

Datenschutz in combit CRM

Die DSGVO und Ihre CRM Software

Inhalt

Einleitung	3
Dokumentationspflicht erfüllen	4
Datenherkunft + Verwendungszweck vermerken	4
Einwilligungen festhalten	8
Widerspruch berücksichtigen	11
Aktionen protokollieren.....	13
Daten schützen	15
Zugriff autorisieren	15
Daten einschränken.....	17
Daten sichern.....	19
Datenbank verschlüsseln	20
Löschfristen einhalten	20
Auskünfte erteilen	23
Daten übertragen.....	24
Disclaimer	26

Sie stehen noch ganz am Anfang bei der DSGVO?

[Jetzt Start-Whitepaper downloaden](#)

Einleitung

Konstanz, April 2019

Sehr geehrter combit CRM-Kunde,

mit der DSGVO hat der Gesetzgeber vielen Unternehmen in Europa eine ganze Fülle an Anforderungen mit auf den Weg gegeben. Die Auseinandersetzung mit den neuen Vorgaben ist für jedes Unternehmen zwingend notwendig. Das bedeutet leider zusätzliche Arbeit für Sie.

Die gute Nachricht ist: Wenn Sie dieses Whitepaper in den Händen halten, haben Sie wahrscheinlich schon den combit Relationship Manager erworben. Sie gehören damit nicht zur Gruppe der Unternehmen, die noch mit Listen und Tabellen arbeiten und somit von vornherein kaum Chancen haben, die DSGVO-Vorgaben umzusetzen. Und Sie gehören auch nicht zu der Gruppe der Unternehmen, die sich nun auf eine Lösung einstellen muss, die Sie in ein festes und umständliches DSGVO-Korsett zwingt, weil die entsprechende Lösung für ALLE entworfen wurde und nicht individuell für Ihr eigenes Unternehmen.

Sie haben mit der CRM-Software von combit eine starke Software, die individuell auf die Bedürfnisse Ihres Unternehmens abgestimmt wird. Unser Ziel für Ihr Unternehmen: Wir möchten, dass Sie mit minimalem Aufwand die Vorgaben der DSGVO umsetzen – ganz individuell und mit nur so viel DSGVO, wie in Ihrem konkreten Fall notwendig ist.

Die Werkzeuge, die der combit Relationship Manager mitbringt, machen nahezu jeden individuellen Prozess möglich. Im Hinblick auf die DSGVO möchten wir Ihnen als Software-Hersteller jedoch mehr bieten. Wir stellen Ihnen für die Herausforderungen der DSGVO eine schlüsselfertige Musterlösung bereit. Im Rahmen dieses Whitepapers möchten wir Ihnen unsere Lösung präsentieren. Zur konkreten technischen Implementierung in Ihre ggf. vorhandene Lösung gibt es ein eigenes Whitepaper in unserer Knowledgebase.

Unsere Kunden erhalten diese Lösung ab Version 10 in allen Editionen kostenfrei. Außerdem können Sie sich durch unser Experten-Team bei der technischen Implementierung in Ihre eigene CRM-Lösung aktiv unterstützen lassen – bei einer Abrechnung fair nach Aufwand und minutengenau.

Mein ganzes Team und ich sind sehr stolz, was wir im Hinblick auf die DSGVO für Sie geschaffen haben. Wir sind uns sicher: Unsere Lösung lässt Sie ruhiger schlafen und unterstützt Sie noch stärker bei dem, was Sie jeden Tag für Ihre Kunden schaffen.

Mit besten Grüßen aus Konstanz



Björn Eggstein
Geschäftsführer & Entwicklungsleiter combit CRM

Dokumentationspflicht erfüllen

Datenherkunft + Verwendungszweck vermerken

Weshalb?

Das Erfassen von Daten ist – nicht nur bei CRM-Systemen – im Hinblick auf die gesetzlichen Regelungen zu Recht ein wichtiger und kritischer Punkt. So müssen Sie nachvollziehbar belegen, auf welchem Weg ein personenbezogenes Datum in Ihren Besitz respektive in Ihr CRM-System gelangt ist, und für welchen Zweck es überhaupt erhoben wurde.

(Rechtsgrundlage: u. a. [Art. 5 DSGVO Abs. 1 lit f](#))

Wie?

Bei der Erfassung und jeder nachträglichen Ergänzung von personenbezogenen Daten sollte der Anwender die Datenquelle und den Verwendungszweck der eingegebenen Werte mit erfassen. Typische Datenquellen können eine Visitenkarte, das Impressum einer Website, ein öffentliches Verzeichnis u.v.m. sein.

Der Verwendungszweck ergibt sich typischerweise aus Ihrem Verarbeitungsverzeichnis, in dem Sie dokumentieren, für welchen Zweck Sie welche Daten erheben, wer darauf Zugriff hat, welche Löschfristen dafür gelten, inwiefern diese Daten an Dritte (z. B. Dienstleister) weitergegeben werden und was sonst noch wichtig sein könnte.

Ein typisches Beispiel ist „eMail-Marketing“:

1. Sie erfassen die eMail-Adresse.
2. Zusätzlich holen Sie auch eine Einwilligungserklärung der Person ein (Double Opt-in).
3. Sie löschen die eMail-Adresse automatisch 2 Jahre nach dem letzten Newsletter-Erhalt.
4. Sie geben ggf. nur dem Marketing-Team Zugriff auf das Feld.
5. Sie übertragen die eMail-Adresse dabei auch an ein externes Newslettertool, dessen Betreiber in der EU ansässig ist.

Lösung combit CRM:

Wesentlicher Fokus bei der Entwicklung unserer Lösung war, die Eingriffe in Ihren Arbeitsalltag so gering wie möglich zu halten und Ihnen trotzdem die Möglichkeit zu geben, die hohen Anforderungen an den Datenschutz vollständig umzusetzen. Eine Akzeptanz bei Ihren Mitarbeiterinnen und Mitarbeitern und damit eine wirkliche Umsetzung der Vorgaben erreichen Sie aus unserer Sicht nur dann, wenn die Vorgaben im Alltag zeitsparend umzusetzen sind.

Unsere Lösung unterstützt Sie hierbei aktiv und intelligent: So erscheint während jeder Änderung und bei der Erfassung von Kontakt-Daten unser neuer „Datenschutz-Block“.

Dieser Datenschutz-Block fragt gezielt nach den wesentlichen Informationen:

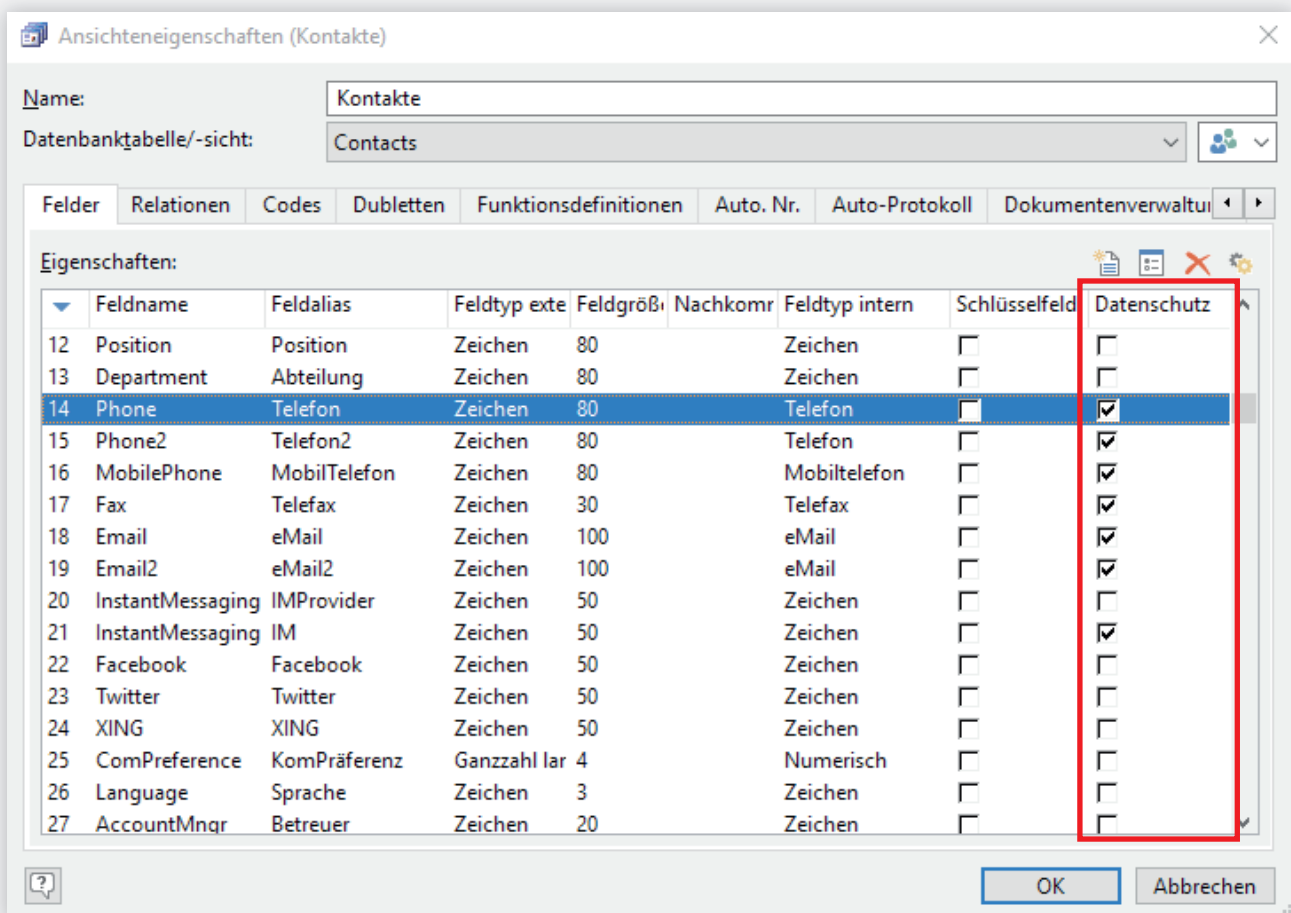
- Zu welchem Zweck werden die Daten erfasst?
- Woher stammen die Daten?
- Zusammenhang mit einer Aktivität?

So können die Benutzerinnen und Benutzer des cRM direkt aus den für Ihr Unternehmen festgelegten Verarbeitungstätigkeiten auswählen. Eine Mehrfachauswahl ist möglich und z. B. auch notwendig, wenn Sie mit einer Eingabe mehrere Verarbeitungstätigkeiten ausführen. Selbst eine sinnvolle Vorbelegung ist in unserer Lösung einstellbar.

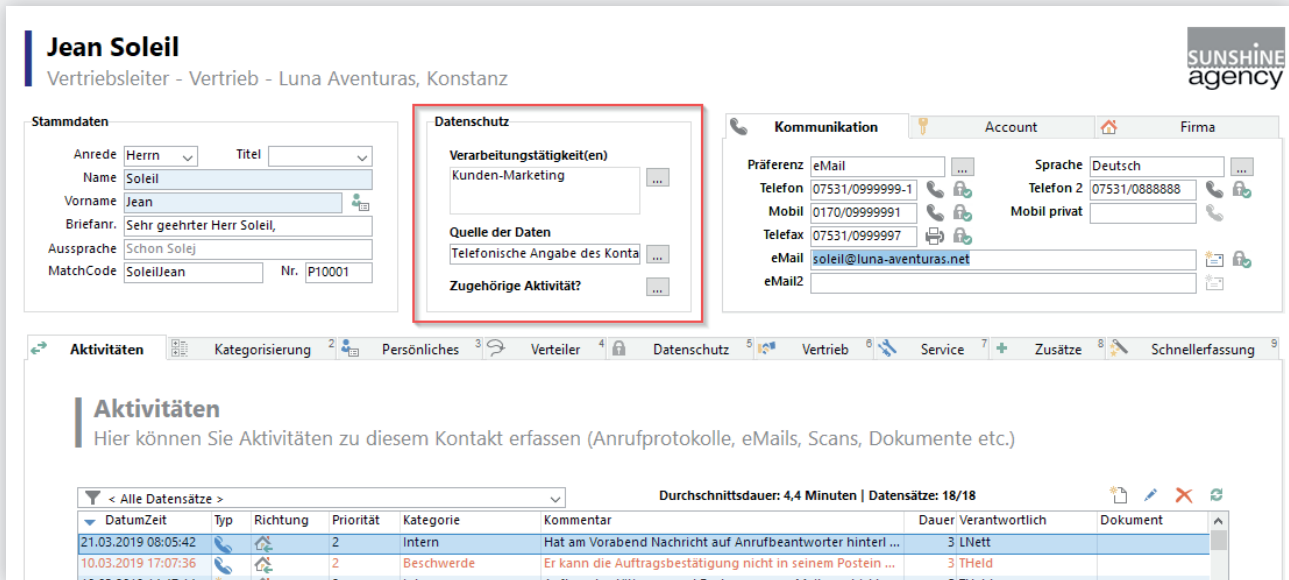
Nach dem Speichern kümmert sich unser System vollautomatisch um den Rest:

- Es ermittelt, welche Eingaben in der Eingabemaske vorgenommen wurden.
- Zu jeder Feld-Änderung wird ein eigener Eintrag im Datenschutz-Protokoll angefertigt.
- Am Ende ist detailliert pro Datensatz protokolliert: Wer hat wann welchen Inhalt aus welchem Grund aus welcher Quelle in welches Feld eingetragen oder gelöscht? Wann müssen die Inhalte wieder gelöscht werden?
- Dieses umfassende Protokoll ist später nicht nur ein Nachweis, sondern auch eine gute Grundlage für andere wichtige Schritte im Hinblick auf den Datenschutz, z. B. das automatisierte Löschen von Feldinhalten und Datensätzen oder auch die Erteilung von Auskünften.

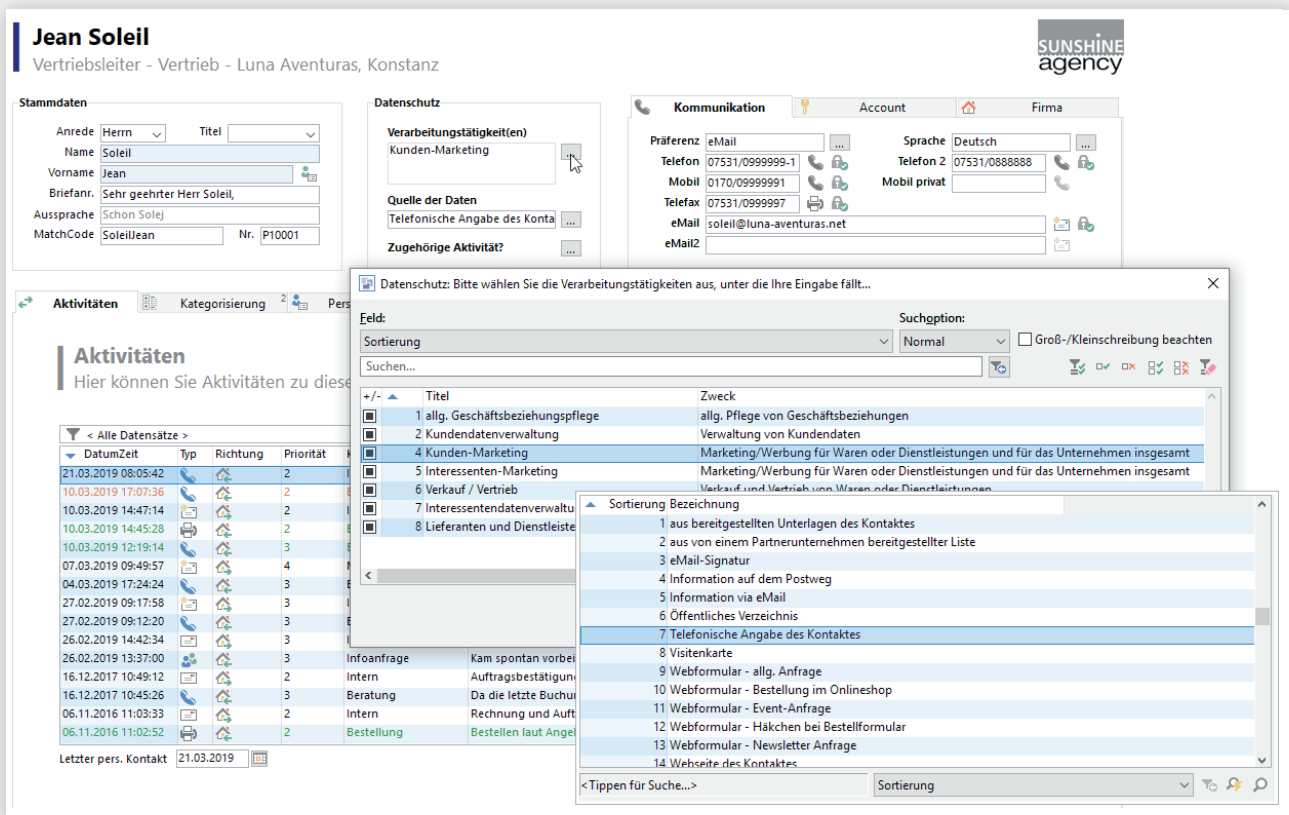
Sie haben eigene individuelle, personenbezogene Felder, die auch in diesem Rahmen derart umfassend protokolliert werden sollen? Dann können Sie frei definieren, welche Felder im Rahmen des Datenschutz-Protokolls überwacht werden sollen. Hierfür finden Sie in den Ansichteneigenschaften unsere Datenschutz-Checkbox.



Eigene, individuelle Felder für den Datenschutz kennzeichnen.



Direkte Erfassung von Verwendungszweck und Herkunft an Ort und Stelle.



Die auswählbaren Verwendungszwecke und Quellen ergeben sich direkt aus den im combit CRM hinterlegten Verarbeitungstätigkeiten.

Jean Soleil

Vertriebsleiter - Vertrieb - Luna Aventuras, Konstanz

Stammdaten

Anrede: Herr | Titel: | Name: Soleil | Vorname: Jean | Briefanr.: Sehr geehrter Herr Soleil, | Aussprache: Schon Solej | MatchCode: SoleilJean | Nr.: P10001

Datenschutz

Verarbeitungstätigkeit(en): allg. Geschäftsbeziehungs-pflege | Quelle der Daten: Telefonische Angabe des Kontakts | Zugehörige Aktivität?:

Kommunikation | Account | Firma

Präferenz: eMail | Sprache: Deutsch | Telefon: 07531/0999999-1 | Telefon 2: 07531/0888888 | Mobil: 0170/09999991 | Mobil privat: | Telefax: 07531/0999997 | eMail: soleil@luna-aventuras.net | eMail2:

← Aktivitäten 1 | Kategorisierung 2 | Persönliches 3 | Verteiler 4 | **Datenschutz** | Vertrieb 6 | Service 7 | Zusätze 8 | Schnellerfassung 9

Informationen und Aktionen zum Datenschutz zu diesem Kontakt

Datenschutz-Protokoll / Historie

Typ	DatumZeit	Kommentar	Verantwortlich	Datenquelle	Alter Wert	Neuer Wert
!	18.03.2019 11:07:50	Status für die Rufnummer 0170/09999991 im Feld "MobilTelefon" ...	THeld			
↻	18.03.2019 11:07:30	Der Inhalt des Feldes "MobilTelefon" wurde aktualisiert.	MPfeffer	Visitenkarte	[Feld ohne Inhalt]	0170/09999991
📄	28.02.2019 11:09:57	Datensatz wurde exportiert mit Vorlage 'Kontakte - Datenübertra...	THeld			
📄	05.02.2019 09:04:29	In den Verteiler "Weihnachtskarte" aufgenommen.	THeld	Webformular ...		
📄	05.02.2019 09:04:29	In den Verteiler "VIP-Kunden" aufgenommen.	THeld	Webformular ...		
📄	05.02.2019 09:04:29	In den Verteiler "Großer eMail-Verteiler" aufgenommen.	THeld	Webformular ...		
📄	28.10.2016 10:57:33	In den Verteiler "Newsletter-Verteiler" aufgenommen.	MPfeffer	Webformular ...		

Aktionen

Den Einträgen zur Kontakt-Neuanlage eine Aktivität zuordnen...

Automatisch erstelltes Datenschutz-Protokoll zum Kontakt mit allen Informationen.

Sortierung	Titel	Zweck
1	allg. Geschäftsbeziehungs-pflege	allg. Pflege von Geschäftsbeziehungen
2	Kundendatenverwaltung	Verwaltung von Kundendaten
3	eMail-Marketing	Newslettermarketing
4	Kunden-Marketing	Marketing/Werbung für Waren oder Di
5	Interessenten-Marketing	Marketing/Werbung für Waren oder D
6	Verkauf / Vertriebs	Verkauf und Vertriebs von Waren oder D
7	Interessentendatenverwaltung	Pflege von Beziehungen zu Interessent
8	Lieferanten und Dienstleisterdatenverwaltung	Einkauf von Waren oder Dienstleistung

Verarbeitungstätigkeiten

Hier können Sie die Verarbeitungstätigkeiten für die DSGVO definieren

Inhalt	Datenschutz-Informationen
<p>Titel: eMail-Marketing</p> <p>Zweck: Newslettermarketing</p> <p>IT-System: combit CRM</p> <p>Betroffene: Kunden, Interessenten</p> <p>Datenkategorien: <bitte ausfüllen> (Beispiel: E-Mail Adresse, (optional) Vorname und Nachname)</p> <p>Datenherkunft: <bitte ausfüllen> (Beispiel: Newsletterformular Webseite)</p> <p>Rechtsgrundlage: Einwilligung</p> <p>Zugriffsberechtigte: Marketing</p> <p>Sonstiges: DIE ANGABEN STELLEN LEDIGLICH BEISPIELE DAR UND MÜSSEN FÜR IHR UNTERNEHMEN KONKRET AUSGEFÜLLT WERDEN.</p>	<p>Verarbeitung durch Dritte: Marketing-Dienstleister</p> <p>Übermittlung an Drittstaaten: (nein)</p> <p>Auftragsverarbeitungsvertrag: abgeschlossen</p> <p>TOM: siehe TOM im AVV</p> <p><input checked="" type="checkbox"/> Datenminimierung</p> <p><input checked="" type="checkbox"/> Prozessdokumentation vorhanden</p> <p>Informiert mittels: <bitte ausfüllen> (Beispiel: Datenschutzerklärung Webseite, Mitarbeiter, Email...)</p> <p><input checked="" type="checkbox"/> Datenübertragbarkeit</p> <p>Löschfrist: Aus Verteiler entfernen 2 Jahre nach letzter Verteiler...</p> <p>Hinweis: Bitte beachten Sie, dass diese Verarbeitungstätigkeit nur für die Ansicht "Verteilerzuordnungen" zur Verfügung steht, die in der ausgewählten Löschfrist festgelegt wurde. Duplizieren Sie die Verarbeitungstätigkeit ggf. und wählen eine andere Löschfrist, um diese auch in anderen Ansichten verwenden zu können.</p> <p>Risikoabschätzung: gering</p> <p>Folgenabschätzung: nicht notwendig</p> <p>eMail-Opt-in für Newsletterverwaltung</p> <p><input checked="" type="checkbox"/> Diese Verarbeitungstätigkeit für die Newsletterverwaltung verwenden</p> <p>Hinweis: Es sollte nur eine Verarbeitungstätigkeit für das eMail-Opt-in-Verfahren der Newsletterverwaltung aktiviert werden.</p>

Verzeichnis für Verarbeitungstätigkeiten direkt im CRM-System administrierbar.

Einwilligungen festhalten

Weshalb?

Personen müssen i.d.R. damit einverstanden sein, dass Sie deren Daten verarbeiten. Diese Einwilligung müssen Sie dann belegen können. (Rechtsgrundlage: u.a. [Art. 6 DSGVO](#) und [Art. 7 DSGVO](#))

Wie?

Kernstück bei diesem Thema ist also eine adäquate allgemeine Einwilligungserklärung. Diese kann z. B. an einer Stelle, an der Ihr Kunde seine Daten „hinterlässt“, z. B. bei einem Webformular, entsprechend angezeigt werden.

Diese konkrete Einwilligung muss dann dokumentiert werden, idealerweise direkt als Aktivität bei einem Datensatz. Bei einer Newsletter-Bestellung kann dies zum Beispiel die Double-Opt-in Bestätigung als Dokument oder eine Nachricht zur Aufnahme der Person in einen Newsletter-Verteiler/-Kampagne sein.

Lösung combit CRM:

Die meisten unserer Kunden erfassen bereits schon alle „Ereignisse“ eines Kunden (also eMails, Telefonate, Briefe, etc.) direkt im entsprechenden Datensatz als Aktivität. Dies hat im Alltag sehr große Vorteile. Sie und Ihre Kolleginnen und Kollegen sehen auf einen Blick: Was war wann zuletzt bei welchem meiner Kontakte los? Welcher Kollege hat sich darum gekümmert? Was wurde kommuniziert? Wie ist man verblieben? Machen Sie dies noch nicht, so ist jetzt ein wirklich guter Zeitpunkt, darüber nachzudenken, dieses mächtige Instrument, das wir in allen unseren Lösungen kostenfrei mitliefern, in Ihren Arbeitsalltag zu integrieren. Der Nutzen ist gewaltig!

Als „Nachweis“ im Hinblick auf den Datenschutz hinterlegen Sie ganz einfach einige dieser Aktivitäten, die Sie routinemäßig erfassen, zusätzlich, um hinterher folgendes schlüssig belegen zu können:

- Aus dieser Quelle habe ich die Mobilfunkrufnummer.
- Aus diesem Grund habe ich diesen Kontakt in den Newsletter-Verteiler/-Kampagne aufgenommen.
- Aus diesem Grund habe ich die Rufnummer von meiner Sperrliste genommen.

In unserer Lösung bieten wir Ihnen die Möglichkeit, direkt eine Aktivität des Kontaktes anzugeben, auf der diese Datenerhebung fußt. Solch eine Aktivität ist zum Beispiel die eMail eines Kunden, in der er bittet, ihm Informationsmaterial per eMail zuzusenden, woraufhin Sie die eMail-Adresse im System überhaupt erst erfassen. Im Falle einer Newsletter-Bestellung über den CRM kann dies alles sogar komplett automatisch erfolgen. Weitere Details zum Thema „Newsletter-Bestellung automatisieren“ finden Sie in unserer [Knowledgebase](#).

Datenschutz-Protokoll / Historie			Aktionen			
Typ	DatumZeit	Kommentar	Verantwortlich	Datenquelle	Alter Wert	Neuer Wert
	18.03.2019 11:07:50	Status für die Rufnummer 0170/09999991 im Feld "MobilTelefon" ...	THeld			
	18.03.2019 11:07:30	Der Inhalt des Feldes "MobilTelefon" wurde aktualisiert.	MPfeffer	Visitenkarte	[Feld ohne Inhalt]	0170/09999991
	28.02.2019 11:09:57	Datensatz wurde exportiert mit Vorlage 'Kontakte - Datenübertra...	THeld			
	05.02.2019 09:04:29	In den Verteiler "Weihnachtskarte" aufgenommen.	THeld	Webformular ...		
	05.02.2019 09:04:29	In den Verteiler "VIP-Kunden" aufgenommen.	THeld	Webformular ...		
	05.02.2019 09:04:29	In den Verteiler "Großer eMail-Verteiler" aufgenommen.	THeld	Webformular ...		
	28.10.2016 10:57:33	In den Verteiler "Newsletter-Verteiler" aufgenommen.	MPfeffer	Webformular ...		

Nachvollziehbarkeit bei der Aufnahme in Verteiler/Kampagnen.

Newsletter-Verteiler / 23.10.2018

Jean Soleil, Luna Aventuras, Konstanz

Reaktion

Datenschutz

Verarbeitungstätigkeit(en)
eMail-Marketing

Quelle der Daten
Webformular - Häkchen bei Be...

Zugehörige Aktivität?

Zuordnungen

Der folgende Kontakt ist zugeordnet...

Jean Soleil, Luna Aventuras

Kontakt zuordnen... Gehe zu Kontakt Gehe zu Firma

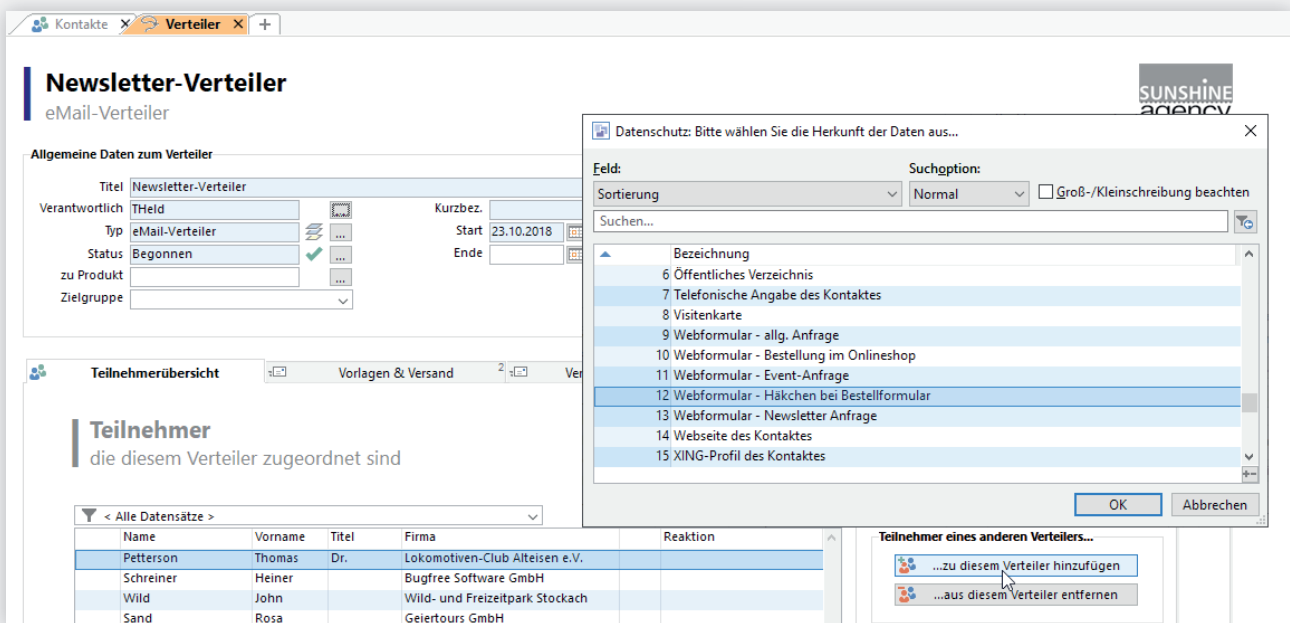
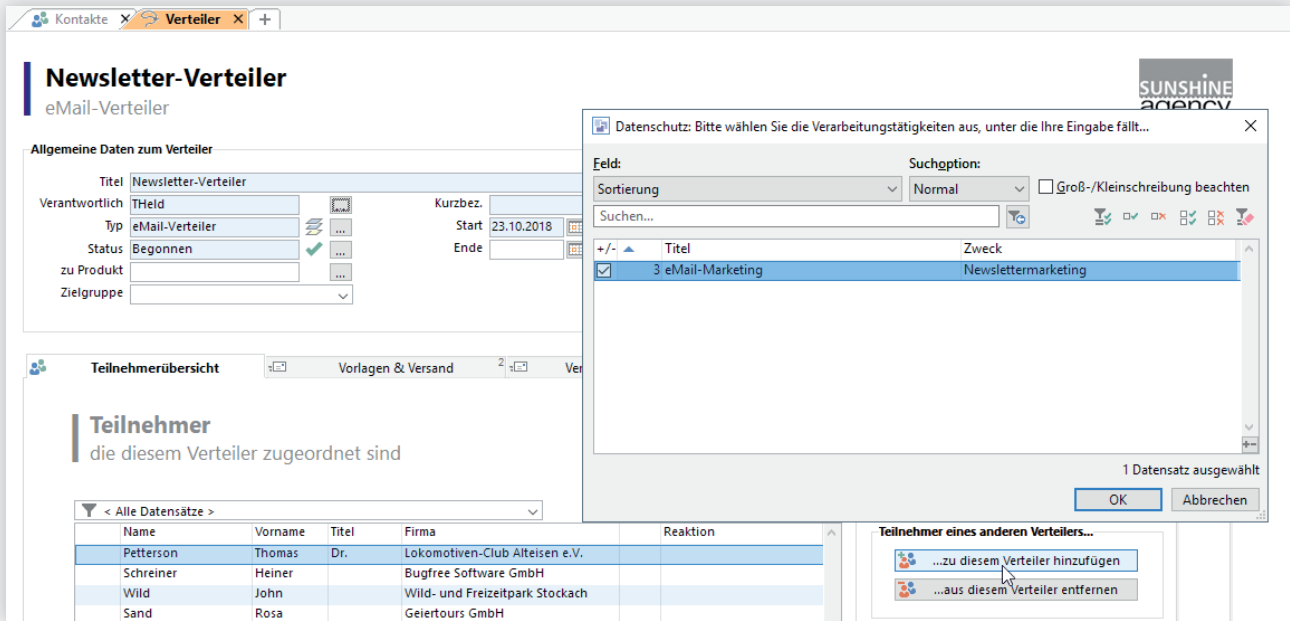
Der folgende Verteiler ist zugeordnet...

Newsletter-Verteiler / 23.10.2018

Verteiler zuordnen... Gehe zu Verteiler

Aktivitäten auswählen...

Dokumentation bei jeder Aufnahme einer Person in einen Verteiler/Kampagne.



Auch bei der Sammelverarbeitung von Verteilern/Kampagnen ist die Datenschutz-Dokumentation direkt im Workflow integriert.

Widerspruch berücksichtigen

Weshalb?

Es wird Menschen geben, die nicht möchten, dass Sie ihre Daten weiter verarbeiten. Sie sind dazu verpflichtet, jedem Widerspruch zur Verarbeitung der Daten einer Person nachzukommen. Und man ist gut beraten, dies gewissenhaft zu tun. Denn besonders kritisch kann es dann werden, wenn z. B. ein übereifriger Vertriebsmitarbeiter einen etwaigen Widerspruch zur telefonischen Kontaktaufnahme übersieht und die betroffene Person diesen Fehler nicht wirklich verzeihen möchte.

(Rechtsgrundlage: u.a. [Art. 21 DSGVO](#))

Wie?

Sie sollten etwaige Kommunikationssperren beim Datensatz direkt in Ihrer CRM-Datenbank hinterlegen können, z. B. bei einer eMail-Adresse oder bei einer Rufnummer.

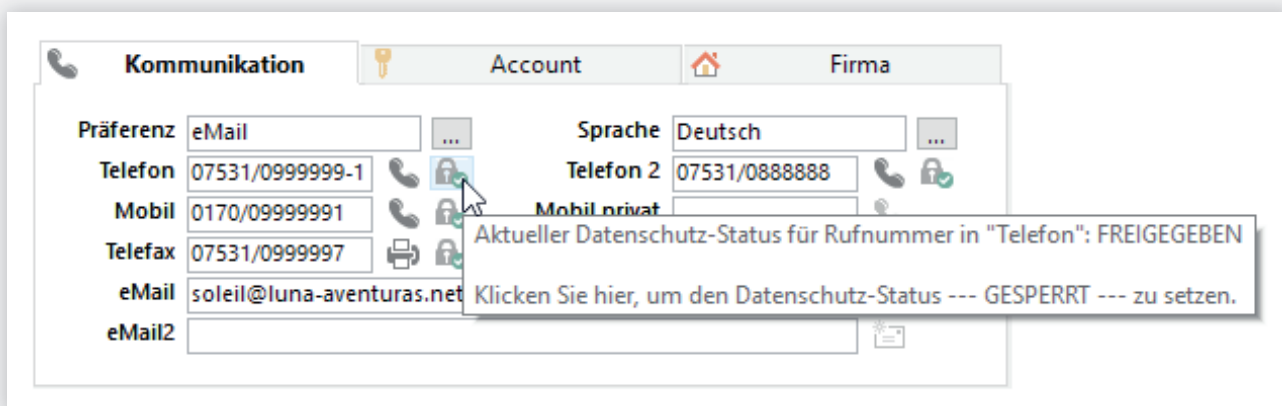
Lösung combit CRM:

Für jedes Kommunikationsfeld im CRM wird ein Status festgehalten. Es gibt die Möglichkeiten „unbekannt“, „erlaubt“ oder „gesperrt“. Der aktuelle Status wird neben den entsprechenden Kommunikationsfeldern über ein Symbol dargestellt. Er kann in Filtern und Formeln jederzeit berücksichtigt werden, z. B. beim Vorbereiten einer Aussendung oder beim Export.

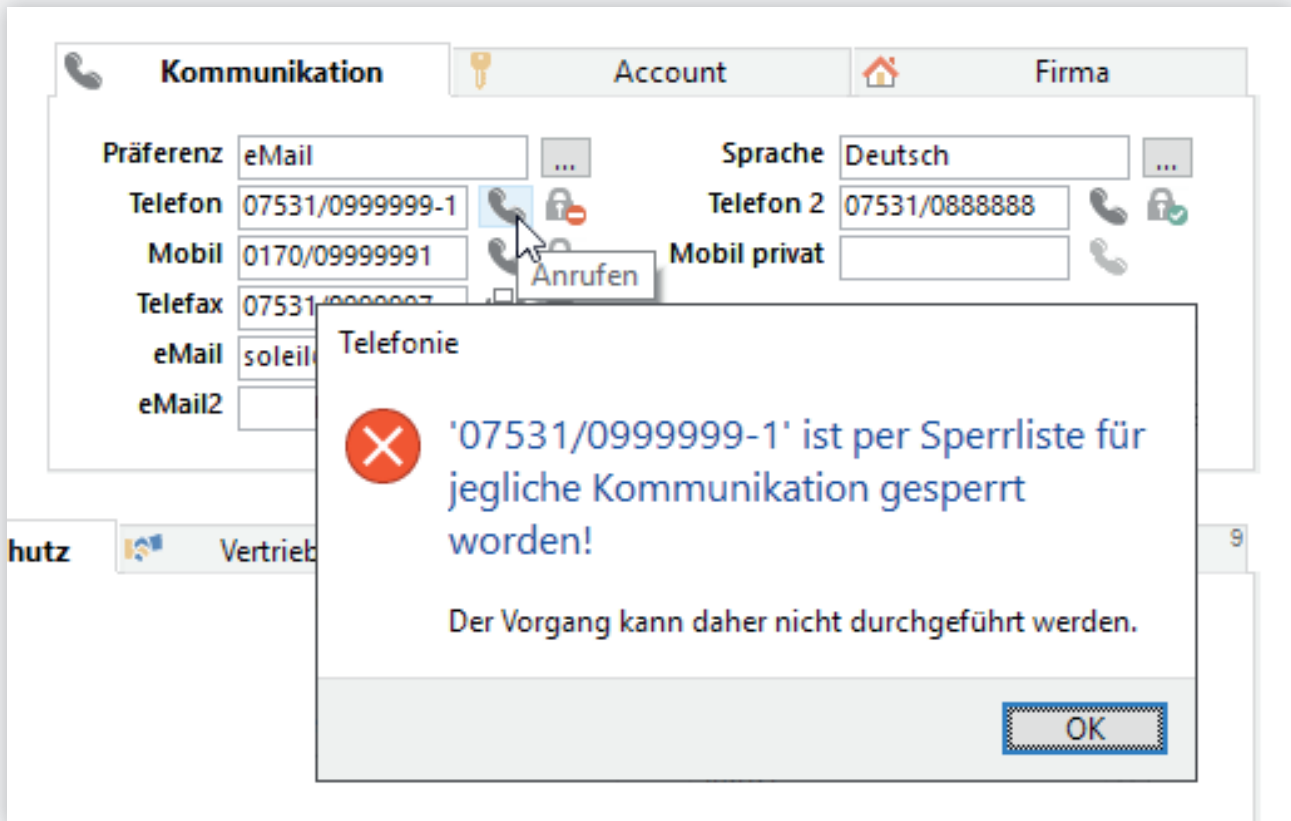
Zusätzlich zum Status eines Kommunikationsfeldes gibt es noch unsere Sperrliste. Es handelt sich dabei um ein „Sicherheitsnetz“: Setzen Sie für den Inhalt eines Kommunikationsfeldes den Status „gesperrt“, wird dieser zusätzlich auf eine globale Sperrliste im CRM gesetzt: Dadurch wird selbst eine unabsichtliche Kontaktaufnahme per eMail oder Telefon aus der Software heraus zuverlässig verhindert. Auch dann, wenn z. B. der Status dieser eMail-Adresse bei einem anderen Datensatz nicht als „gesperrt“ gekennzeichnet wurde.

Die Erlaubnis zum Ändern dieser globalen Sperrliste (Hinzufügen und Entfernen von eMail-Adressen und Telefonnummern) wird über zwei Benutzerrechte „Kommunikationsdaten in Sperrliste aufnehmen bzw. entfernen“ in der Benutzerverwaltung gesteuert.

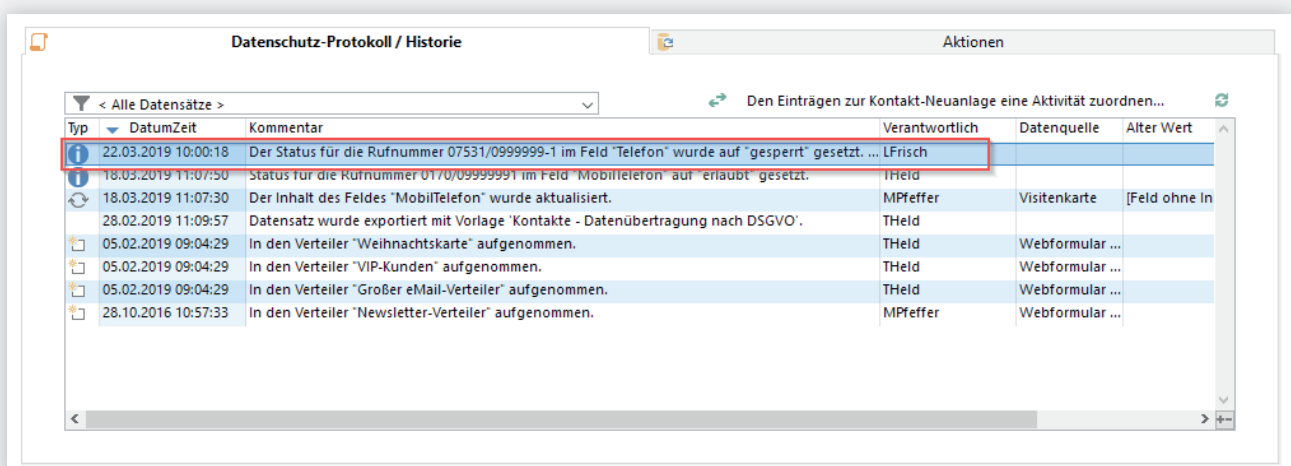
Das Setzen des Status und das Hinzufügen und Entfernen von Sperrlisten-Einträgen ist in unserer Lösung für alle Telefonnummern und eMail-Adressen in der Ansicht „Kontakte“ bereits für Sie vorkonfiguriert. Es gilt aber auch hier: Sie können diese Lösungen auch in eigene Ansichten für eigene Felder vom Typ „eMail“ oder „Rufnummer“ übernehmen. Ein entsprechender datenschutzrechtlicher Nachweis wird vollautomatisch im Datenschutz-Protokoll angefertigt.



Einwilligungsstatus bei jedem Kommunikationsfeld erkennbar und einstellbar.



Zuverlässiges Blockieren der Kommunikation.



Datenschutzrechtlicher Nachweis.

Aktionen protokollieren

Weshalb?

Nicht nur die Erhebung personenbezogener Daten, sondern auch ihre weitere Verarbeitung sind im Hinblick auf den Datenschutz von großem Interesse. Beides muss dokumentiert werden, um eine lückenlose Nachvollziehbarkeit des Datenflusses zu gewährleisten. (Rechtsgrundlage: u.a. [Art. 5 DSGVO](#))

Besonders wichtig ist diese Dokumentation insbesondere dann, wenn die Daten das Unternehmen verlassen und zum Beispiel an einen Dienstleister (Druckerei, Newsletter-Versender o.ä.) übergeben werden.

Ein prägender Begriff ist in diesem Zusammenhang das „Recht auf Vergessenwerden“. Sie sind verpflichtet, die Löschung eines personenbezogenen Wertes oder Datensatzes auch an alle Empfänger dieser Daten, wie eben externe Dienstleister, weiterzuleiten. Dies ist nur möglich, wenn Sie diese Empfänger entsprechend im System nachführen.

Wie?

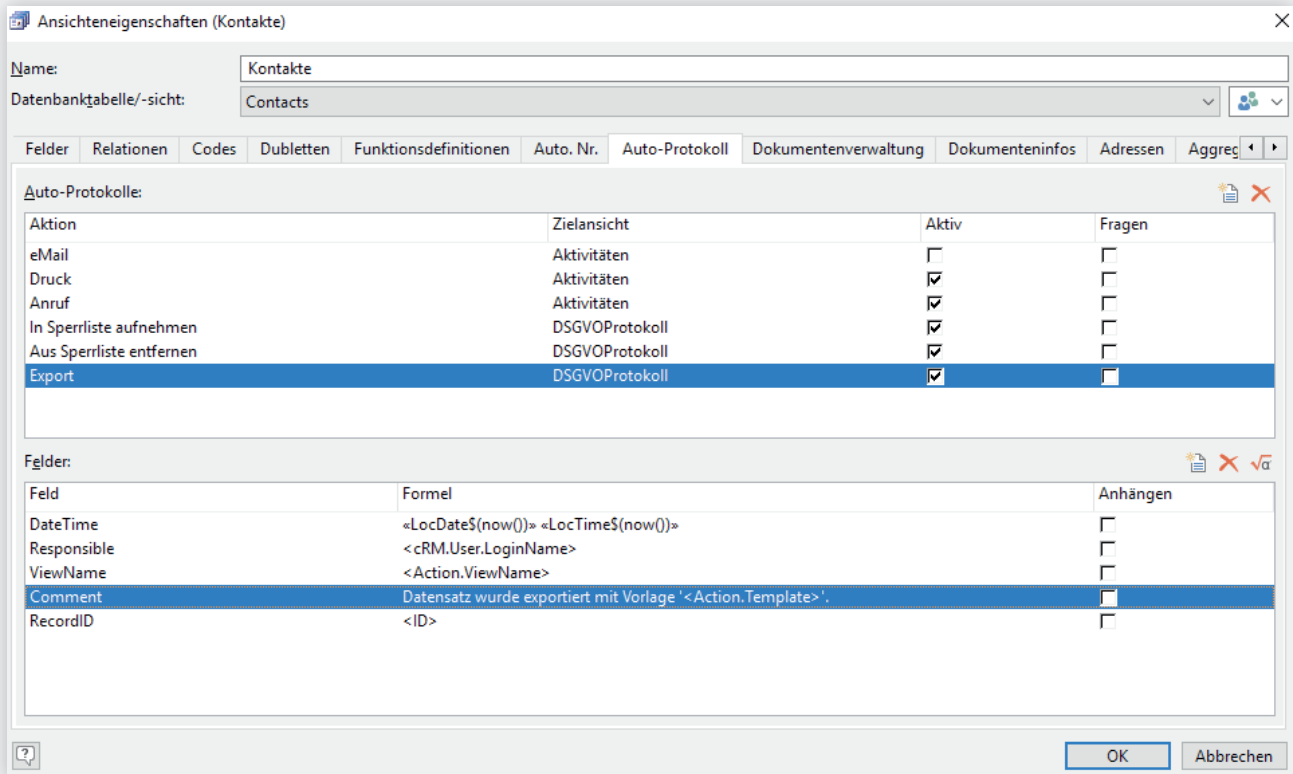
Bei bestimmten kritischen Aktionen / Verarbeitungstätigkeiten sollten automatisch entsprechende Vermerke im Datenschutz-Protokoll vorgenommen und dem jeweiligen Kontakt zugeordnet werden. Das schafft - ohne Zusatzaufwand für Ihr Unternehmen - absolute Transparenz und Klarheit darüber, was mit den erfassten Daten passiert ist.

Lösung combit CRM:

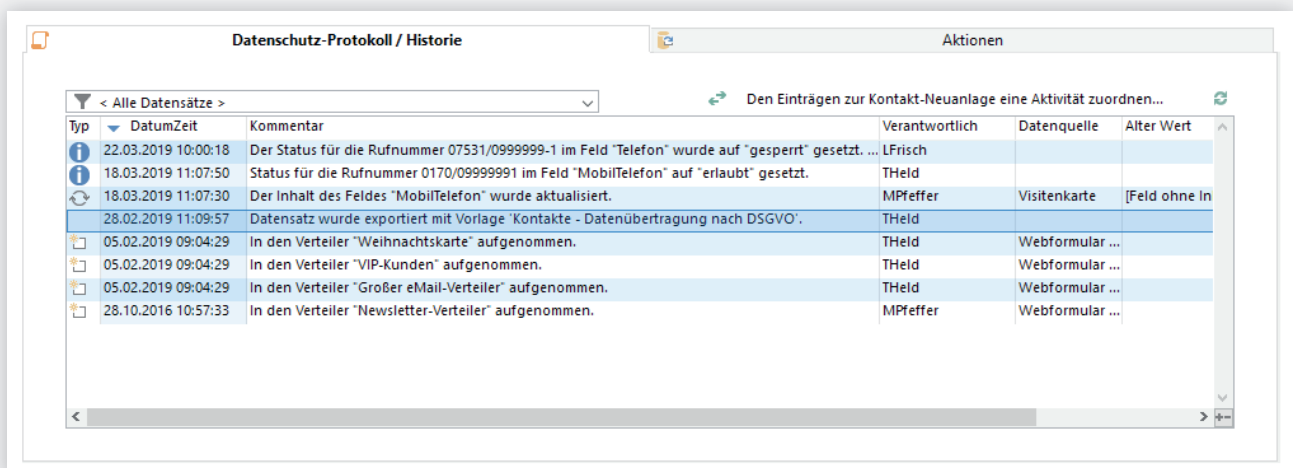
Die Auto-Protokoll-Funktion im cRM war schon immer ein starkes und bei unseren Kunden beliebtes Feature. Damit können Sie selbst beliebige Auto-Protokoll-Aufgaben im cRM definieren und frei über die Oberfläche einstellen.

Die definierten Auto-Protokolle lösen dann bei den gewünschten Aktionen aus und legen z. B. automatisch im Hintergrund einen Protokolleintrag oder eine Aktivität bei jedem betroffenen Datensatz an. Besonders wichtige Aktionen im Hinblick auf das Auto-Protokoll sind z. B. „Datensatz wurde exportiert“ und möglicherweise auch „Datensatz wurde gedruckt“.

Diese typischen Fälle haben wir in unserer Lösung bereits als Muster für Sie vorkonfiguriert. Sie können diese 1:1 in Ihre Lösung übernehmen oder auch nur als Basis für Ihre eigenen, individuellen Auto-Protokolle heranziehen.



Sinnvolle Autoprotokoll-Einstellungen sind bereits konfiguriert.



Autoprotokolle ergänzen das Datenschutz-Protokoll für eine lückenlose Nachvollziehbarkeit des Datenflusses.

Daten schützen

Weshalb?

Daten sind für Ihr Unternehmen, aber auch für die betroffenen Personen, ein sehr wertvolles Gut. Für sehr viele unserer Kunden sind sie die entscheidende Grundlage für ihren Unternehmenserfolg. Schon allein deshalb lohnt es sich, diese Daten zu schützen. Aber auch der Gesetzgeber erwartet von Ihnen, dass Sie geeignete technisch-organisatorische Maßnahmen ergreifen, um personenbezogene Daten adäquat vor Missbrauch, Diebstahl, Verlust und unautorisiertem Zugriff zu schützen. (Rechtsgrundlage: u.a. [Art. 32 DSGVO](#) und [Art. 5 DSGVO](#))

Lösung combit CRM:

Die combit CRM Software ist als „on premise“ Lösung schon einmal grundsätzlich eine Lösung, die Datenschützer lieben: Denn sie zwingt Sie nicht in eine Cloud, bei der Sie nicht wissen, wo genau auf der Welt der Server steht, sondern gibt Ihnen die Möglichkeit, sie auf eigener Hardware zu betreiben.

Sie müssen also nicht zwingend überprüfen, inwiefern der Cloud Anbieter DSGVO-konform arbeitet oder einen Auftragsverarbeitungsvertrag (AVV) mit einem Cloud Anbieter abschließen. Allein Sie selbst haben die komplette Hoheit über Ihre Kundendaten.

Für etwaige Verschlüsselungsroutinen kommt die im Windows-Betriebssystem integrierte Microsoft Kryptographie-Plattform „Cryptography API: Next Generation (CNG)“ zum Einsatz.

Zugriff autorisieren

Weshalb?

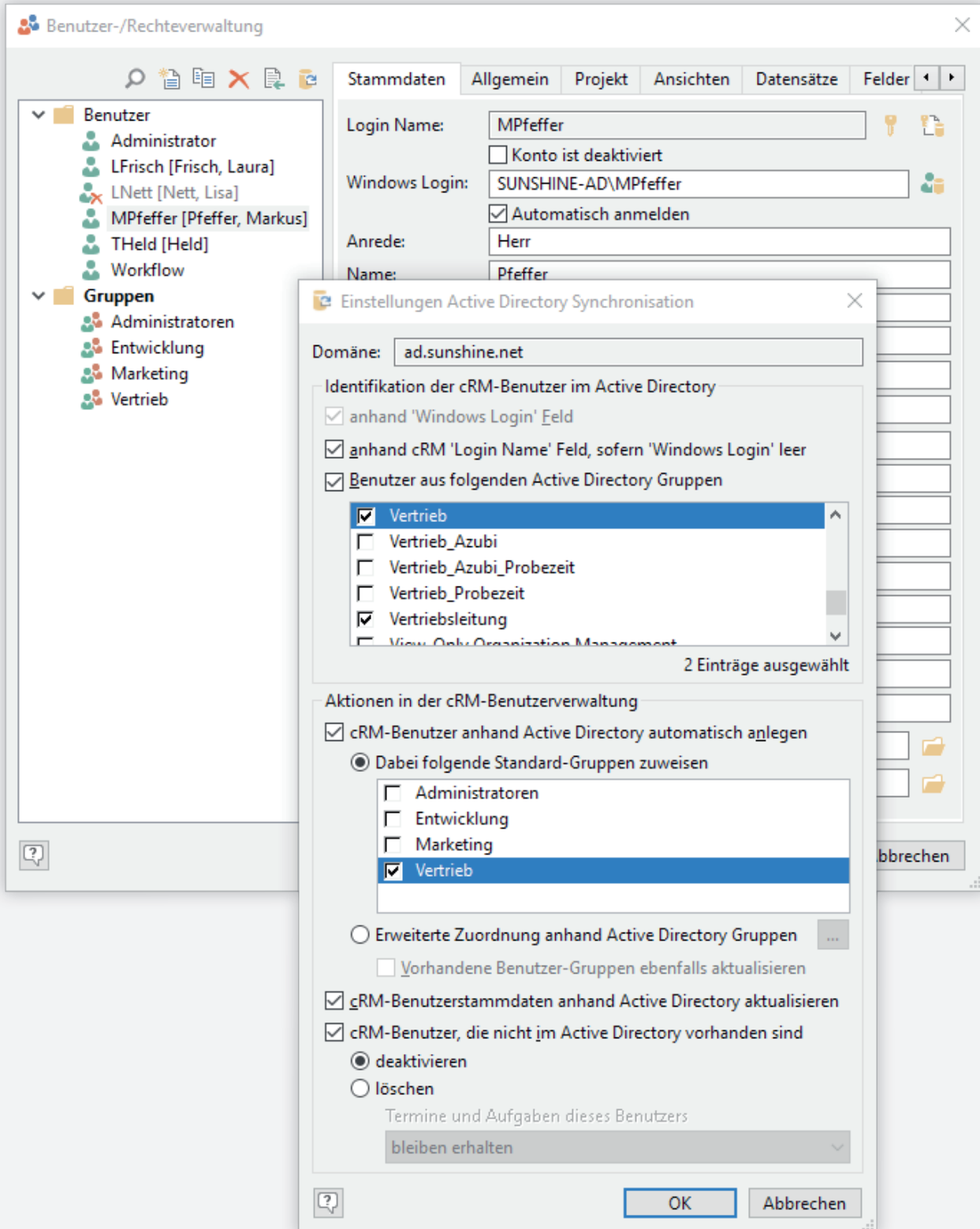
Die CRM-Lösung ist bei vielen Unternehmen ein wichtiges und sehr zentrales System, das es vor unbefugtem Zugriff zu schützen gilt. Sie müssen deshalb dafür sorgen, dass nur autorisierte Personen Zugriff darauf haben. (Rechtsgrundlage: u.a. [Art. 32 DSGVO](#) und [Art. 5 DSGVO](#))

Lösung combit CRM:

Unsere Software schützt auf verschiedenen Wegen vor unbefugtem Zugriff. Besonders wichtig ist natürlich, dass Sie sicherstellen, dass für jeden Benutzer in der Software ein Kennwort vergeben wurde.

Außerdem ist die Aktivierung der Anmeldung über die Windows-Authentifizierung empfehlenswert (Single-Sign-On) und spart bei hoher Sicherheit jeden Tag Ihren Mitarbeitern wertvolle Zeit. Die Benutzerverwaltung kann automatisch mit dem Active Directory Ihrer Domäne synchronisiert werden (ab Enterprise Edition). Hier ist auch die Zuordnung von Gruppen im combit Relationship Manager zu Domänen-Benutzergruppen möglich.

Nicht vergessen: Benutzerkonten von ausgeschiedenen Mitarbeitern unbedingt deaktivieren!



Zugriffskontrolle über eine ausgeklügelte Benutzerverwaltung inklusive Active Directory Anbindung.

Daten einschränken

Weshalb?

Um das Risiko für einen Datenmissbrauch zu reduzieren, fordert das Datenschutzgesetz, dass der Zugriff auf personenbezogene Daten nur dem Mitarbeiterkreis zugänglich gemacht werden darf, für die der Zugriff darauf für ihre Arbeit unbedingt erforderlich ist. (Rechtsgrundlage: u.a. [Art. 32 DSGVO](#) und [Art. 25 DSGVO](#))

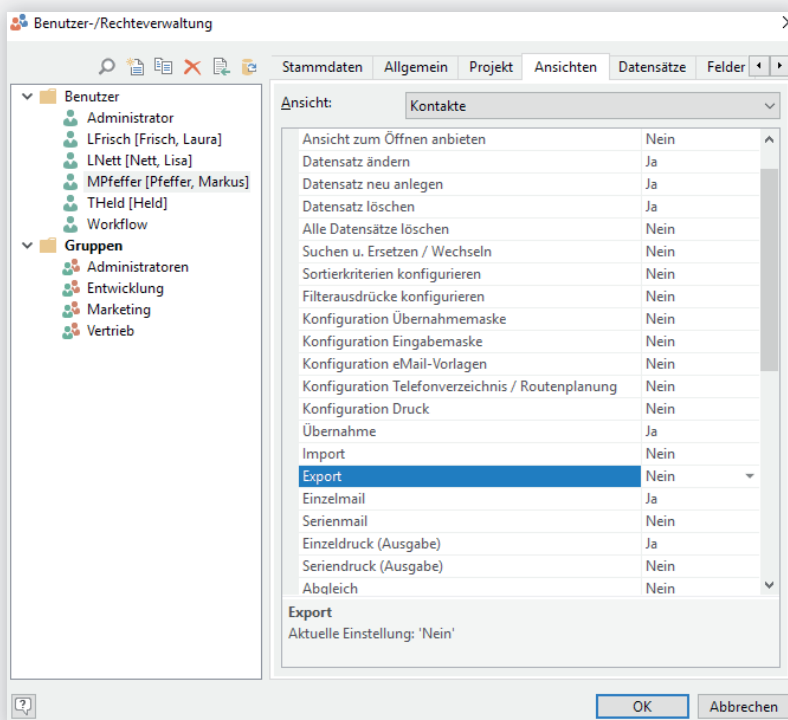
Lösung combit CRM:

Der combit Relationship Manager hat eine sehr ausgeklügelte und granulare Benutzerverwaltung. Sie haben hier die Möglichkeit, für einzelne Benutzer oder ganze Gruppen u. a. das Folgende freizugeben oder zu ganz zu sperren:

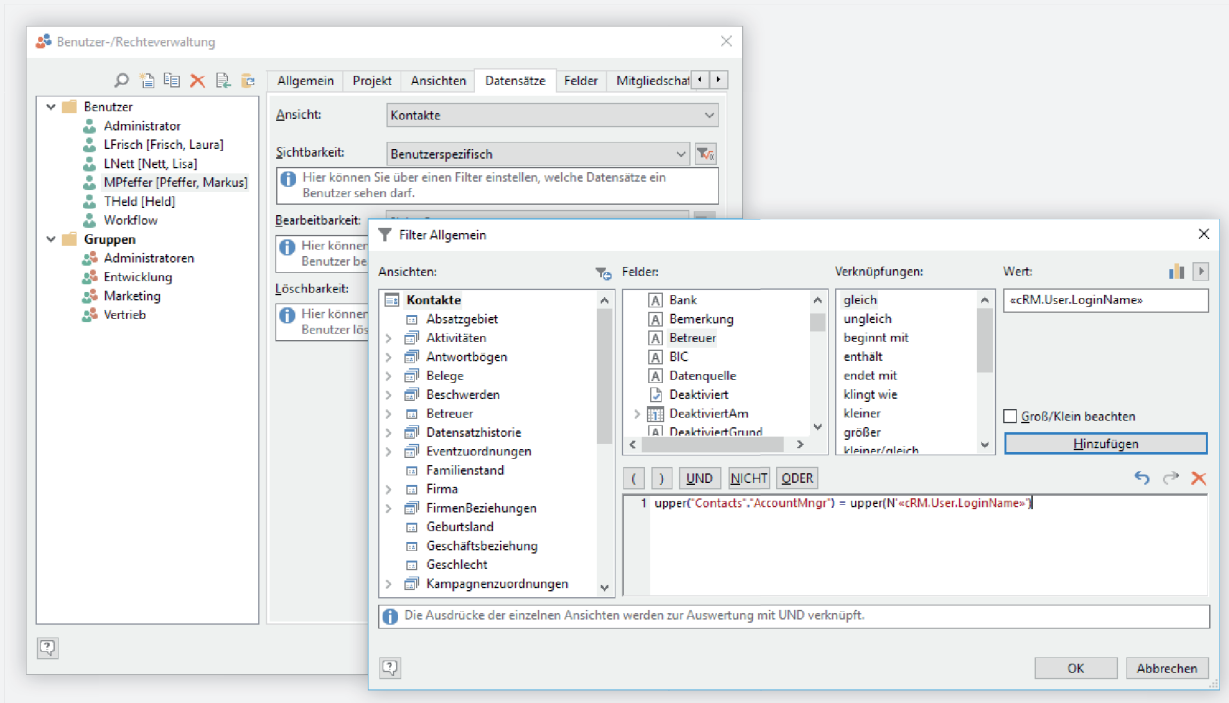
- Zentrale Funktionen der Software.
- Funktionen ganz individuell und frei pro Ansicht.
- Individuell die Sichtbarkeit, Bearbeitbarkeit und Löschbarkeit bestimmter Datensätze (z. B. nur der Vertrieb darf Interessenten-Datensätze überhaupt sehen. Nur der zuständige Betreuer darf diese Datensätze auch bearbeiten. Und ausschließlich die Geschäftsführung darf diese Datensätze löschen.)
- Sogar einzelne Felder – ebenfalls völlig frei und ganz individuell (z. B. das Feld mit der Bonität ist nur für die Geschäftsführung, die Buchhaltung und den Vertrieb sichtbar).

Schränken Sie also, wo sinnvoll, den Zugriff auf Ansichten, Datensätze oder sogar einzelne Felder auf bestimmte Gruppen oder gar Einzelpersonen ein.

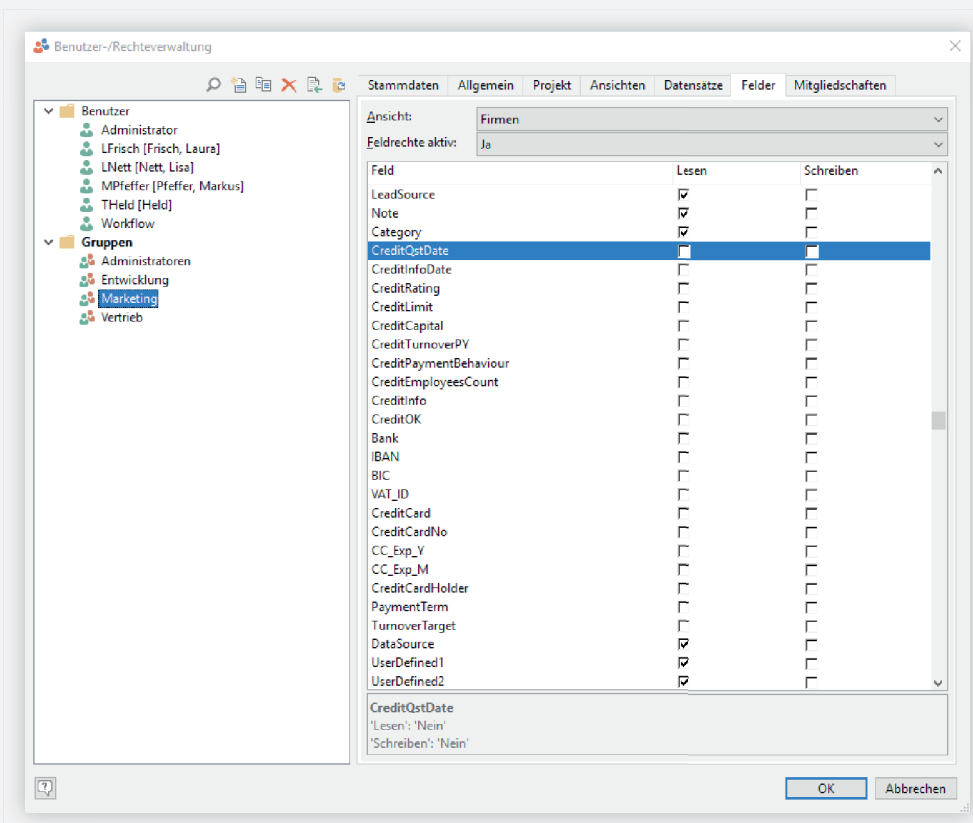
Die Benutzerverwaltung ist nicht nur ein unverzichtbares Instrument für den Datenschutz. Sie ermöglicht auch, dass jeder Benutzer seine „eigene“ Software hat, die perfekt auf die individuellen Bedürfnisse abgestimmt ist. Jeder Benutzer sieht nur die für die eigene Arbeit wichtigen Bereiche und Datensätze. Dies verringert die Komplexität der Software, schafft Klarheit, reduziert den Schulungsaufwand und sorgt für Akzeptanz, weil das Arbeiten mit der Software Freude macht.



Autorisieren Sie einzelne Mitarbeiter oder Teams nur für bestimmte Tätigkeiten.



Sichtbarkeit von Datensätzen auf den jeweiligen Betreuer einschränken.



Anwendungskreis auf das erforderliche Mindestmaß einschränken.

Daten sichern

Weshalb?

Daten sind wertvoll! Ein Verlust schmerzt oft nicht nur, sondern kann die Existenz eines Unternehmens gefährden. Aber nicht nur in eigenem Interesse sollten Sie sich um eine Datensicherung mit viel Engagement kümmern. Denn auch gemäß Datenschutzgesetz sind Sie verantwortlich für die Integrität der Daten. Dies schließt auch die schnelle Wiederherstellbarkeit bei Verlust/Beschädigung der Daten mit ein (Rechtsgrundlage: u.a. Art. 32 Abs. 1 und Abs. 2 DSGVO).

Wie?

Unverzichtbar ist ein Sicherungskonzept, in dem Datenbanken und alle anderen Dateien, die Bestandteil der CRM-Lösung sind, eingeschlossen sind. Diese Datensicherung muss regelmäßig durchgeführt werden, idealerweise automatisiert. Ganz wichtig ist in diesem Zusammenhang auch die Prüfung dieser Sicherungen. Sie müssen und sollten regelmäßig prüfen: Funktioniert im Notfall auch meine regelmäßige Sicherung?

Lösung combit CRM:

Der CRM unterstützt Sie aktiv beim Erstellen einer Sicherung Ihrer Daten. Mit dem Assistenten zum Sichern und Wiederherstellen kann direkt aus der Programmoberfläche heraus eine vollständige Sicherung der Projekt- und System-Datenbanken und des gesamten Projektverzeichnisses mit allen Unterordnern und Dateien angefertigt werden. Weitere Ordner können Sie einfach hinzufügen. Die Datensicherung kann auch über die Windows-Aufgabenplanung durchgeführt werden sodass regelmäßige automatische Sicherungen erstellt werden. Bei einer späteren Wiederherstellung können die zu wiederherstellenden Projektbestandteile einzeln ausgewählt werden. Auch technisch weniger versierte Anwender können schnell und auf einfache Art und Weise eine Datensicherung durchführen, sofern sie dazu die Berechtigung erteilt bekommen haben.

Unser Tipp – nicht nur im Hinblick auf den CRM:

Behalten Sie dieses Thema fortlaufend im Auge. Überprüfen Sie regelmäßig das, was Sie sichern. Simulieren Sie den Notfall! Hinterfragen Sie sich selbst-kritisch: Habe ich bei der Sicherung nichts vergessen? Ziehen Sie im Zweifel gut ausgebildete Experten hinzu. Sorgen Sie so für ein Höchstmaß an Sicherheit!



Der Sicherungsassistent erleichtert Systemadministratoren die Arbeit.

Datenbank verschlüsseln

Weshalb?

Auch Daten können gestohlen werden. Der Gesetzgeber fordert deshalb, dass Ihre Daten gegen Diebstahl technisch adäquat geschützt sind und Sie angemessene Schutzmaßnahmen im Sinne der „Datenträgerkontrolle“ ergreifen. (Rechtsgrundlage: u.a. Art. 32 Abs. 1 lit. a und lit. b DSGVO)

Wie?

Neben technischen und organisatorischen Maßnahmen, die den Zugang zu den Datenbankdateien wirksam verhindern, können Sie z. B. beim Microsoft SQL Server die Datenbank zusätzlich physikalisch verschlüsseln. Dadurch sind selbst bei einem Diebstahl der Datenbankdateien die Daten darin weiterhin wirksam geschützt. Eine Anleitung zur Aktivierung der Verschlüsselung mit combit CRM finden Sie in unserer Knowledgebase.

Löschfristen einhalten

Weshalb?

Aus vielen Gründen ist es sinnvoll, dass personenbezogene Daten nicht „für immer“ in einem CRM-System vorgehalten werden. Aber auch die datenschutzrechtlichen Vorgaben sehen vor, dass personenbezogene Daten gelöscht werden müssen, wenn der Zweck ihrer Verwendung erfüllt ist. Ebenso müssen diese Daten gelöscht werden, wenn die betroffene Person dies verlangt. (Rechtsgrundlage: u.a. Art. 17 DSGVO)

Wie?

Für personenbezogene Daten muss ein Löschkonzept im CRM-System implementiert werden. Machen Sie sich dazu folgende Gedanken: Wann soll/muss ein Datensatz aus meinem CRM-System entfernt werden?

Der Gesetzgeber gibt Ihnen hier Orientierung: Zum einen werden die gesetzlichen Aufbewahrungsfristen relevant, zum anderen der konkrete Verwendungszweck der erfassten Daten.

Typische Löschrufen können in der Praxis sein:

- 10 Jahre nach Ende der Kundenbeziehung.
- 2 Jahre nach dem letzten persönlichen Kontakt (sofern längere gesetzliche Aufbewahrungsfristen dem nicht entgegenstehen).
- 6 Jahre nach Erfassung.
- etc.

Beachten Sie, dass es für manche Verarbeitungstätigkeiten keine vom Gesetzgeber festgelegte Löschrufe gibt, sondern sich diese im Zweifel erst noch durch die Rechtsprechung ergeben werden. Im Zweifel: Lassen Sie sich von Ihrem Anwalt im Hinblick auf Ihren individuellen Fall umfassend beraten.

Lösung combit CRM:

Selbst hochkomplexe Löschkonzepte, die Ihnen Ihr Anwalt empfiehlt, rauben Ihnen nicht den Schlaf. Denn in unserer Lösung lässt sich zu Ihren eigenen Verarbeitungstätigkeiten direkt eine frei definierbare Löschrufe hinterlegen – dies frei einstellbar über unseren mächtigen Filter-Assistenten.

Einmal eingestellt, erledigt der Filter-Assistent für Sie den Rest: Er filtert für Sie im Zusammenhang mit Ihrer individuellen Geschäftstätigkeit die Datensätze heraus, deren Frist zur Aufbewahrung überschritten ist. Natürlich können Sie vor dem endgültigen Löschen noch einmal übersichtlich prüfen, was konkret gelöscht wird.

Das DSGVO Center im combit CRM sorgt hier zusätzlich für mehr Übersicht, selbst beim Erstellen konkurrierender Löschräume mit verschiedenen Löschfristen. Typischerweise führen Sie dann spätestens einmal jährlich die Löschräume aus.

Die Löschfunktion unserer CRM-Lösung ist gründlich und entfernt die Datensätze nach Prüfung tatsächlich unwiderruflich in der Datenbank.

Darüber hinaus werden auch Löschfristen auf Feld-Ebene unterstützt: Bei der Erfassung eines personenbezogenen Feldes wird ein Verarbeitungszweck angegeben (siehe Kapitel „Datenherkunft + Verwendungszweck vermerken“), der wiederum mit einer Löschfrist verknüpft ist.

Auch hier profitieren Sie von unseren intelligenten Erfassungsmöglichkeiten im Hinblick auf den Datenschutz: Im combit DSGVO Center können Sie nun eine sog. „geordnete Löschung“ von Feldinhalten durchführen. Hierbei wird das komplette Datenschutz-Protokoll durchlaufen und Felder, deren Aufbewahrungsfrist verstrichen ist, werden geleert. Ein vorher erforderlicher Testlauf simuliert die Löschung, so dass Sie prüfen können, welche Felder welcher Datensätze tatsächlich betroffen sind. Erst danach kann der abschließende „Echtlauf“ durchgeführt werden.

Ansichtsname	Löschfrist.Titel	Löschfrist.Beschreibung
Kontakte	10 Jahre nach letztem Kauf	Gelöscht wird ein Kontakt oder ein Feldinhalt in diesem Fall immer dann, wenn dort 10 Jahre keine Belege vom Typ Auftrag, Lieferschein oder Rechnung (aufbewahrungspflichtige Geschäftsunterlagen i.S.d. HGB bzw. buchungsrelevante Daten) mehr hinterlegt wurden oder Kontakt gar keine Belege zugeordnet sind.
Kontakte	10 Jahre nach letzter Interaktion	Gelöscht wird ein Kontakt oder ein Feldinhalt in diesem Fall immer dann, wenn dort 10 Jahre (universelle Löschfrist) keine Aktivitäten mehr hinterlegt wurden oder dem Kontakt gar keine Aktivitäten zugeordnet sind.
Kontakte	2 Jahre nach letzter Verteiler-Aussendung	Gelöscht wird ein Kontakt oder ein Feldinhalt in diesem Fall immer dann, wenn dort 2 Jahre lang keine Verteiler vom Typ "Einmalige Aussendung" durchgeführt wurde oder dem Kontakt gar keine Verteiler zugeordnet sind.
Verteilerzuordnungen	Aus Verteiler entfernen 2 Jahre nach letzter Verteiler-Aussendung	Ein Kontakt wird aus allen Verteilern vom Typ "eMail-Verteiler" entfernt, wenn er 2 Jahre lang kein Teilnehmer eines Verteilers vom Typ "Einmalige Aussendung" war.

Verschaffen Sie sich einen Überblick darüber, welche Daten als nächstes gelöscht werden müssen.

Verarbeitungstätigkeiten

Hier können Sie die Verarbeitungstätigkeiten für die DSGVO definieren

Inhalt	Datensatz-Informationen
Titel Kundendatenverwaltung Zweck Verwaltung von Kundendaten IT-System combit CRM Betroffene Kunden Interessenten Lieferanten Dienstleister Datenkategorien <bitte ausfüllen> Beispiel: Name, Adresse, E-Mail, Telefon, Bankverbindung <input type="checkbox"/> Besondere Kategorie Datenherkunft <bitte ausfüllen> Beispiel: Direkterhebung (z.B. E-Mail, Kontaktformular) Rechtsgrundlage Vertragserfüllung (Art. 6 Abs.1 b) DSGVO Zugriffsberechtigte Vertrieb Marketing Service IT-Abteilung Datenschutzbeauftragter Sonstiges DIE ANGABEN STELLEN LEDIGLICH BEISPIELE DAR UND MÜSSEN FÜR IHR UNTERNEHMEN KONKRET AUSGEFÜLLT WERDEN!	Verarbeitung durch Dritte nein Übermittlung an Drittstaaten nein Auftragsverarbeitungsvertrag nein TOM <input checked="" type="checkbox"/> Datenminimierung <input checked="" type="checkbox"/> Prozessdokumentation vorhanden Informiert mittels <bitte ausfüllen> Beispiel: Datenschutzerklärung Website <input checked="" type="checkbox"/> Datenübertragbarkeit Löschfrist 10 Jahre nach letztem Kauf Hinweis Bitte beachten Sie, dass diese Verarbeitungstätigkeit nur für die Ansicht 'kontakte' zur Verfügung steht, die in der ausgewählten Löschfrist festgelegt wurde. Duplizieren Sie die Verarbeitungstätigkeit ggf. und wählen eine andere Löschfrist, um diese auch in anderen Ansichten verwenden zu können. Risikoabschätzung gering Folgenabschätzung nicht notwendig eMail-Opt-in für Newsletterverwaltung <input type="checkbox"/> Diese Verarbeitungstätigkeit für die Newsletterverwaltung verwenden. Hinweis: Es sollte nur eine Verarbeitungstätigkeit für das eMail-Opt-in-Verfahren der Newsletterverwaltung aktiviert werden.

Definieren Sie individuelle Verarbeitungstätigkeiten.

Automatisches Bereinigen von Feldinhalten in Ihrem System

Hier können Sie in allen relevanten Datensätzen personenbezogene Daten gemäß Ihren Einstellungen löschen

Testlauf
Echtlauf

Ein Testlauf wurde --- erfolgreich --- von Benutzer 'Administrator' durchgeführt. --- Start Datum/Zeit: 22.03.2019 - 10:39:47

22.03.2019 - 10:39:43: Ein Feldinhalt steht zur Löschung an:
 Ansicht: Kontakte
 Datensatz: [combit GmbH, Björn Florian Eggstein](#)
 Feld: eMail
 zu löschender Wert: eggstein@combit.net

22.03.2019 - 10:39:45: Ein Feldinhalt steht zur Löschung an:
 Ansicht: Kontakte
 Datensatz: [combit GmbH, Jochen Bartlau](#)
 Feld: Telefon
 zu löschender Wert: 07531/9060-10

Testlauf starten...
Löschvorgang starten (Testlauf)...

Verpassen Sie nicht „abgelaufene“ Daten zu löschen.

Auskünfte erteilen

Weshalb?

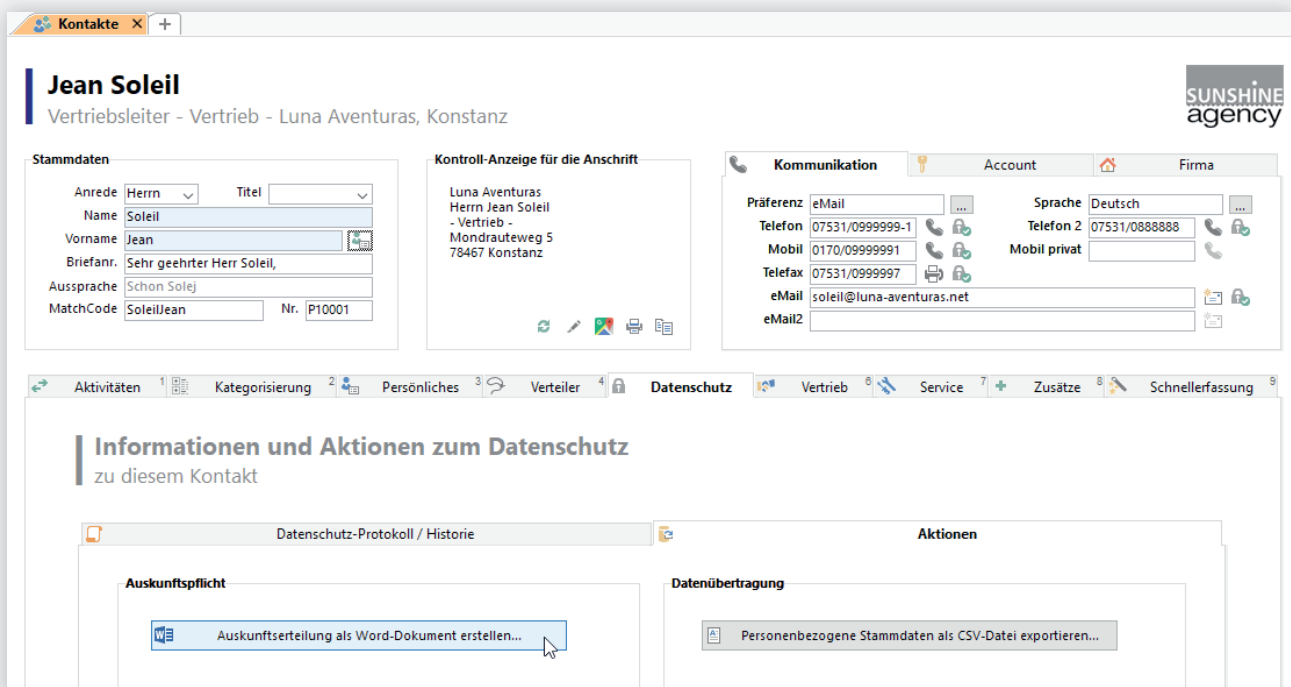
Personen, deren Daten Sie speichern, steht ein gesetzliches Auskunftsrecht zu, zu erfahren, welche Daten über sie gespeichert sind. Die gesetzlich vorgegebene Frist, innerhalb derer Sie dem Antrag auf Erteilung dieser Auskunft nachkommen müssen, lautet zunächst „unmittelbar“, spätestens jedoch 1 Monat nach Antragseingang, in komplexen Fällen lässt sich diese Frist um 2 Monate verlängern. (Rechtsgrundlage: u.a. [Art. 15 DSGVO](#) für die Frist u.a. [Art. 12 DSGVO](#))

Wie?

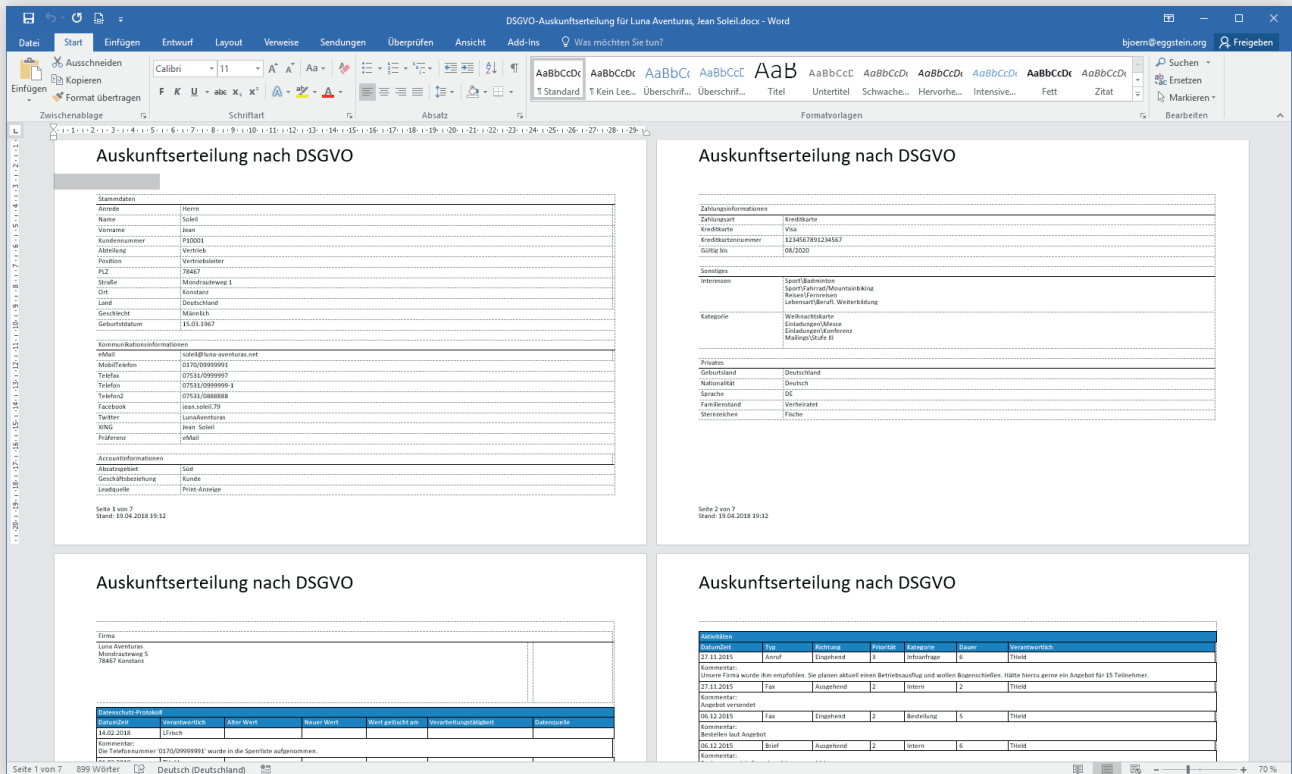
Sie sind also gut beraten, auf eine Berichtsvorlage zugreifen zu können, die alle Daten zum betroffenen Kontakt aufführt. Die Vorlage sollte auch etwaige Relationen zu anderen Ansichten, wie z. B. Verkaufschancen, Verteiler-/Kampagnenzugehörigkeiten, Eventteilnahmen etc. einschließen. Wenn die Daten an Dritte weitergegeben wurden, z. B. von einem Dienstleister/Vertriebspartner o.ä., so muss dies aus dem Auskunftsdocument ebenfalls mit hervorgehen (vgl. Kapitel „Aktionen protokollieren“).

Lösung combit CRM:

Die gute Nachricht: Selbst hier müssen Sie nicht bei Null anfangen. Wir stellen Ihnen eine entsprechende Vorlage bereit, auf die Sie aufbauen können. Mit einem einfachen Klick erstellen Sie für jeden Kontakt ein Word-Dokument, das die zum Kontakt gespeicherten Informationen enthält. Dieser Bericht kann im Druckvorlagendesigner von Ihnen selbst völlig frei angepasst und erweitert werden, abhängig davon, wie bei Ihnen im Unternehmen die Kundendaten-Ablage in Ihrer individuellen CRM-Lösung realisiert wurde. Vor dem Versand lässt sich das Dokument noch individuell bearbeiten. So stellen Sie z. B. sicher, dass keine Rechte Dritter verletzt werden. Zu diesem Zweck ist es auch möglich, einzelne Datensätze, wie z.B. eine Aktivität, für die Auskunftserteilung zu sperren, die dann von vorneherein nicht in das Word-Dokument übernommen werden.



Ein vorgefertigter Bericht als Word-Dokument kann per Knopfdruck ausgegeben werden.



Auskunftserteilung nach DSGVO als Word-Dokument.

Daten übertragen

Weshalb?

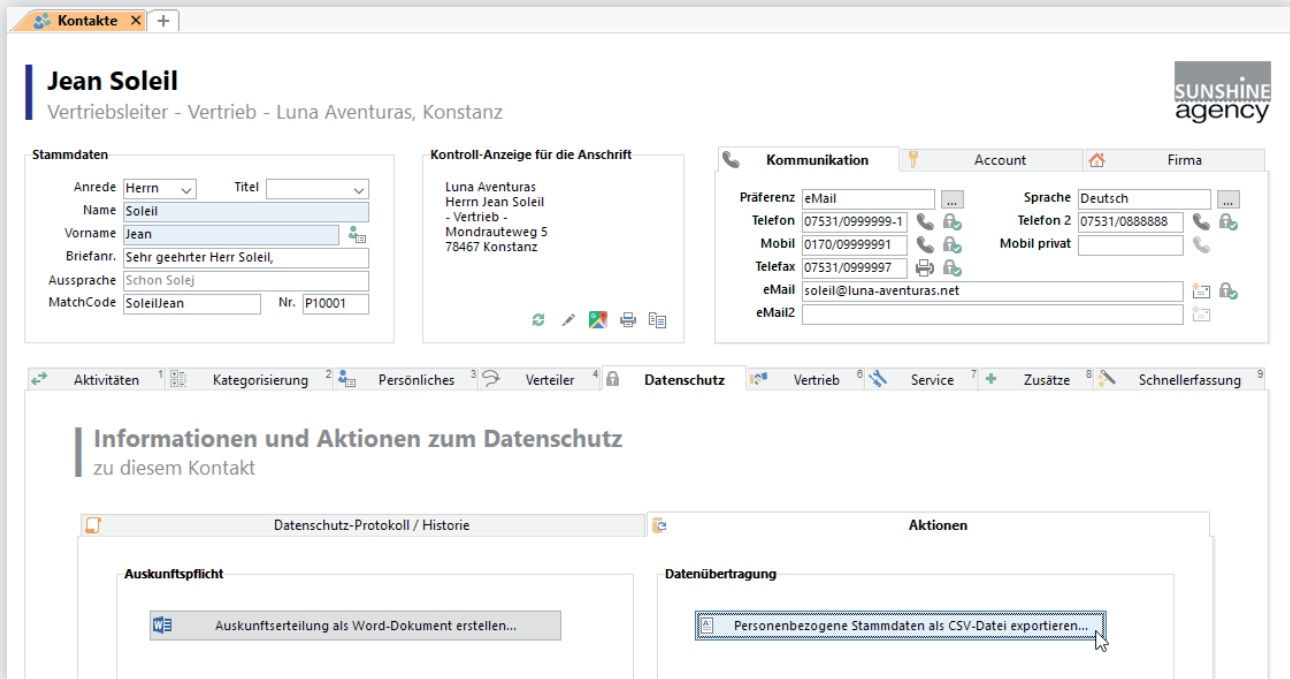
Es kann vorkommen, dass Personen die Daten, die sich in Ihrem System befinden, auf elektronischem Weg „mitnehmen“ möchten. Diese Personen haben nun die Möglichkeit von Ihnen zu verlangen, dass die von Ihnen zur Verfügung gestellten Daten in einer gängigen, elektronischen Form an Dritte übertragen werden können. (Rechtsgrundlage: u.a. [Art. 20 DSGVO](#))

Wie?

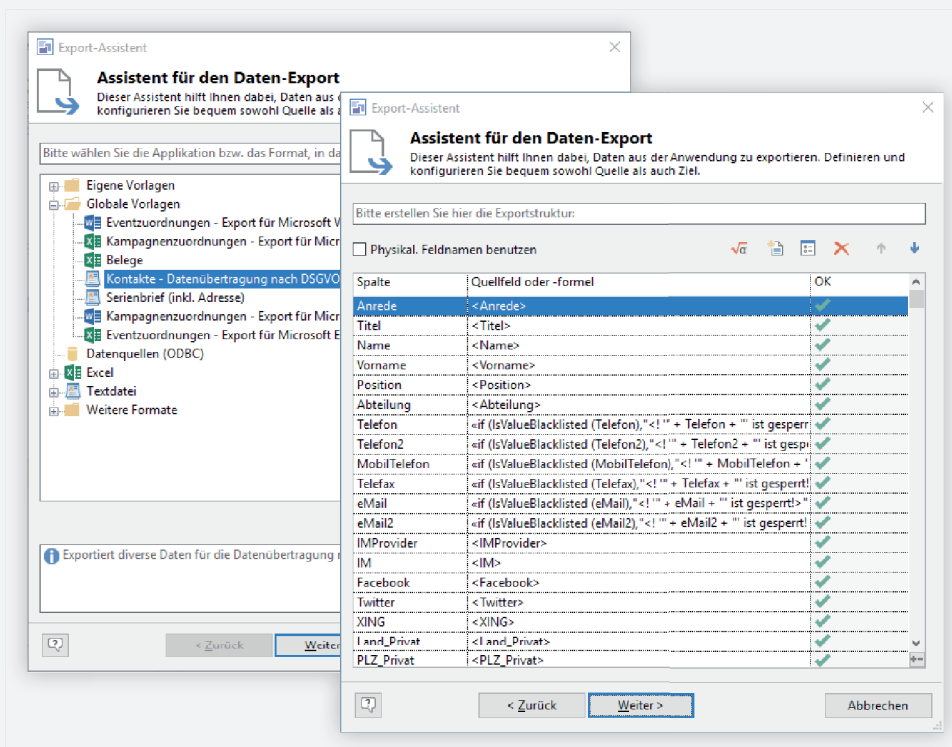
Definieren Sie eine möglichst standardisierte Export-Vorlage, mit der Sie bestimmte Stammdaten-Felder des Kontaktes zum Beispiel in eine CSV-Datei exportieren. Wir empfehlen zur Vereinfachung dieses Prozesses auf die Ermittlung der genauen Datenfelder zu verzichten, die die Person Ihnen im konkreten Einzelfall tatsächlich seinerzeit überlassen hat. Diesen Aufwand können Sie sich sparen, indem Sie immer denselben typischen Grundstock an Daten exportieren (der diese natürlich enthalten muss).

Lösung combit CRM:

Auch hier werden Sie von der combit CRM Software unterstützt: Mit einem simplen Klick auf die entsprechende Schaltfläche wird direkt eine in der Exportvorlage hinterlegte Auswahl an Stammdaten-Feldern für den aktuellen Kontakt als CSV-Datei erzeugt. Machen Sie die DSGVO-Standard-Export-Vorlage zu Ihrer eigenen Export-Vorlage. Sie können diese Vorlage entweder 1:1 zu verwenden oder an Ihre individuellen Felder anpassen.



Für die Datenübertragung generieren Sie per Knopfdruck eine CSV-Datei.



Passen Sie die CSV-Datei für die Datenübertragung an Ihre Anforderungen an.

Sie haben Fragen zur DSGVO in der combit CRM Software?

Zur technischen Implementierung in Ihre ggf. vorhandene Lösung wird es im Mai 2018 ein eigenes Whitepaper geben. Außerdem können Sie sich durch unser Experten-Team bei der technischen Implementierung in Ihre eigene CRM-Lösung kostenpflichtig unterstützen lassen.

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

Weitere Informationen, auch für Einsteiger, finden Sie auf unserer Website.

www.combit.net/crm-software/datenschutz/

Disclaimer

Dieses Whitepaper kann nicht als rechtliche Beratung für Ihr Unternehmen dienen, auf das Sie sich bei der Einhaltung der Datenschutzgesetze der EU z. B. bei der Einhaltung der DSGVO und dem BDSG-neu, stützen können. Wir weisen Sie deshalb darauf hin, dass Sie bei rechtssicherem Beratungsbedarf über die Ausgestaltung Ihrer Geschäftsprozesse, z. B. im Hinblick auf den Datenschutz, einen Anwalt hinzuziehen sollten.

