können verhindern, dass Daten, insbesondere personenbezogene Adressdaten aus dem System abfließen. So sollten einzelne Funktionen wie z. B. Export, Berichte und Reports, mobile Datennutzung an spezielle Benutzerrechte gekoppelt werden, die der Administrator komplett abschalten oder nur für einzelne Mitarbeiter gezielt freigeben kann.

Dem gegenüber steht wiederum der Wunsch nach

- flexiblem Zugriff auf Daten von unterwegs über Schnittstellen,
- effizientes Arbeiten durch komfortable Funktionen wie Drag & Drop und
- Anpassbarkeit des Systems.

Jedes Unternehmen muss sein individuelles Optimum zwischen diesen beiden konträren Zielen selbst finden. Ein hundertprozentiger Schutz vor Datendiebstahl und/oder Missbrauch ist technisch nicht möglich – er kann aber deutlich erschwert werden.

Das sagt der Experte

Lassen Sie eine **Datenschutzerklärung** von Ihren Mitarbeitern unterschreiben, aus der klar hervorgeht, dass personenbezogene Daten Eigentum des Unternehmens sind und nur in definierten Anwendungsfällen und zu bestimmten Zwecken in bestimmtem Umfang verwendet werden dürfen.

Definieren Sie neben den technischen und organisatorischen Maßnahmen detaillierte Anweisungen und **Prozessbeschreibungen** für Ihre Mitarbeiter und schulen Sie diese darin, wie Datensätze zu erstellen, zu ändern und zu löschen sind. Vermitteln Sie Ihren Mitarbeitern die Relevanz der vorstehenden Themen.

Praxistipps zur Datensicherheit

- Für CRM-Lösungen wie auch für alle anderen Systeme gilt: Mit **Kennwörtern und Richtlinien** sorgen Sie für eine wirkungsvolle Zugriffskontrolle.
- Schaffen Sie klare **Rechtestrukturen** und sorgen Sie für deren Einhaltung. Je ausgefeilter und ausgereifter das Rechtesystem Ihrer CRM-Lösung ist, umso besser.

  Mögliche Rechte-Ebenen:

  - Rechte für Benutzergruppen, z. B. für Abteilungen und Hierarchiestufen
  - Rechte auf Module, z. B. Report und Marketing
  - Rechte für Funktionen, z. B. Im- und Export sowie mobile Nutzung von Daten
  - Individuelle Rechte auf Datensatz-Typen, z. B. Verkaufschancen
  - Individuelle Rechte auf Feldebene, z. B. für Mitarbeiterdaten
  - Individuelle Rechte auf einzelne Datensätze, z. B. vertrauliche Termine
  - Verschiedene Rechte von Lesen bis Vollständige Rechte
- Eine ausführliche Dokumentation des Rechtekonzeptes sorgt für Klarheit und Transparenz.
- Um den Admin-Aufwand im Rahmen zu halten, sollten im CRM die Rechte mehrerer Benutzer gleichzeitig geändert werden können und alle Rechteeinstellungen beim Duplizieren übernommen werden.
- Auch für das Löschen von Datensätzen sollte ein spezielles Recht einstellbar sein, damit keine Daten mutwillig oder aus Versehen permanent gelöscht werden können. Um einem Versehen vorzubeugen, ist beim Löschen von Daten ein 2-stufiger Prozess über den Papierkorb zu empfehlen.
- Achten Sie auf Qualitätssiegel wie **„Software Made in Germany“** und insbesondere **„Software Hosted in Germany“**. Software-Lösungen mit insbesondere dem zuletzt genannten Zertifikat zeichnen sich nicht nur durch erstklassige Qualität und Zukunftsfähigkeit aus, sondern werden zudem in einem Rechenzentrum in Deutschland nach deutschem Datenschutzrecht gehostet.[13]

[13] Die Qualitätssiegel „Software Made in Germany“ und „Software Hosted in Germany“ werden vergeben vom Bundesverband IT-Mittelstand (BITMi e.V.), www.software-made-in-germany.org

Notizen

Checkliste:
Was Unternehmen jetzt tun sollten

Bewusstsein schaffen

Schaffen Sie in Ihrem Unternehmen das Bewusstsein für den Datenschutz. Informieren Sie alle Mitarbeiter, die mit personenbezogenen Daten arbeiten über die Neuerungen und Richtlinien der EU-DSGVO.

Jeder Mitarbeiter muss wissen, welche Regelungen in seinem Aufgabenbereich anzuwenden sind. Nur so gewährleisten Sie, dass der Datenschutz in Ihrem gesamten Unternehmen gleichermaßen befolgt wird.

Datenschutzbeauftragten benennen und stärker einbinden

Sind regelmäßig mindestens neun Mitarbeiter mit der Verarbeitung personenbezogener Daten befasst, sollten Sie einen Datenschutzbeauftragten benennen.

Der Datenschutzbeauftrage kontrolliert und regelt die Umsetzung der Datenschutzbestimmungen in Ihrem Unternehmen.

Jede beliebige Person im Unternehmen kann zum Datenschutzbeauftragen benannt werden, sofern sie über die nötige Fachkompetenz im Datenschutz verfügt – oder sich diese im Rahmen von Schulungen und/oder Fortbildungen aneignet.

Audit der personenbezogenen Daten

Betrachten Sie die in Ihrem Unternehmen gespeicherten personenbezogenen Daten.

Dokumentieren Sie,

- welche personenbezogenen Daten gespeichert sind – dazu gehören sowohl Kundendaten, als auch Mitarbeiterdaten,
- woher die Daten stammen,
- zu welchem Zweck sie erhoben wurden,
- wo und wie lange sie gespeichert werden.

Falls nötig führen Sie eine Datenbereinigung durch, bei der nur diejenigen Daten beibehalten werden, die für die angegebenen Zwecke erforderlich sind. Die übrigen werden gelöscht.

Verfahrensverzeichnis / Verzeichnis der Verarbeitungstätigkeiten anlegen

Setzen Sie, wenn nicht bereits vorhanden, ein Verfahrensverzeichnis in Form einer Tabelle auf und stellen Sie es den Aufsichtsbehörden bereit. In der Tabelle wird aufgelistet, welche Daten wann, wie und warum im Unternehmen erhoben werden. Wichtig dabei ist, dass auch interne Personaldaten aufgeführt werden müssen, nicht nur die der Kunden.

Jede Stelle im Unternehmen legt eine Tabelle an, die Verfahrensbeschreibungen zu folgende Themen enthält:

- Art bzw. Kategorie der Daten (z. B. Adressdaten, Lebensläufe, Kontodaten etc.)
- Zweck der Datenverarbeitung (z. B. Bewerbermanagement, Marketing etc.)
- Erhebungsdatum
- Information des Betroffenen über die Erhebung, Speicherung und Verarbeitung seiner/ihrer Daten
- Einwilligung des Betroffenen
- Empfänger/Verantwortliche (wer hat Zugriff auf die Daten)
- Löschung und Löschfristen
- Verfahren der Auskunftserteilung und Inhalte der Auskunft
- Übertragung von Daten in ein anderes Format zur Datenportabilität
- Dauer der Speicherung von Daten (wenn sie nicht genutzt werden)
- Technische und organisatorische Maßnahmen des Datenschutzes (u. a. Pseudonymisierung)
- Weitergabe von Daten (z. B. in Drittstaaten)

Dokumentieren Sie künftig zudem den gesamten Weg personenbezogener Daten – von der Erhebung, über die Speicherung, bis hin zur Nutzung der Daten.

Prozesse festlegen und Prozesshandbuch erstellen

Dokumentieren Sie jetzt alle Prozesse in Ihrem Unternehmen, die mit der Datenverarbeitung zu tun haben und passen Sie sie, wenn nötig, an die Datenschutzrichtlinien an.

Zu diesen Prozessen gehören u. a. das Vorgehen zur Bearbeitung von Anfragen im Rahmen der Betroffenenrechte und Informationspflichten, zur Dokumentation bzw. der Nachweispflicht der Datenverarbeitung, sowie zur Meldung von Datenschutzverletzungen. Betrachten Sie dabei sowohl die technische Verarbeitung, als auch das Verhalten Ihrer Mitarbeiter.

Datenschutz-Folgeabschätzung

Wer mit besonders sensiblen Daten arbeitet, muss damit besonders umsichtig umgehen und unter Umständen eine so genannte Datenschutz-Folgeabschätzung durchführen. Sie dient Ihrem Unternehmen als Vorsorgemaßnahme, mit deren Hilfe Sie etwaige Risiken für die Persönlichkeitsrechte der Betroffenen bei der Verarbeitung ihrer Daten einschätzen können, um geeignete Schutzmaßnahmen planen zu können.

Insbesondere Unternehmen, die sensible Informationen wie z. B. zu Gesundheit, Finanzen, ethnischer Zugehörigkeit und politischer Einstellung etc. verarbeiten, sollten die Folgen abschätzen.

Einwilligung

Prüfen Sie, wie in Ihrem Unternehmen Einwilligungen zur Datenverarbeitung eingeholt, gespeichert und gemanagt werden. Kontrollieren Sie dabei sämtliche Formulare und Verfahren. Ist Ihr derzeit eingesetztes Verfahren nicht datenschutzkonform, dann passen Sie Ihre Verfahren und zugehörigen Formulare an. Erneuern Sie evtl. bestehende Einwilligungen.

TOM planen, prüfen und dokumentieren

Führen Sie in Ihrem Unternehmen technischen und organisatorischen Maßnahmen (TOM) zum Schutz personenbezogener Daten ein, sofern dies noch nicht geschehen ist. Neben den Vorrichtungen zu Privacy by Design und Privacy by Default, gehören zu den geeigneten Maßnahmen die Pseudonymisierung und die Verschlüsselung von Daten, sowie das Einführen von strikten Berechtigungsstrukturen für den Zugriff auf Daten.

Notizen

Fazit

In diesem Leitfaden haben wir uns lediglich mit den Datenschutz-Vorschriften beschäftigt, die sich insbesondere auf das Kundenbeziehungsmanagement auswirken. Wir haben weiterhin versucht, Möglichkeiten aufzuzeigen, wie mithilfe von CRM wichtige Anforderungen der EU-DSGVO, dem UWG und weiterer Gesetze umgesetzt werden können.

Setzen Sie sich intensiv mit dem Thema Datenschutz auseinander, prüfen Sie die vorhandenen Daten sowie sämtliche Prozesse im Hinblick auf personenbezogene Kundendaten und leiten Sie individuell für Ihr Unternehmen geeignete Maßnahmen zum Datenschutz ab.

Sprechen Sie mit Ihrem Datenschutzbeauftragten und erarbeiten Sie ein Handbuch für den Datenschutz in Ihrem Unternehmen.

Unternehmen ohne CRM haben es schwer, dem Datenschutz gerecht zu werden.

Nutzen Sie die CRM-Lösungen der CAS Software AG und profitieren Sie von den umfangreichen Möglichkeiten. Damit nehmen Sie die Herausforderung Datenschutz an und nutzen die Chancen.

Wir wünschen Ihnen ein gutes Gelingen und weiterhin begeisternde, erfolgreiche Kundenbeziehungen.

Ihre
CAS Software AG
www.cas.de

in Kooperation mit:

Thomas Heimhalt
DATENSCHUTZ *perfect* GbR
Datenschutz-Berater, -Beauftragter und -Auditor (TÜV)
www.datenschutz-perfect.de

Kontakt

CAS Software AG
CAS-Weg 1 - 5
76131 Karlsruhe
Telefon: +49 721 9638-188
E-Mail: crm@cas.de
www.cas.de