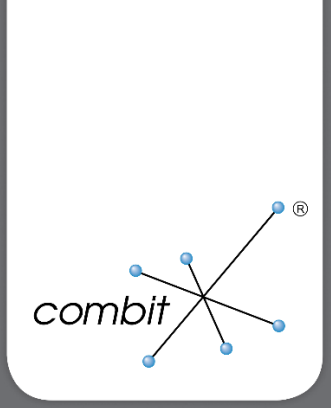


Whitepaper

combit Relationship Manager 10

Whitepaper - Datenschutz Integration in Solution

Inhalt

Einleitung

Dieses Whitepaper zeigt Ihnen, wie Sie wesentliche, für Sie schlüsselfertig vorbereitete, Funktionalitäten zur EU-DSGVO in Ihre eigene, individuelle und bereits bestehende combit CRM Lösung integrieren können. Das Whitepaper richtet sich also nur an Kunden, die den combit Relationship Manager bereits im Einsatz haben.

Wenn Sie Unterstützung bei der Implementierung wünschen: Rufen Sie uns an! Unser Experten-Team unterstützt Sie aktiv bei der technischen Implementierung in Ihre eigene CRM-Lösung – bei einer Abrechnung fair nach Aufwand und minutengenau.

Zur Integration der DSGVO-Funktionen steht Ihnen ein eigenes Projekt "Large_DSGVO" zur Verfügung. Dieses Projekt können Sie verwenden, um die einzelnen Bestandteile in Ihre bestehende Solution zu übernehmen.

Bitte beachten: Die Integration kann nur in den combit Relationship Manager 10 oder höher erfolgen! Außerdem wird in dieser Anleitung nur speziell auf den Microsoft SQL Server 2008-2017 eingegangen.

Bitte lesen Sie zum besseren Verständnis der implementierten Funktionen auch das Profi-Whitepaper "Datenschutz in combit CRM - Die DSGVO und Ihre CRM Software". Außerdem erklärt unser Start-Whitepaper "Fit im Datenschutz" die wichtigsten Neuerungen der EU-Datenschutz-Grundverordnung (EU-DSGVO) und liefert Checklisten für Bestandsaufnahme und erste Maßnahmen. Sie finden beide Whitepaper auf unserer combit CRM Datenschutz Seite unter https://www.combit.net/crm-software/datenschutz/.

Installation der DSGVO-Solution

Datensicherung

Mit dem Assistenten für die Sicherung und Wiederherstellung sollten Sie eine Sicherung Ihres aktuellen Projekts, der Projektdatenbank und der Systemdatenbank durchführen. Dabei wird das gesamte Projektverzeichnis gesichert. Die Sicherungen werden als zip-Archiv gespeichert.

1. Den Assistenten starten Sie über "**DATEI > Information > Sichern und Wiederherstellen"**.
2. Wählen Sie "Konfiguration" um den Sicherungsvorgang einzurichten.
3. Geben Sie die Verbindungsdaten für den Datenbankserver an, verwenden Sie die Option "Aktuelle Verbindungsdaten des combit Relationship Manager verwenden".
4. Alle weiteren Informationen zur Sicherung finden Sie im combit Relationship Manager Handbuch im Kapitel "Datensicherung und Wiederherstellung".
5. Überprüfen Sie anschließend die Sicherung.

Wichtig: Heben Sie diese Datensicherung – dauerhaft! – auf, damit Sie auch später noch in der Lage sind, etwaige übersehene eigene Änderungen nachziehen zu können.

DSGVO-Projekt vorbereiten

Das DSGVO-Projekt zur Integration finden Sie in unserer Knowledgebase unter https://www.combit.net/kb/KBAD001351

Entpacken Sie das dort enthaltene zip-Archiv "combit_Large_DSGVO_Integration.zip". Benennen Sie den entpackten Ordner um in "Large_DSGVO".

Kopieren Sie nun den entpackten Ordner in Ihr Solution-Verzeichnis. Standardmäßig ist dies auf dem Server(!) unter C:\Program Files (x86)\combit\cRM\Solutions zu finden.

Wichtig: Das DSGVO-Projekt aus dem zip-Archiv ist nur für den Projekt-Import in Ihre eigene Solution vorgesehen und sollte daher nicht direkt geöffnet werden.

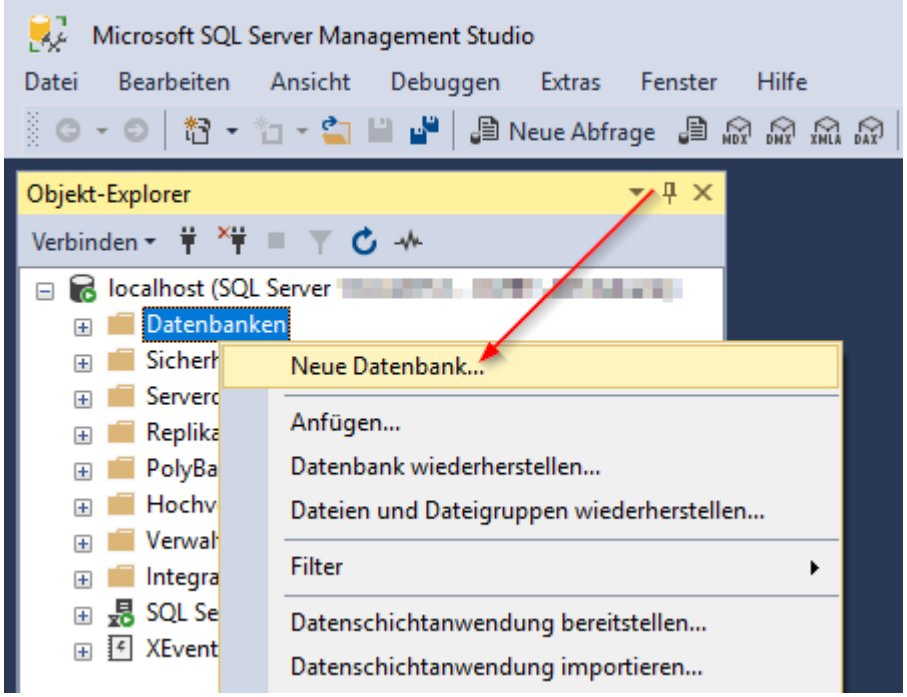
DSGVO-Datenbank einspielen

Nun müssen Sie die Datenbank mit den neuen DSGVO-Funktionen auf Ihrem Datenbank-Server bereitstellen. Hierzu benötigen Sie das Microsoft SQL Server Management Studio, das Sie in der Regel auf Ihrem Server im Programmverzeichnis finden. Sie können das Microsoft SQL Server Management Studio auch über folgenden Link in unserer Knowledgebase herunterladen: https://www.combit.net/kb/KBAD001332.

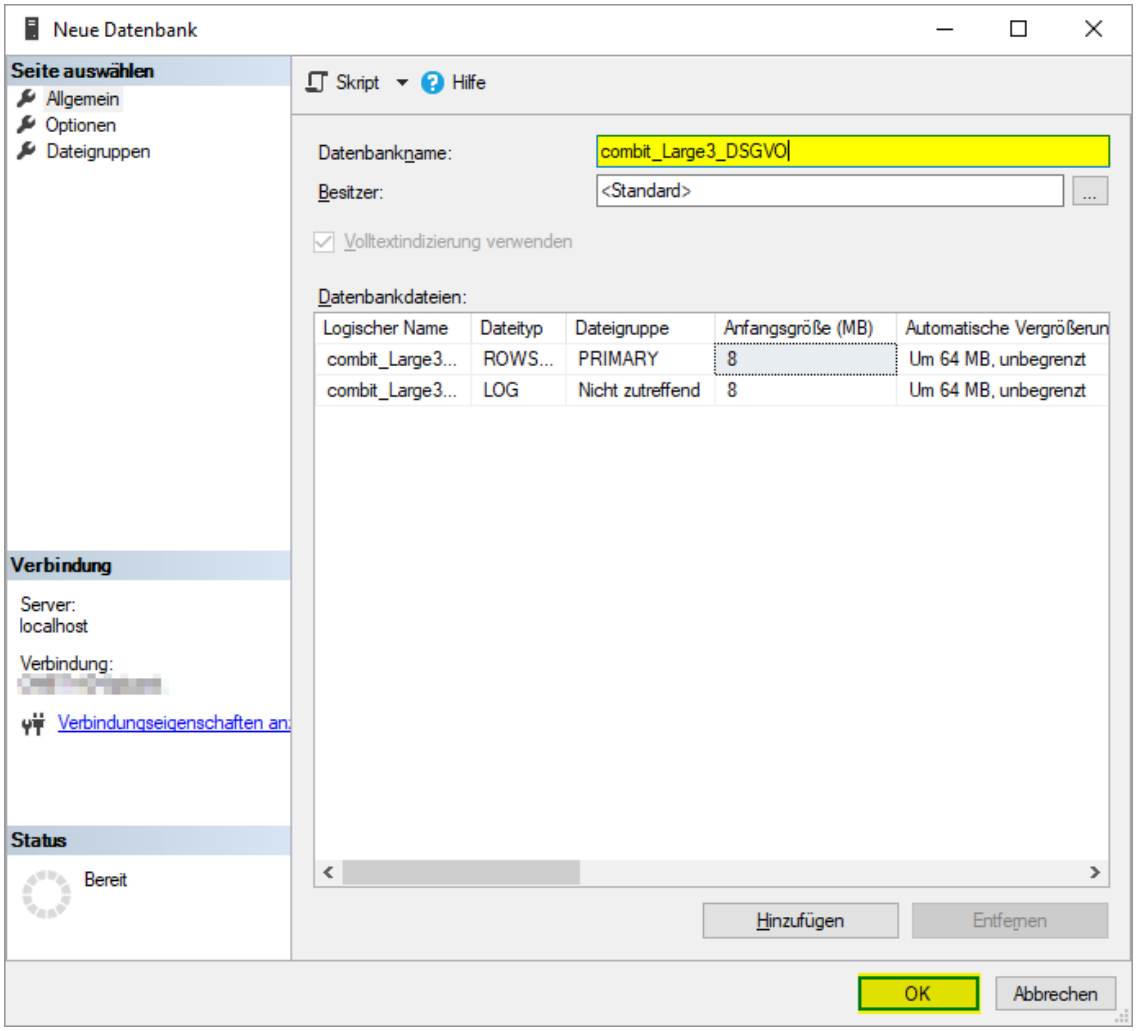
Öffnen Sie das Microsoft SQL Server Management Studio. Geben Sie bitte den Servernamen Ihres combit Relationship Manager Datenbankservers ein. Arbeiten Sie bereits auf dem combit Relationship Manager Datenbankserver so ist der Servername "localhost". Tragen Sie die entsprechenden Authentifizierungsdaten ein. Achten Sie darauf, dass Ihnen Authentifizierungsdaten vorliegen, die mit

umfassenden Rechten ausgestattet sind (z. B. "sa"-User). Klicken Sie danach bitte auf "Verbinden".

Klicken Sie nun im "Objekt-Explorer" mit der rechten Maustaste auf "Datenbanken" und dann auf "Neue Datenbank…".

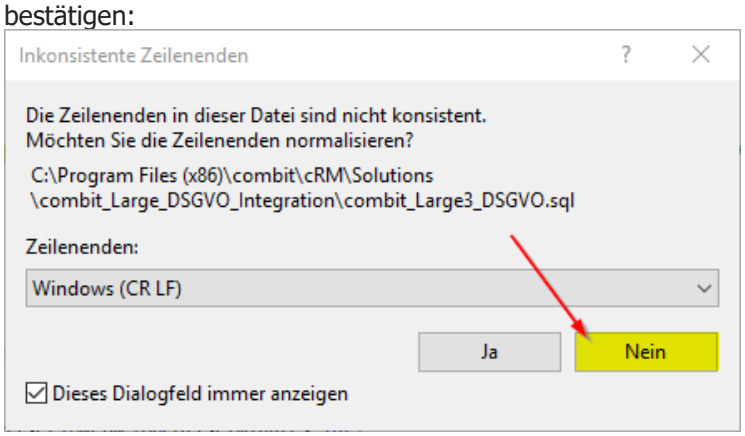


Tragen Sie in das Feld "Datenbankname"
combit_Large3_DSGVO
ein und bestätigen Sie den Dialog mit "OK".

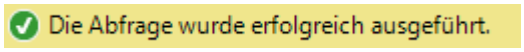


Öffnen Sie nun im Microsoft SQL Server Management Studio die Datei
combit_Large3_DSGVO.sql
aus dem "Large_DSGVO"-Ordner, den Sie entpackt und in Ihr Solution-Verzeichnis kopiert haben.

Sollte eine Meldung zu "Inkonsistenten Zeilenenden" erscheinen, so können Sie diese mit "Nein" bestätigen:



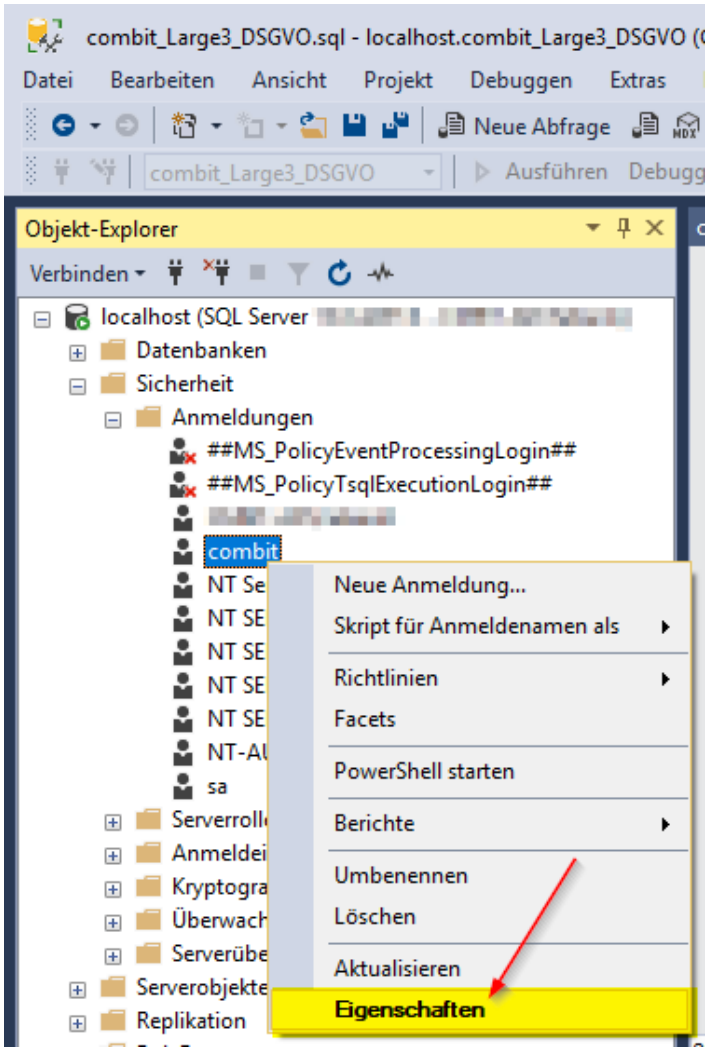
Drücken Sie die F5-Taste, um die Abfragen auszuführen. Das Ausführen kann ja nach Server- und/oder Netzwerkleistung kurze Zeit dauern. Nach Abschluss finden Sie unten in der Statusleiste diesen Hinweis:



Nun müssen Sie noch abschließend sicherstellen, dass der combit Relationship Manager auch auf diese von Ihnen neu erstellte Datenbank zugreifen kann. Wenn z. B. der combit Relationship Manager über den Datenbank-Benutzer "combit" auf die Datenbank zugreift (dies ist häufig der Standard-Fall), ist es wichtig, diesen Benutzer der von Ihnen neu erstellten Datenbank zuzuordnen.

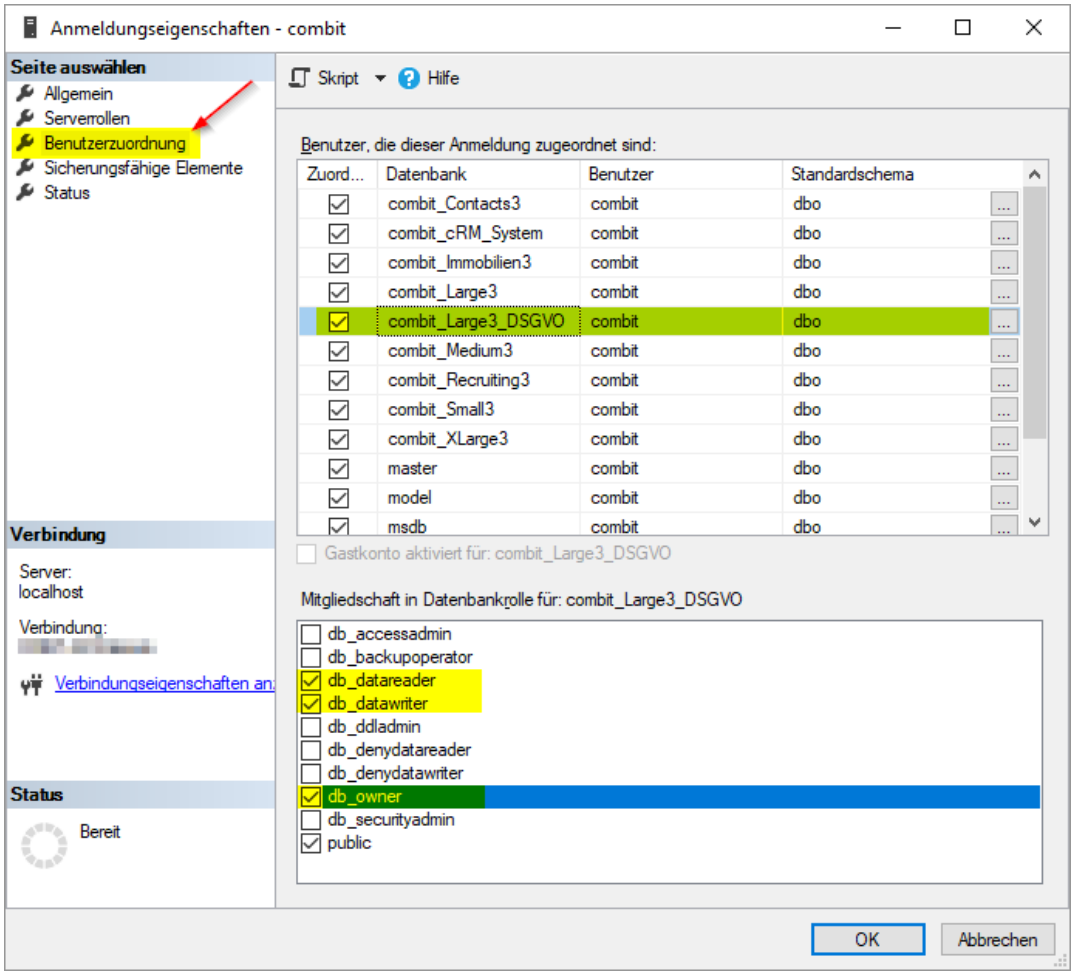
Öffnen Sie hierfür im Objekt-Explorer des Microsoft SQL Server Management Studio den Ordner "Sicherheit" > "Anmeldungen".

Wählen Sie nun den Datenbank-Benutzer aus, über den der combit Relationship Manager auf die Datenbanken zugreift (z. B. combit). Klicken Sie auf diesen Benutzer mit der rechten Maustaste und wählen Sie dann "Eigenschaften".



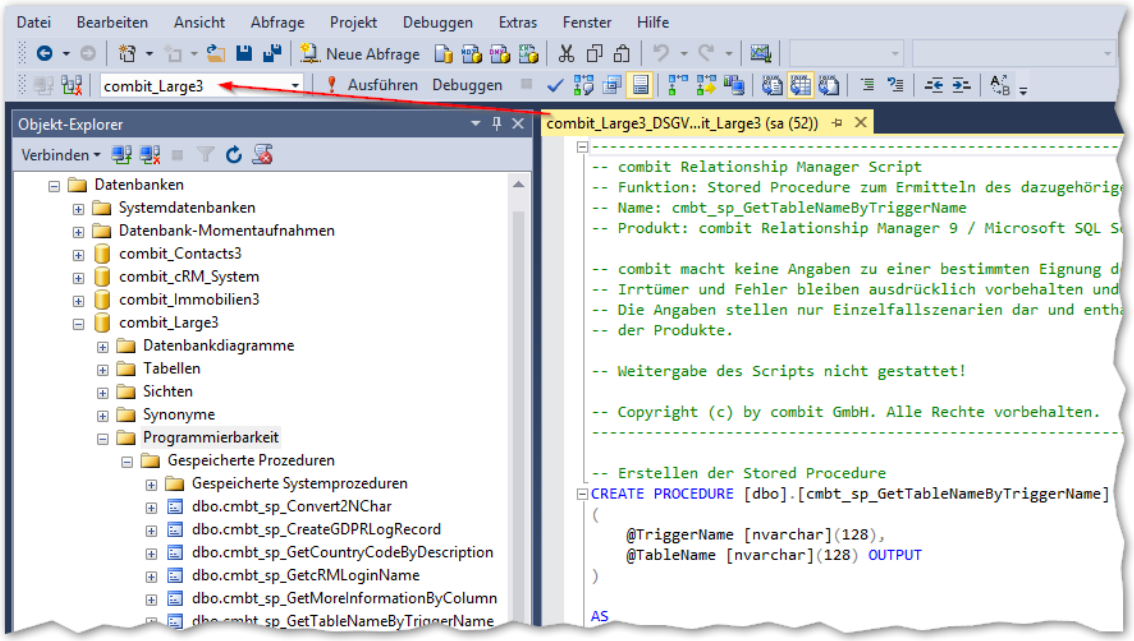
Wählen Sie dann die Seite "Benutzerzuordnung". Aktivieren Sie das "Zuordnen"-Häkchen bei "combit_Large3_DSGVO". In der Spalte "Standardschema" tragen Sie bitte "dbo" ein.

Ergänzen Sie nun unten weitere Häkchen bei "db_datareader", "db_datawriter" und "db_owner". Bestätigen Sie alles mit Klick auf "OK".



Öffnen Sie nun im Microsoft SQL Server Management Studio die Datei "combit_Large3_DSGVO_StoredProcecures.sql" aus dem "Large_DSGVO"-Ordner.

Stellen Sie sicher, dass in dem Auswahlfeld oben links Ihre Datenbank ausgewählt ist. Betätigen Sie anschließend die Schaltfläche "Ausführen".



Alles erledigt? Dann können Sie das Microsoft SQL Server Management Studio schließen.

DSGVO-Projekt in bestehende Solution importieren

Öffnen Sie nun wieder Ihre bestehende Solution, in die die DSGVO-Funktionen integriert werden sollen.

In diese Solution importieren Sie nun die Ansichten, Tabellen, Scripte usw.

Achtung! Bei diesem Import werden einige Dateien überschrieben! Sofern Sie hier selbst Anpassungen vorgenommen haben, müssen diese in den neuen Versionen nachgezogen werden!

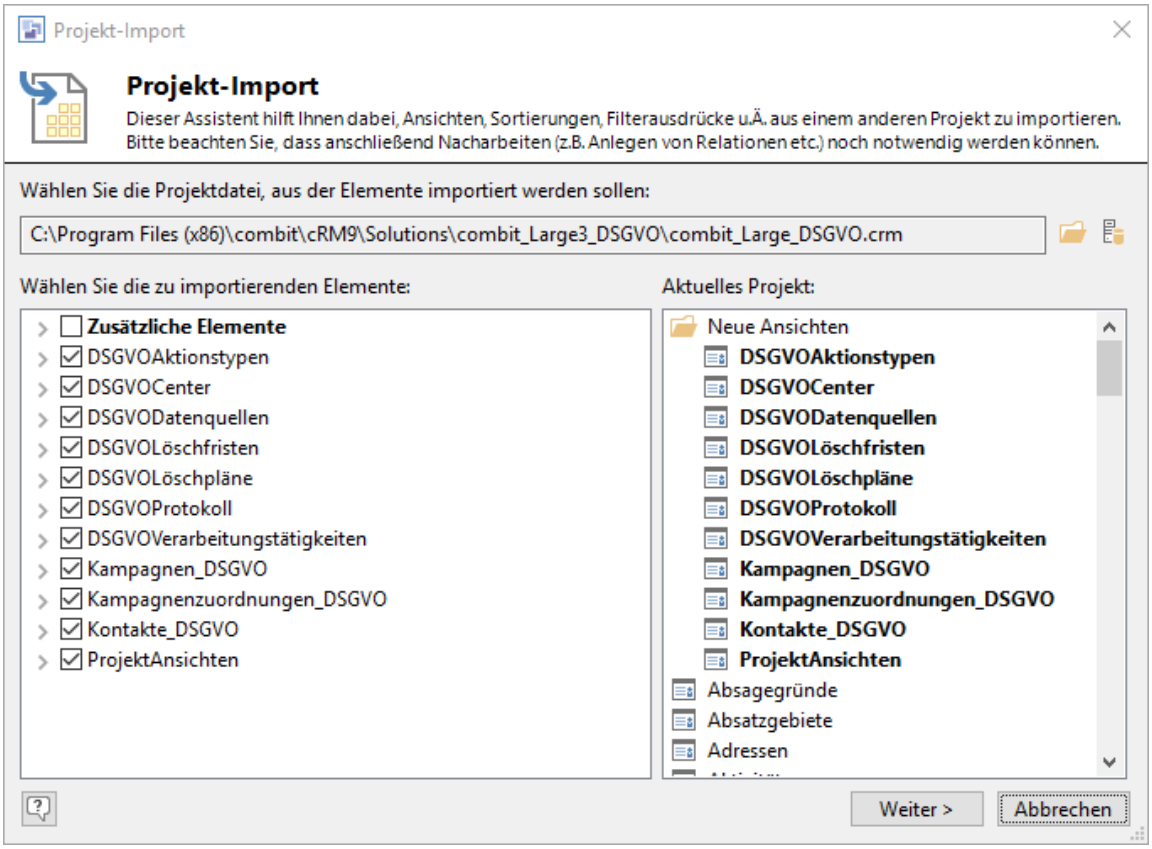
Folgende Dateien werden u.a. überschrieben oder neu angelegt:

1. Ansichten
   a. DSGVOAktionstypen.dli
   b. DSGVOCenter.dli
   c. DSGVODatenquellen.dli
   d. DSGVOLöschfristen.dli
   e. DSGVOLöschpläne.dli
   f. DSGVOProtokoll.dli
   g. DSGVOVerarbeitungstätigkeiten.dli
   h. Kampagnen_DSGVO.dli
   i. Kampagnenzuordnungen_DSGVO.dli
   j. Kontakte_DSGVO.dli
   k. ProjektAnsichten.dli
2. Scripte
   a. AddressManagement.vbs

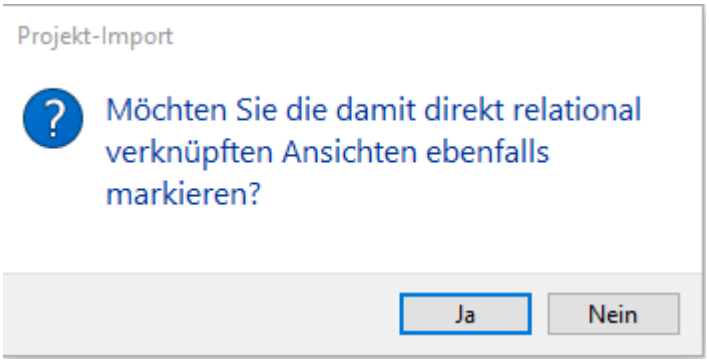
   b. AddressManagementClassic.vbs
   c. BasicCollection.vbs
   d. BasicSettings.vbs
   e. ContactCompanyManagement.vbs
   f. cRMEventManagement.vbs
   g. GDPRManagement.vbs
   h. GroupManagement.vbs
   i. ProjectLogging.vbs
   j. ShowInGoogleMaps.vbs
3. Druckvorlagen
   a. Kontakte - Auskunftserteilung nach DSGVO.lst
4. Exportvorlagen
   a. Kampagnenzuordnungen - Export für Microsoft Excel - Muster.etp
   b. Eventzuordnungen - Export für Microsoft Excel - Muster.etp
   c. Kontakte - Datenübertragung nach DSGVO.etp
   d. Kontakte - Serienbrief (inkl. Adresse).etp
5. Vorlagen zur Datenbank-Trigger-Erstellung im "Scripts"-Unterordner
   a. CreateAddressesDeleteTrigger_MSSQL.sql
   b. CreateAddressesSplitTrigger_MSSQL.sql
   c. CreateAddressesSplitTrigger_PostgreSQL.sql
   d. CreateGDPRLogRecordFunction_PostgreSQL.sql
   e. CreateGDPRLogTriggers_MSSQL.sql
   f. CreateGDPRLogTriggers_PostgreSQL.sql
6. Bilder
   a. Icon_Lock_Warning.png
   b. Icon_Tick_Grey.png

Gehen Sie nun folgendermaßen vor:

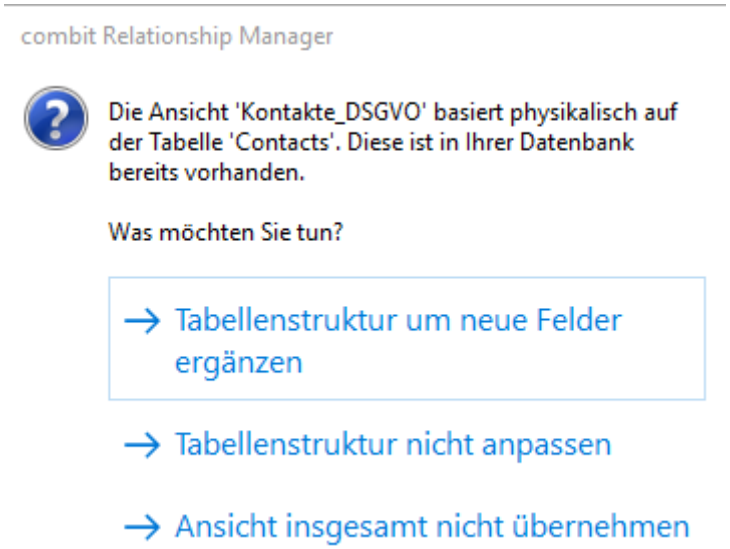
1. Um den Import zu starten wählen Sie **Datei > Information > Projekt-Import** und wählen Sie die Projektdatei "combit_Large_DSGVO.crm" im zuvor erstellten Solution-Verzeichnis "Large_DSGVO" aus.
2. Im linken Fenster wählen Sie über die Checkboxen diejenigen Elemente aus, die Sie importieren möchten.
3. Wählen Sie alle Elemente aus. Einzige Ausnahme: "Zusätzliche Elemente" NICHT aktivieren!



4. Bei einigen Ansichten kommt die Frage, ob die relational verknüpften Ansichten ebenfalls markiert werden sollen. Bestätigen Sie diese Frage mit 'Ja'.



5. Wenn Sie die Elemente "Kampagnen_DSGVO", "Kampagnenzuordnungen_DSGVO" und "Kontakte_DSGVO" auswählen, müssen Sie über einen Dialog bestätigen, dass die Tabellenstruktur um neue Felder ergänzt werden soll.



6. Starten Sie den Import
7. Tipp für Profis: Kopieren Sie vor dem Beenden des Projekt-Import-Assistenten den kompletten Text aus dem Protokoll in eine Textdatei und speichern Sie diese ab. So können Sie auch später noch nachvollziehen, was in welcher Ansicht durch den Projekt-Import ergänzt wurde.
8. Speichern Sie nach erfolgtem Import das Projekt über DATEI > Speichern ab.

Kopieren restlicher Dateien

Einige wenige Dateien werden nicht durch den Projektimport übernommen. Kopieren Sie daher die folgenden Dateien und Ordner von Hand aus dem "Large_DSGVO" Verzeichnis in das Verzeichnis Ihrer Solution (überschreiben Sie dabei evtl. vorhandene Dateien und Ordner).

- Datei "Eventzuordnungen - Export für Microsoft Excel - Muster.etp"
- Datei "Kampagnenzuordnungen - Export für Microsoft Excel - Muster.etp"
- Datei "Kontakte - Datenübertragung nach DSGVO.etp"
- Datei "Kontakte - Serienbrief (inkl. Adresse).etp"
- Ordner "Newsletterverwaltung"
- Ordner "Scripts"
- Ordner "Web-Elemente"

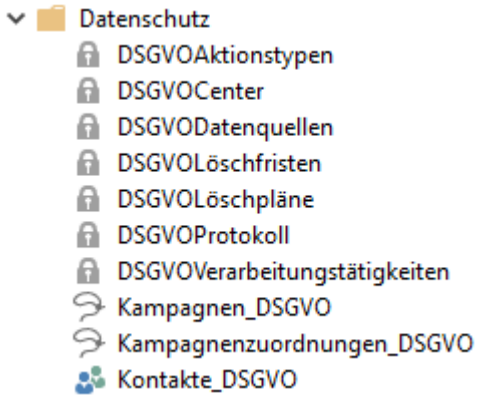
Projekt anpassen

Nachdem Sie das Projekt importiert haben, sind noch einige Nacharbeiten notwendig.

Projektnavigation

Verschieben Sie die neuen Ansichten in der Projektnavigation in einen noch anzulegenden Ordner "Datenschutz". Öffnen Sie hierzu den Dialog der Navigationsstruktur über Rechtsklick in das Navigationsfenster und Auswahl "Navigationsstruktur". Dann klicken Sie auf die Schaltfläche "Neuen Ordner anlegen" und benennen diesen "Datenschutz".

Die folgenden elf Ansichten ziehen Sie nun per Drag & Drop in den eben neu angelegten Ordner.

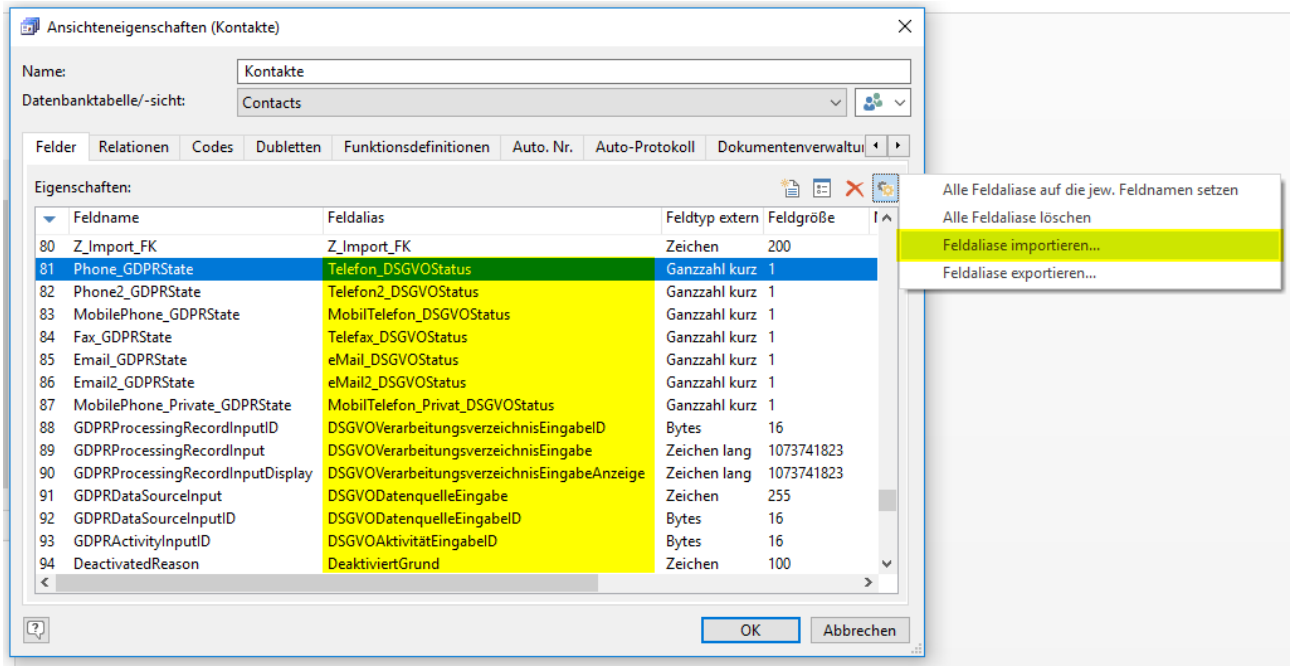


Denken Sie auch daran, dass die Anwender Zugriff auf diese Ansichten benötigen. Passen Sie daher die Zugriffsrechte in der Benutzerverwaltung an. Die Anwender benötigen mindestens das Recht "Auf Ansicht zugreifen". Weitere Informationen hierzu finden Sie im Kapitel "Zugriff autorisieren und Daten einschränken".

Feldaliase

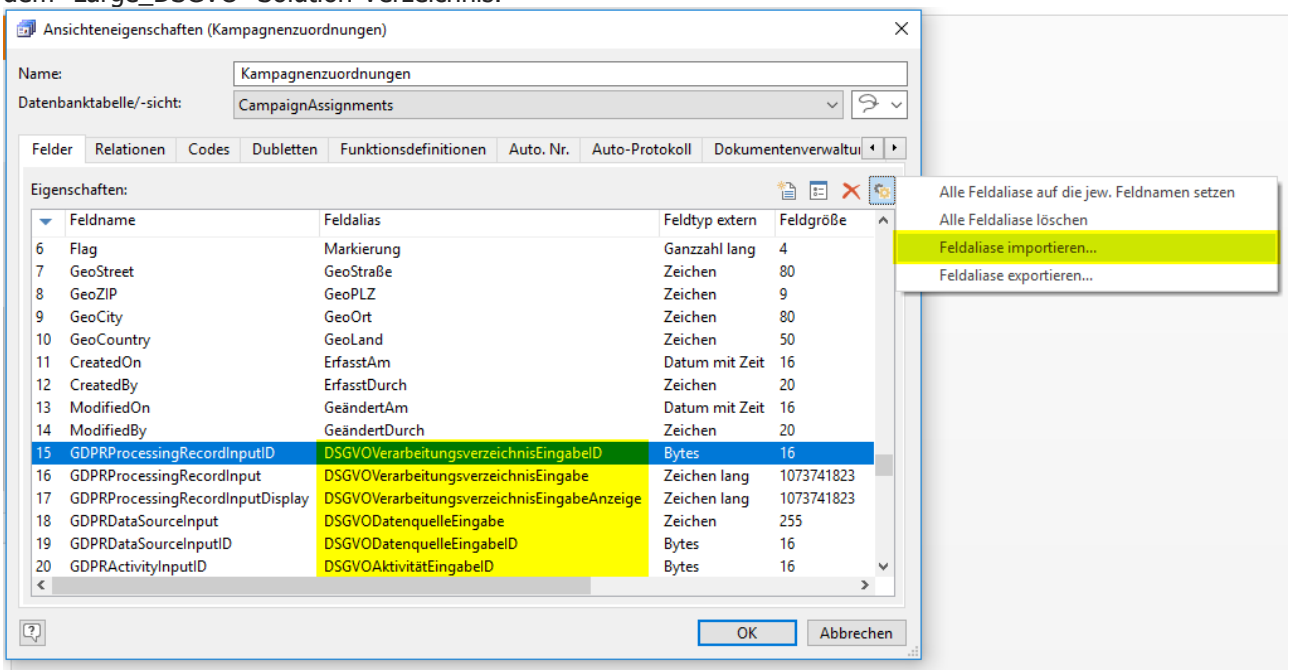
Ansicht Kontakte

Öffnen Sie die Ansichteneigenschaften der Ansicht "Kontakte" per Rechtsklick > Eigenschaften in der Projektnavigation und ergänzen Sie für die neu angelegten Datenbankfelder die entsprechenden Feldaliase. Importieren Sie dazu die Datei "Feldaliase_Kontakte.txt" aus dem "Large_DSGVO" Solution-Verzeichnis.



Ansicht Kampagnenzuordnungen

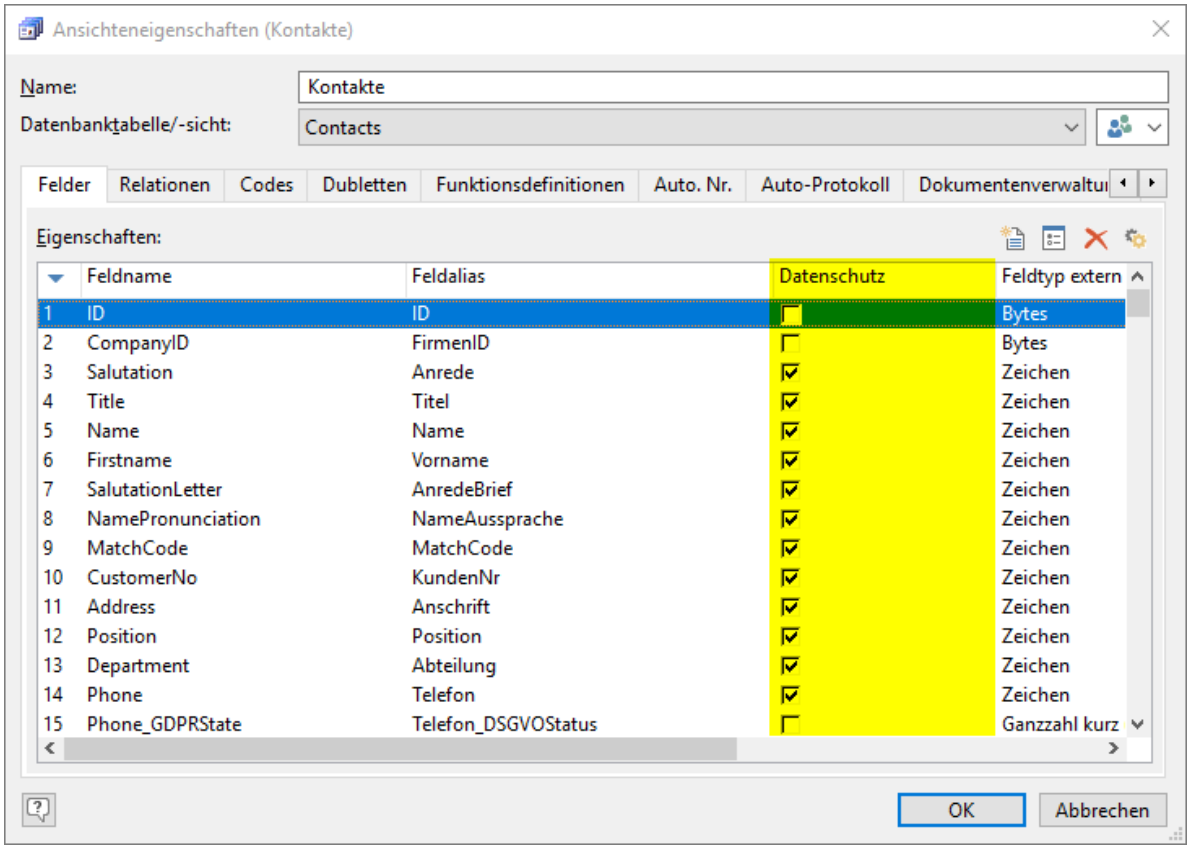
Öffnen Sie die Ansichteneigenschaften der Ansicht "Kampagnenzuordnungen" per Rechtsklick > Eigenschaften in der Projektnavigation und ergänzen Sie für die neu angelegten Datenbankfelder die entsprechenden Feldaliase. Importieren Sie dazu die Datei "Feldaliase_ Kampagnenzuordnungen.txt" aus dem "Large_DSGVO" Solution-Verzeichnis.



Datenschutzeigenschaft setzen

Setzen Sie die Eigenschaft "Datenschutz" bei allen zu protokollierenden Feldern in der Ansicht "Kontakte". Öffnen Sie hierzu die Ansichteneigenschaften der Ansicht "Kontakte" per Rechtsklick > Eigenschaften in der Projektnavigation. In der nachfolgenden Abbildung sehen Sie einen Ausschnitt der relevanten Felder für diese Ansicht. Eine vollständige Liste der relevanten Felder finden Sie in den Ansichteneigenschaften der Ansicht "Kontakte_DSGVO".

Weitere Informationen hierzu finden Sie im Kapitel "Dokumentationspflicht erfüllen".



Funktionen übertragen

Dokumentationspflicht erfüllen

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?" und "Zusammenhang mit einer Aktivität?". Diese Informationen werden dann protokolliert.

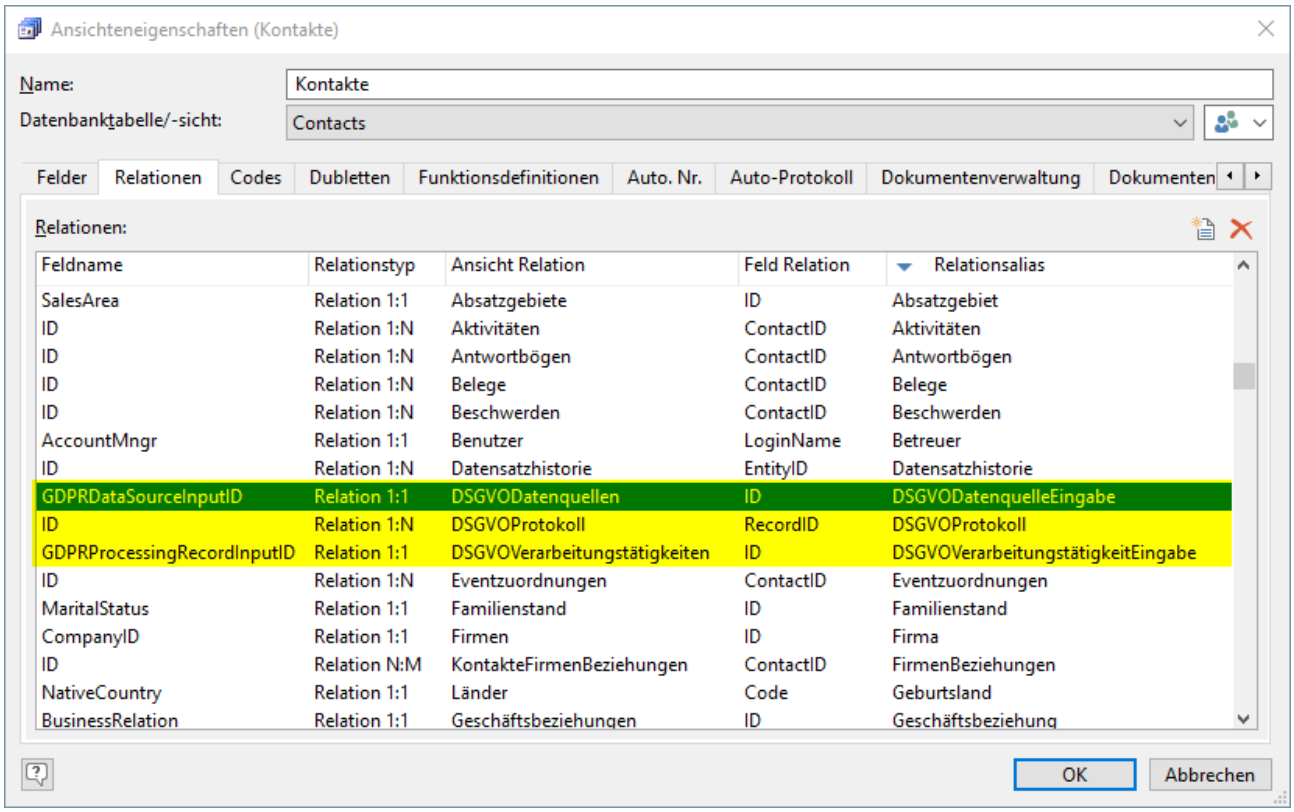
Ansicht Kontakte (oder andere Zielansicht)

Bevor die Funktionen eingebaut werden können, müssen nun noch die passenden Relationen angelegt werden.

Relationen anlegen

Öffnen Sie die Ansichteneigenschaften der Ansicht "Kontakte" per "Rechtsklick > Eigenschaften" in der Projektnavigation und ergänzen Sie für die neuen Schaltflächen und den neuen Container die 3 entsprechenden Relationen gemäß der nachstehenden Abbildung:

DSGVODatenquelleEingabe
DSGVOProtokoll
DSGVOVerarbeitungstätigkeitEingabe



Speichern Sie anschließend das Projekt über "DATEI > Speichern".

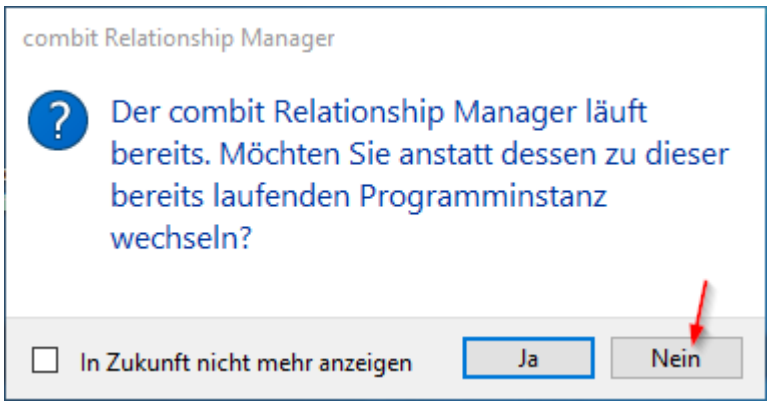
Eingabemaske anpassen

Nun können Sie die Objekte (Eingabefelder, Schaltflächen, Container etc.) in der Eingabemaske der Kontakte-Ansicht platzieren.

Dazu öffnen Sie am besten die Eingabemaske der Ansicht "Kontakte_DSGVO" im Eingabemaskendesigner (Strg+J) und kopieren von dort über Strg+C und Strg+V die Objekte in die vorhandene Kontakte-Ansicht. Somit dient Ihnen unsere Kontakte_DSGVO-Ansicht als Kopiervorlage für Ihre bestehende Ansicht.

Am einfachsten wird es sein, wenn Sie den combit Relationship Manager in einer weiteren Instanz öffnen und dann beide Ansichten im jeweiligen Eingabemaskendesigner öffnen. So können Sie schnell die Elemente hin- und her kopieren. Eine weitere Instanz öffnen Sie, indem Sie den combit Relationship Manager nochmals über das Desktopsymbol starten und folgenden Dialog verneinen.

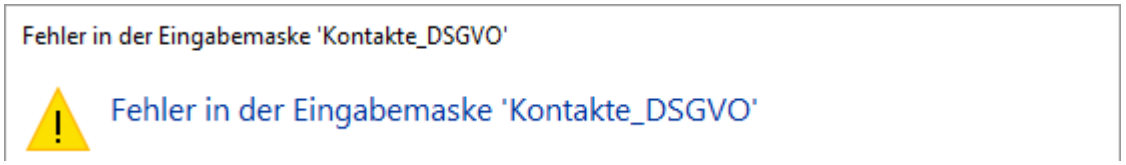
Wichtig: Laden Sie in der zweiten Instanz erneut Ihre Solution und nicht das DSGVO-Projekt aus dem zip-Archiv. Dieses ist nur für den Projekt-Import in Ihre eigene Solution vorgesehen und sollte daher nicht direkt geöffnet werden.



Beim Öffnen der folgenden Ansichten

- Kontakte_DSGVO
- Kampagnen_DSGVO
- Kampagnenzuordnungen_DSGVO

wird jeweils eine Fehlermeldung erscheinen, zum Beispiel so wie hier:



Von diesen Fehlermeldungen dürfen Sie sich nicht irritieren lassen. Hintergrund hierfür ist, dass wir in den oben genannten 3 Vorlagen-Ansichten bewusst auf den Einbau von Relationen verzichtet haben, um diese Vorlagen nicht allzu sehr mit Ihrer bestehenden Solution zu "vernetzen". Auf diese Weise können wir Ihnen die Eingabemasken-Vorlagen so komplett wie nur möglich zur Verfügung stellen.

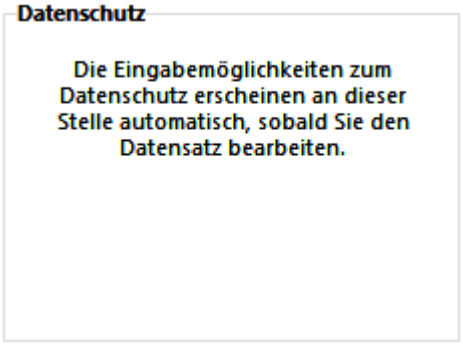
Wenn bei den nachfolgenden Schritten also eine dieser Fehlermeldungen erscheint, bestätigen Sie diese einfach mit Klick auf "OK".

Die Anzeigemöglichkeiten beim Datenschutz-Block

Diesen Datenschutz-Block können Sie nun aus der Kontakte_DSGVO-Ansicht herauskopieren. Vorab sollten Sie sich überlegen, an welcher Stelle der Datenschutz-Block in Ihrer Kontakte Ansicht positioniert werden soll. Hier gibt es zwei Möglichkeiten.

Variante 1: Sie können diesen Datenschutz-Block über ein anderes Element (in unserem Beispiel über die "Kontroll-Anzeige für die Anschrift") legen. Dann wird der Block nur im Bearbeitungsmodus (Kontakt wird bearbeitet) angezeigt, also immer dann, wenn hier Eingaben vorzunehmen sind.

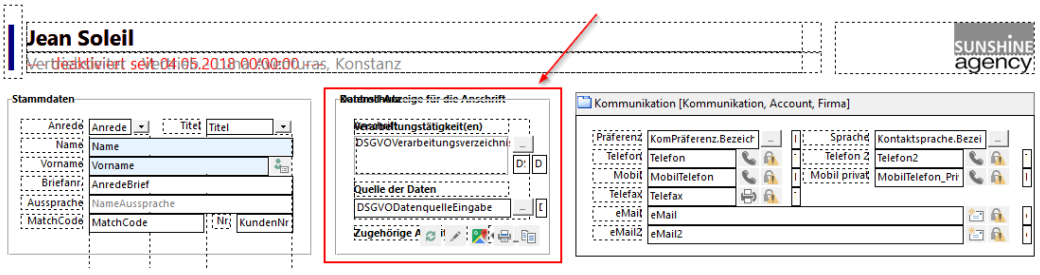
Variante 2: Wenn Sie über ausreichend Platz in Ihrer Eingabemaske verfügen, können Sie diesen Datenschutz-Block an einen von Ihnen gewählten Platz frei positionieren. Wenn Sie sich im Anzeigemodus befinden, also den Datenschutz-Block nicht benötigen, wird er dann wie folgt angezeigt:



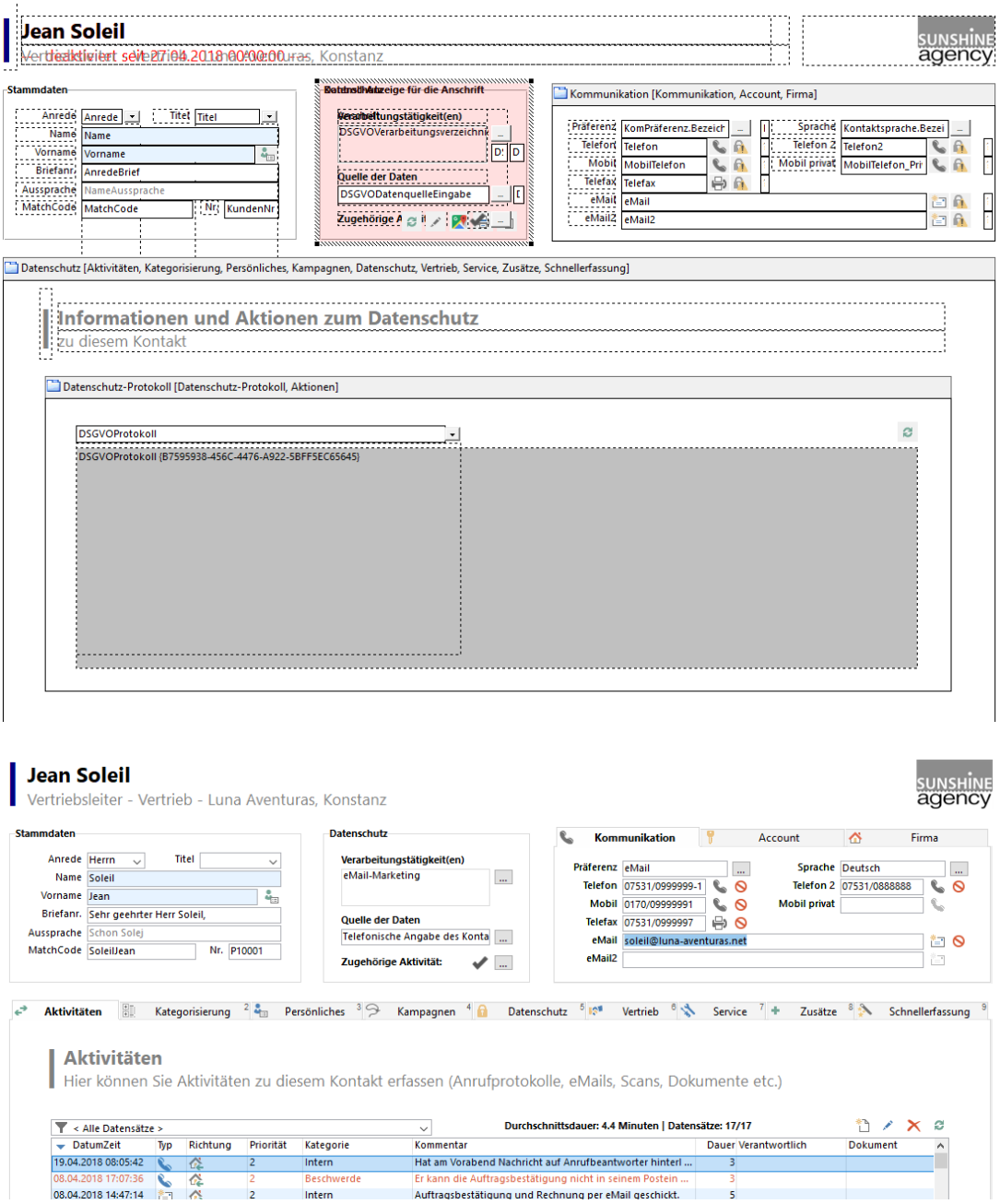
Sobald Sie sich im Bearbeitungsmodus befinden, werden Ihnen die entsprechenden Eingabefelder im Datenschutz-Block wieder angezeigt.

Die Implementierung des Datenschutz-Blocks

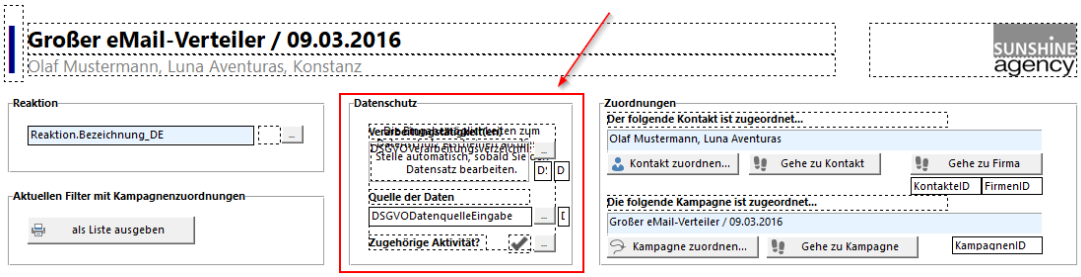
1. Variante 1: Datenschutz-Block und Kontrollanzeige für die Anschrift überlagen sich
    a. Öffnen Sie die Kontakte-Ansicht im Eingabemaskendesigner und löschen den Block "Kontroll-Anzeige für die Anschrift".
    b. In der neu geöffneten zweiten combit Relationship Manager Instanz öffnen Sie die Ansicht "Kontakte_DSGVO" ebenfalls im Eingabemaskendesigner. Nun markieren Sie den neuen kombinierten Datenschutz-/Adress-Block und kopieren diesen mit STRG+C.



    c. In der Kontakte-Ansicht fügen Sie nun den kopierten Datenschutz-/Adress-Block an die nun frei gewordene Stelle ein (STRG+V), an der Sie zuvor die Gruppierung "Kontroll-Anzeige für die Anschrift" entfernt haben.



2. Variante 2: Datenschutz-Block steht alleine und überlagert keine anderen Controls
    a. Wechseln Sie hierzu in die Ansicht "Kampagnenzuordnungen_DSGVO", markieren und kopieren (STRG+C) Sie die Gruppierung "Datenschutz".

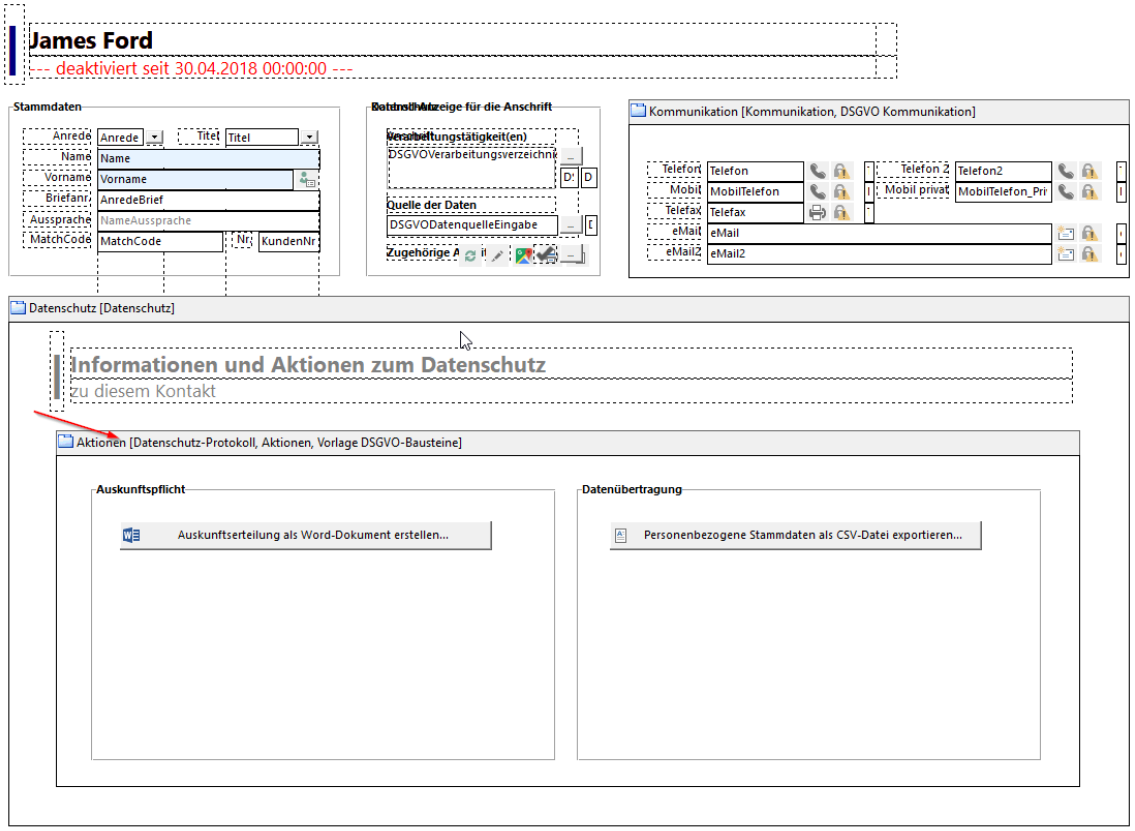


b. Fügen Sie nun den kopierten Datenschutz-Block in der Kontakte-Ansicht an eine von Ihnen gewählte freie Position ein (STRG+V).

3. Speichern Sie die Eingabemaske.

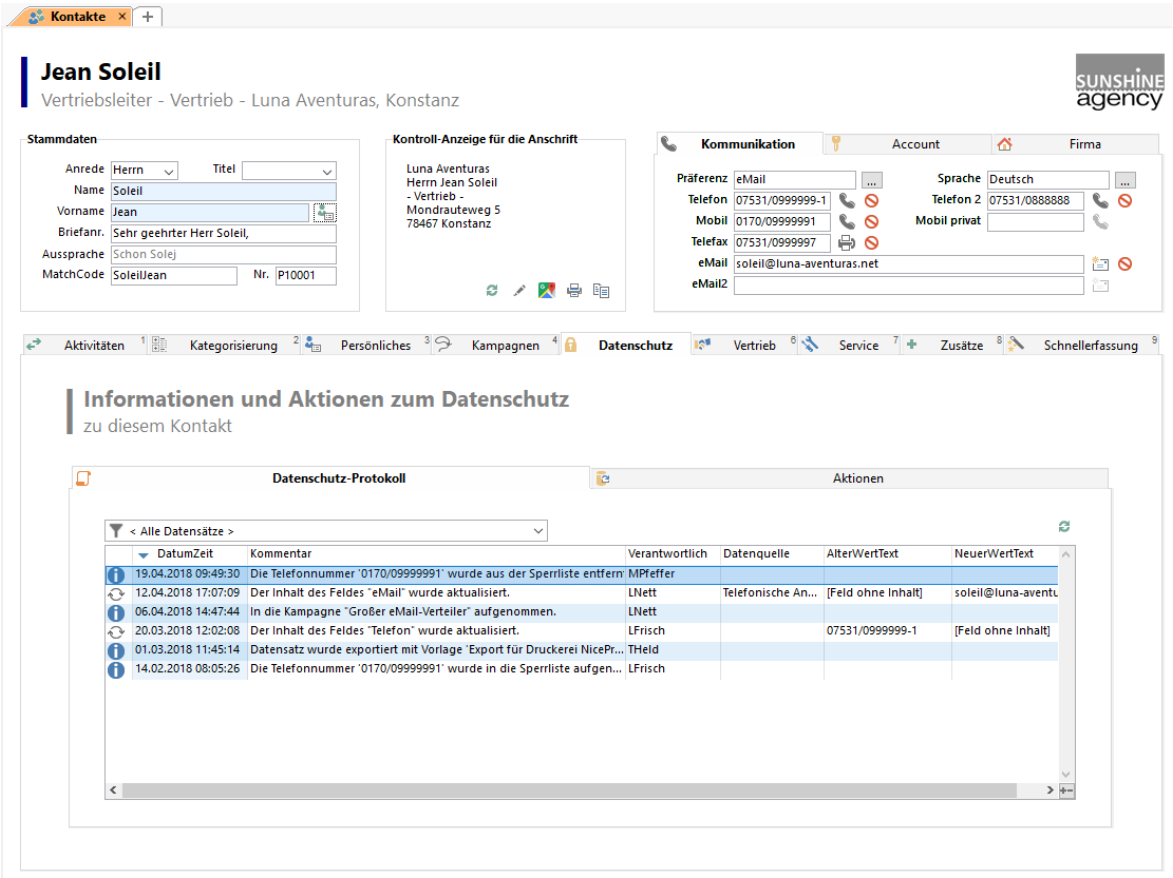
Fügen Sie nun die Hauptregisterkarte "Datenschutz" inklusive der Registerkarten "Datenschutz-Protokoll" und "Aktionen" (Auskünfte erteilen) in Ihre Kontakte-Ansicht ein:

1. Öffnen Sie die Kontakte-Ansicht im Eingabemaskendesigner.
2. Erstellen Sie in Ihrer Kontakte-Ansicht eine neue Hauptregisterkarte.
3. Doppelklicken Sie die neue Hauptregisterkarte. Benennen Sie die Lasche in "Datenschutz" um und wählen ein entsprechendes Symbol, z.B. das graue Schloss-Symbol in der Symbol-Gruppe "Symbole 17".
4. Öffnen Sie die Ansicht "Kontakte_DSGVO" in der zweiten combit Relationship Manager Instanz im Eingabemaskendesigner. Kopieren Sie die komplette Hauptregisterkarte "Datenschutz" inklusive aller Registerkarten und Elemente, indem Sie mit dem Cursor zunächst den inneren Block markieren und kopieren (STRG+C).

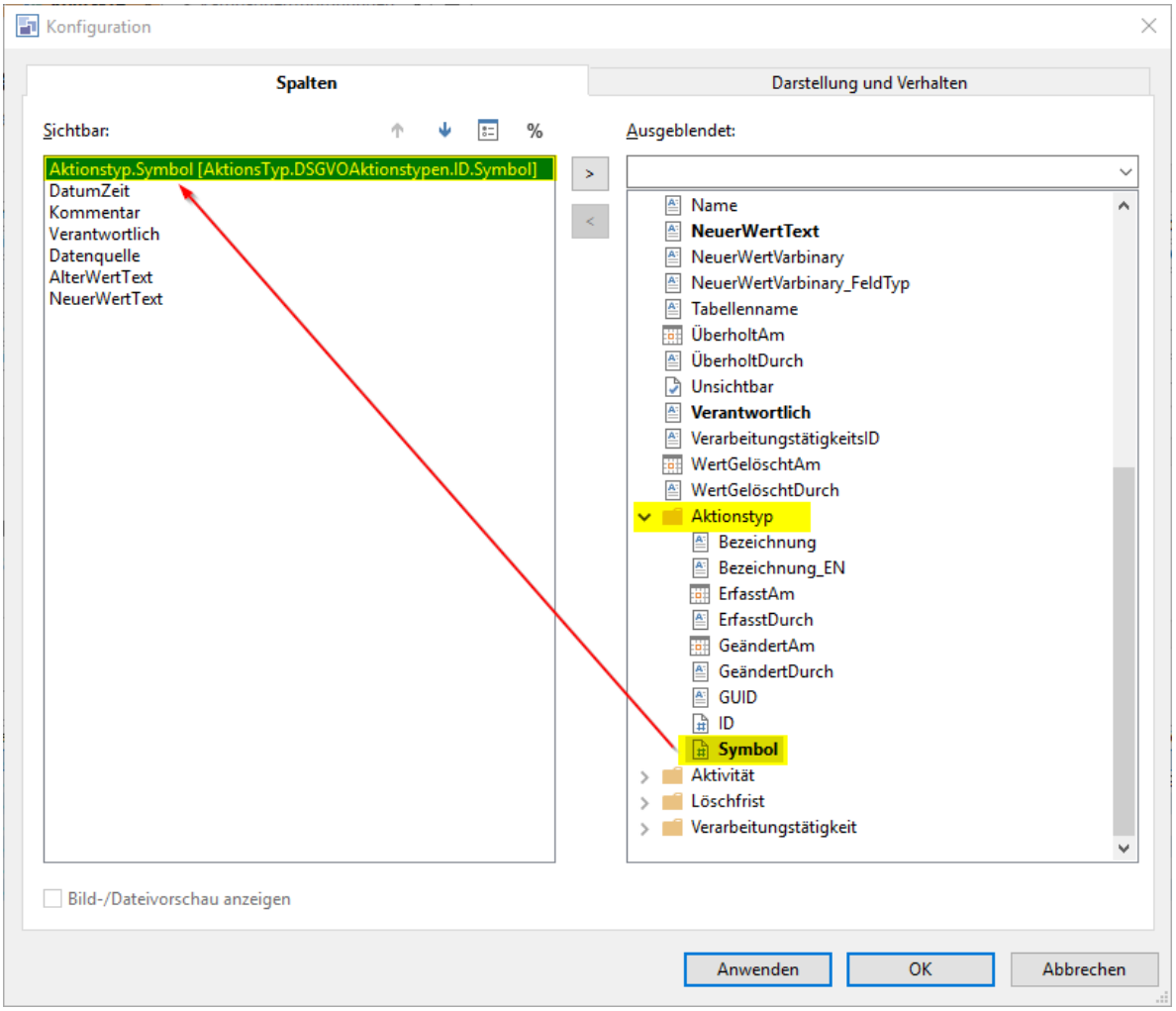


5. Fügen Sie nun die kopierten Elemente in der Kontakte-Ansicht in die neue Hauptregisterkarte "Datenschutz" ein, indem Sie den Cursor irgendwo in den leeren Reiter setzen und STRG+V drücken (verschieben Sie dabei evtl. falsch platzierte Controls an die richtige Stelle).
6. Kopieren Sie die drei fehlenden Elemente ebenfalls und fügen Sie diese in die Kontakte-Ansicht ein.

7. Speichern Sie und Schließen anschließend den Eingabemaskendesigner.



8. Klicken Sie in der neuen Registerkarte "Datenschutz-Protokoll" per Rechtsklick auf den Spaltentitel und wählen Sie "Konfigurieren > Layout und Spalten". Passen Sie nun die Spaltenkonfiguration an (Ziel ist die Darstellung im nachstehenden Screenshot). Speichern Sie am Ende die vorgenommene Konfiguration für alle Nutzer per "Rechtsklick > Konfigurieren > Als Projekteinstellungen für alle Anwender speichern" ab.



9. Den Spaltentitel und die Bearbeitbarkeit der einzelnen Spalten können Sie ändern, indem Sie mit der rechten Maustaste auf den Spaltentitel klicken und "Konfigurieren > Spalteneigenschaften" wählen.

Schaltfläche "Alle aktuell gefilterten Kontakte einer Kampagne zuordnen..."
Bei der Nutzung unseres Kampagnenmoduls für z.B. die Zusammenstellung von Newsletter Verteilern, müssen Sie nun die folgende Schaltfläche in der Kontakte-Ansicht ersetzen, damit beim Hinzufügen von Kontakten zu einer Kampagne der neue Datenschutz-Dialog starten kann.

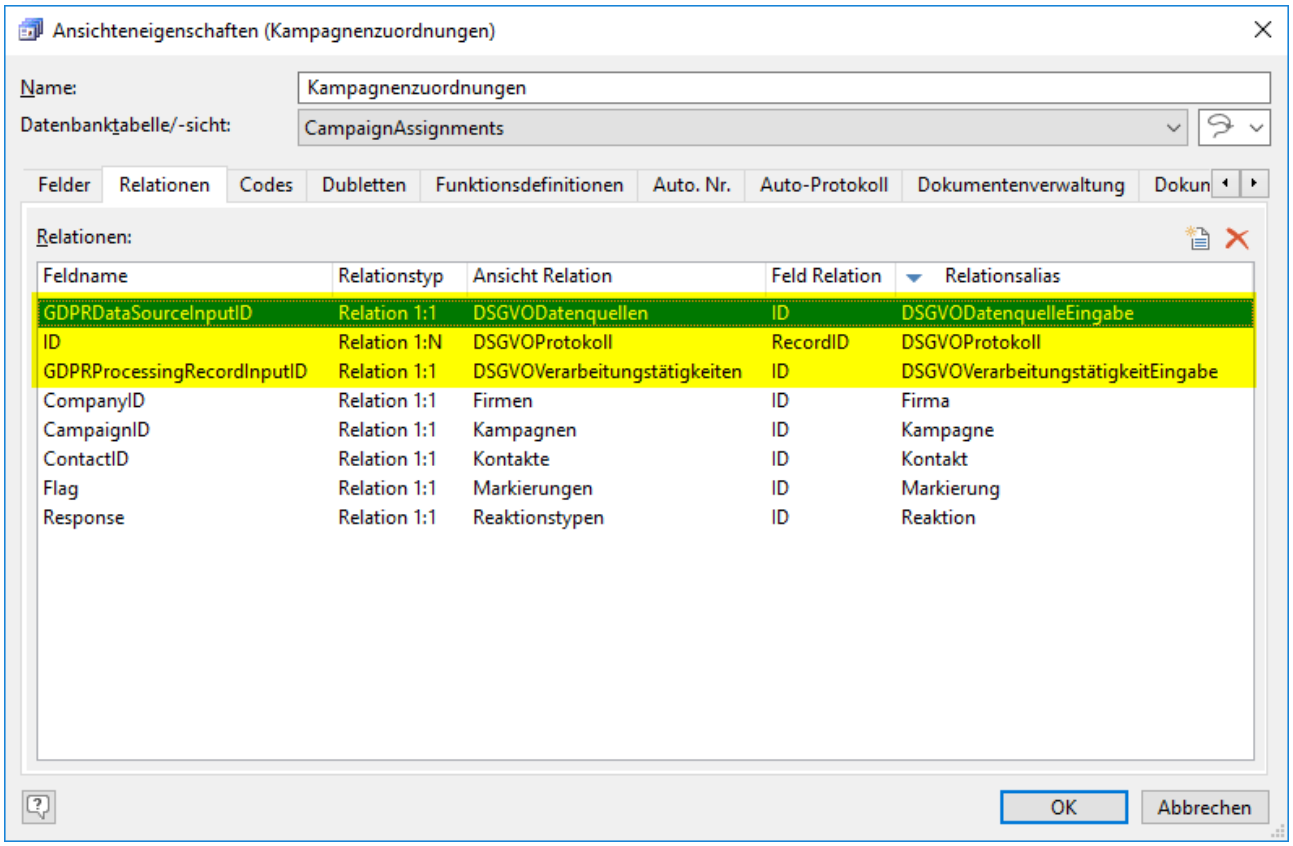
1. Öffnen Sie die Ansicht "Kontakte_DSGVO" im Eingabemaskendesigner.
2. Kopieren Sie auf der Lasche "Kampagnen" die Schaltfläche "Alle aktuell gefilterten Kontakte einer Kampagne zuordnen...".
3. Öffnen Sie die Ansicht "Kontakte" im Eingabemaskendesigner und löschen dort eben diese Schaltfläche.
4. Fügen Sie die kopierte Schaltfläche an derselben Stelle ein.
5. Speichern Sie und Schließen anschließend den Eingabemaskendesigner.

Ansicht Kampagnenzuordnungen

Relationen anlegen

Öffnen Sie die Ansichteneigenschaften der Ansicht "Kampagnenzuordnungen" per "Rechtsklick > Eigenschaften" in der Projektnavigation und ergänzen Sie für die neuen Schaltflächen und den neuen Container die 3 entsprechenden Relationen gemäß der nachstehenden Abbildung:

DSGVODatenquelleEingabe
DSGVOVerarbeitungstätigkeitEingabe
DSGVOProtokoll

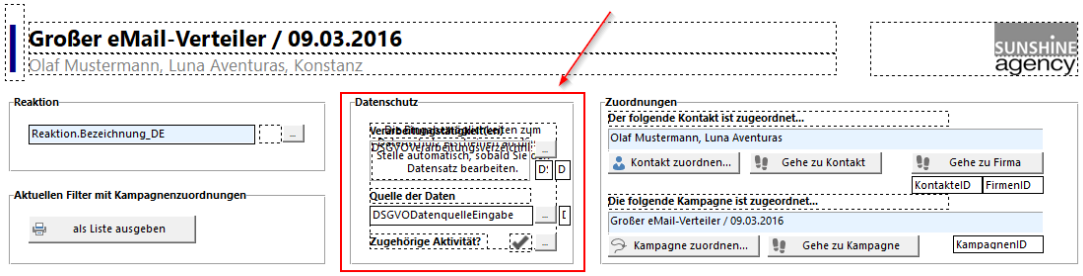


Speichern Sie anschließend das Projekt über "DATEI > Speichern".

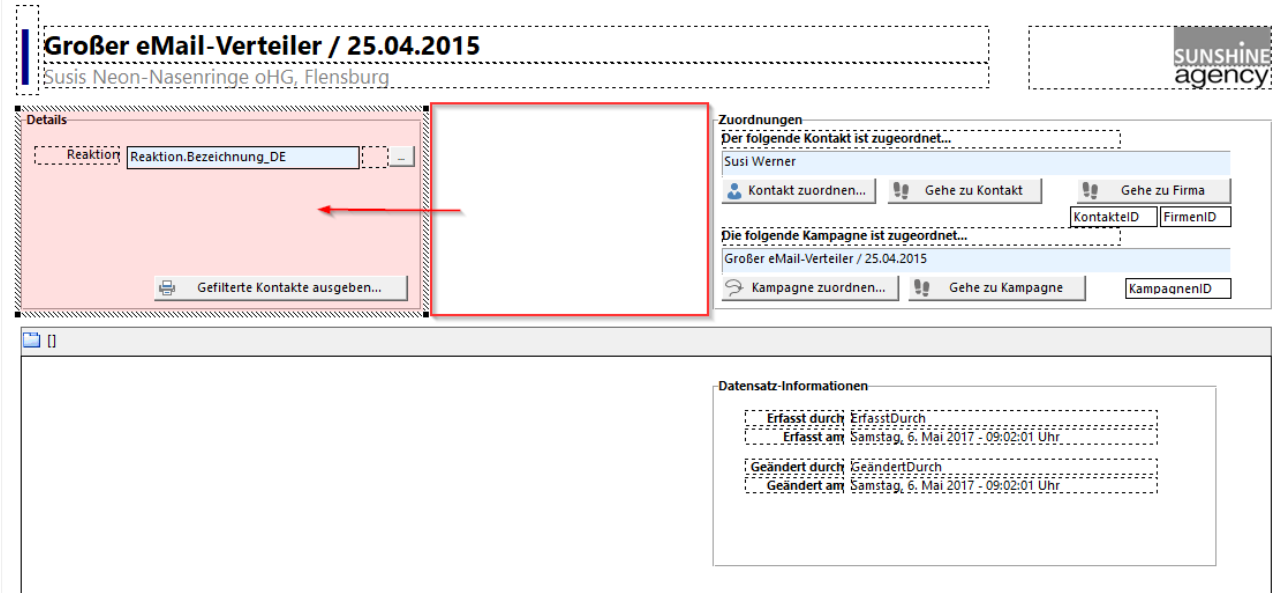
Eingabemaske anpassen

Fügen Sie nun den Datenschutzblock auch in die Ansicht "Kampagnenzuordnungen" ein:

1. Öffnen Sie die Ansicht "Kampagnenzuordnungen_DSGVO" im Eingabemaskendesigner.
2. Markieren und kopieren (STRG+C) Sie hierzu oben in der Mitte den "Datenschutz-Block".



3. Öffnen Sie die Ansicht "Kampagnenzuordnungen" in der zweiten combit Relationship Manager Instanz im Eingabemaskendesigner.
4. Verschieben oder verkleinern Sie ggf. hierzu den oder die bereits bestehenden Blöcke, um den entsprechenden Platz zu erhalten. In diesem Fall bietet es sich an die oberen rechten Blöcke zu verkleinern, damit Sie in der Mitte den entsprechenden Platz erhalten.



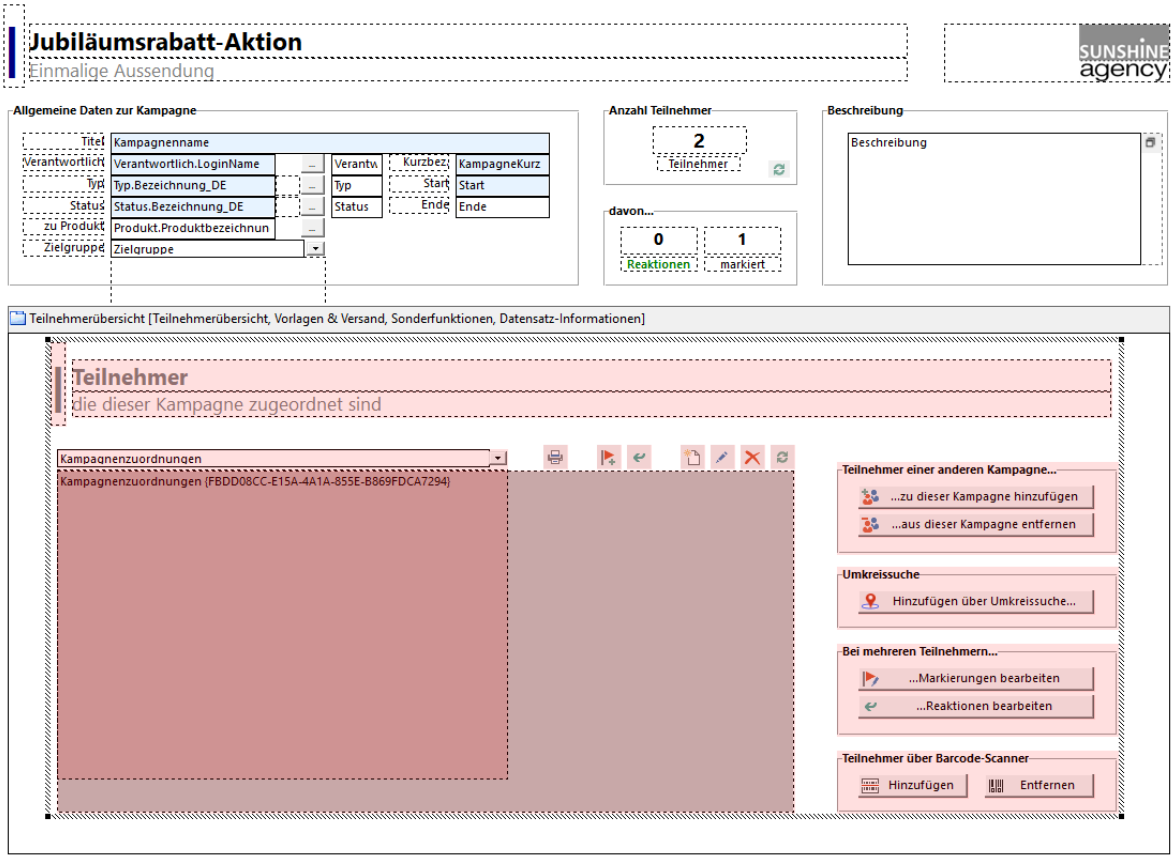
5. Den kopierten "Datenschutz-Block" können Sie an die oben in der Mitte frei gewordene Position einfügen (STRG+V).
6. Speichern Sie und Schließen anschließend den Eingabemaskendesigner.

Ansicht Kampagnen

Eingabemaske anpassen

Passen Sie nun die Eingabemaske der Ansicht "Kampagnen" an. Wichtig ist hier primär der Austausch der Schaltflächen, da die neuen Schaltflächen nun auch zum Teil Datenschutz-Themen mit behandeln. Voraussetzung ist insbesondere für die nachstehenden Schritte, dass Sie unsere aktuelle Kampagnen-Lösung der Large Solution des combit Relationship Manager 9 bereits im Einsatz haben.

1. Öffnen Sie die Ansicht "Kampagnen_DSGVO" im Eingabemaskendesigner.
2. Markieren und kopieren (STRG+C) Sie im Reiter "Teilnehmerübersicht" möglichst alle Elemente innerhalb des Reiters.



3. Öffnen Sie in der zweiten combit Relationship Manager Instanz die Ansicht "Kampagnen" im Eingabemaskendesigner.
4. Löschen Sie dort im Reiter "Teilnehmerübersicht" alle Elemente.
5. Die kopierten Elemente können Sie nun in dem leer gewordenen Reiter wieder einfügen (STRG+V). Tipp: Klicken Sie zunächst mit der Maus in den leeren Reiter, bevor Sie die Elemente einfügen. Damit stellen Sie sicher, dass alles gleich richtig positioniert wird.
6. Wiederholen die Schritte 1-5 für die Reiter "Vorlagen & Versand" sowie "Sonderfunktionen".
7. Speichern Sie und Schließen anschließend den Eingabemaskendesigner.

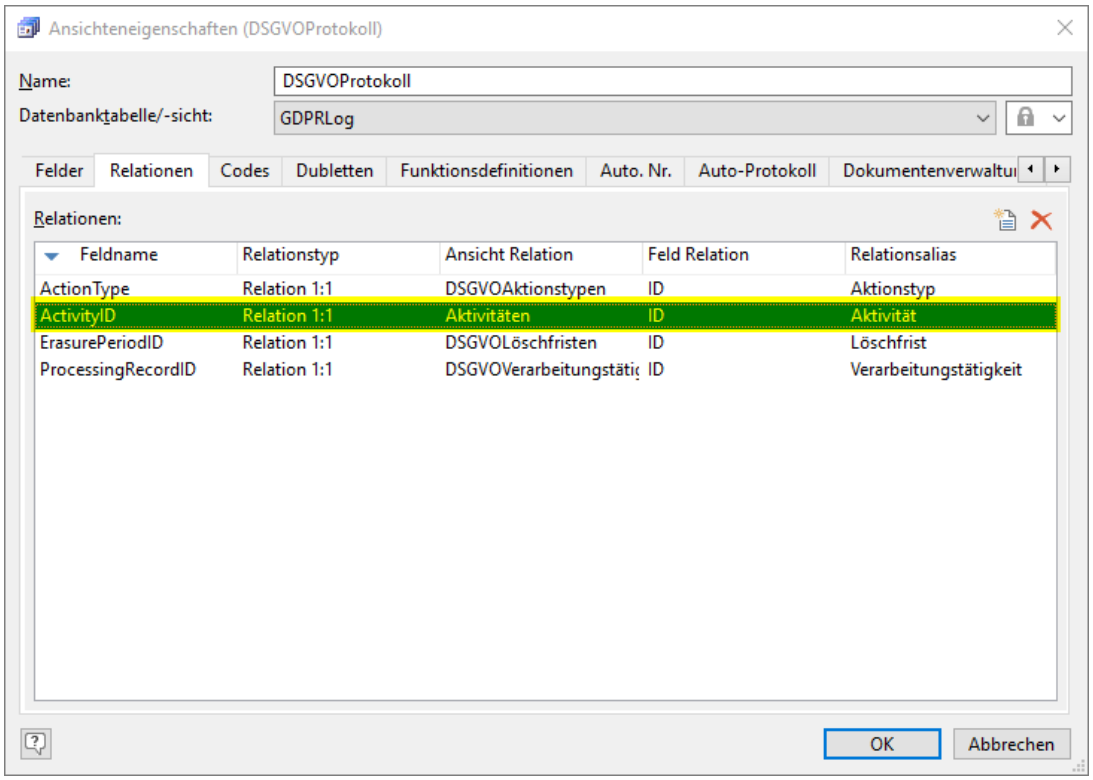
Wichtig zu wissen: Optisch verändert sich nichts! Im Hintergrund wurden aber die betroffenen Schaltflächen um die Datenschutz-Prozesse angereichert.

Ansicht DSGVOProtokoll

Relationen anlegen

Öffnen Sie die Ansichteneigenschaften der Ansicht "DSGVOProtokoll" per "Rechtsklick > Eigenschaften" in der Projektnavigation und ergänzen Sie die Relation gemäß der nachstehenden Abbildung:

Aktivität



Speichern Sie anschließend das Projekt über "DATEI > Speichern".

Widerspruch berücksichtigen

Für jedes Kommunikationsfeld im combit Relationship Manager kann ein Status festgehalten werden. Es gibt hier die folgenden 3 Status-Werte:

- "unbekannt"
- "erlaubt"
- "gesperrt"

Der aktuelle Status kann neben den entsprechenden Kommunikationsfeldern über ein Symbol dargestellt werden. Er kann dann auch in Filtern und Formeln jederzeit berücksichtigt werden, z. B. beim Vorbereiten einer Aussendung oder beim Export.

Zusätzlich zum Status eines Kommunikationsfeldes gibt es noch die Sperrliste im combit Relationship Manager. Es handelt sich dabei um eine Art zusätzliches "Sicherheitsnetz": Setzen Sie für den Inhalt eines

Kommunikationsfeldes den Status "gesperrt", wird dieser zusätzlich auf eine globale Sperrliste im combit Relationship Manager gesetzt: Dadurch wird selbst eine unabsichtliche Kontaktaufnahme per eMail oder Telefon aus der Software heraus zuverlässig verhindert. Übrigens 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 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. In den nachfolgenden Schritten erfahren Sie, wie Sie dieses Konzept in Ihre Solution einbauen. Unser Beispiel ist wieder die Kontakte-Ansicht, da eben hier der Einbau oftmals sinnvoll ist.

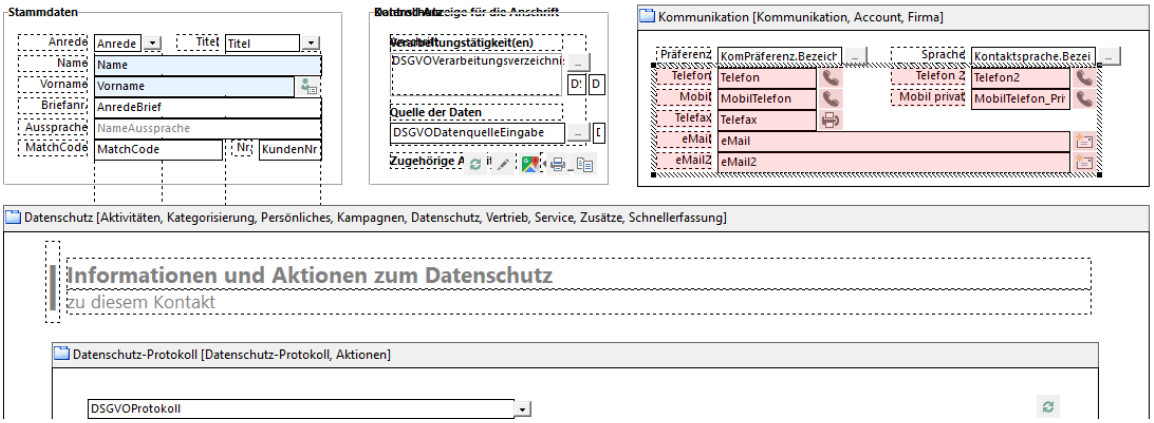
Ansicht Kontakte

Eingabemaske anpassen

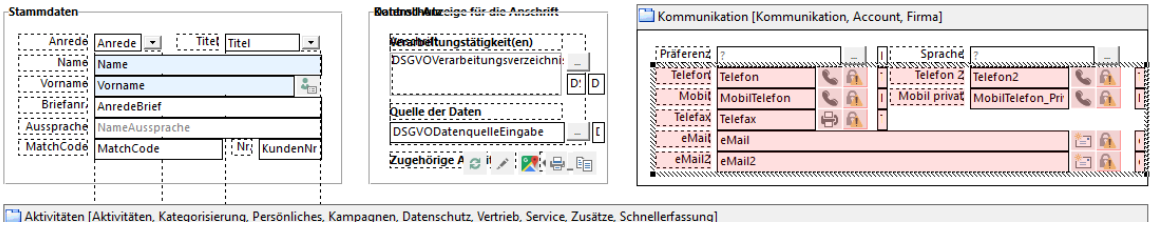
Fügen Sie nun die entsprechenden Schaltflächen zu den Kommunikationsfeldern Ihrer Kontakte-Ansicht ein. Gerade wenn Sie den Kommunikations-Block im Hinblick auf unseren Standard gar nicht verändert haben, lohnt es sich, sämtliche Felder in diesem Bereich austauschen.

So tauschen Sie den gesamten Kommunikations-Block aus:

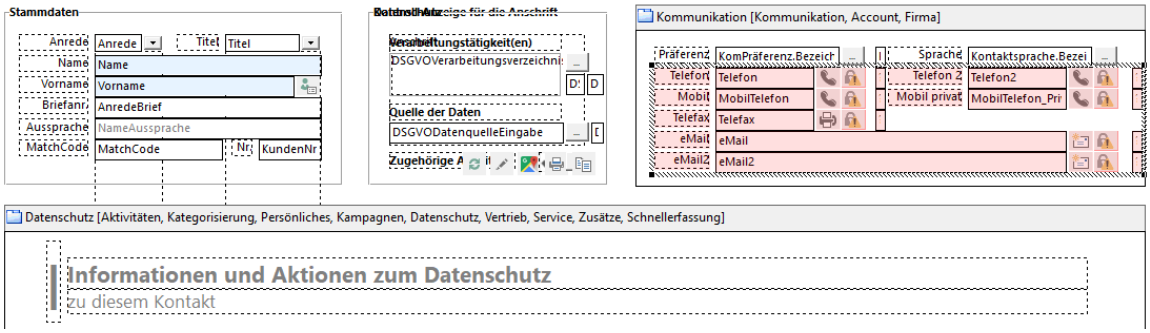
1. Öffnen Sie die Ansicht "Kontakte" Eingabemaskendesigner.
2. Markieren Sie oben rechts im Reiter "Kommunikation" alle Elemente außer den beiden oberen Feldern "Präferenz" und "Sprache" (wenn vorhanden) und löschen diese.



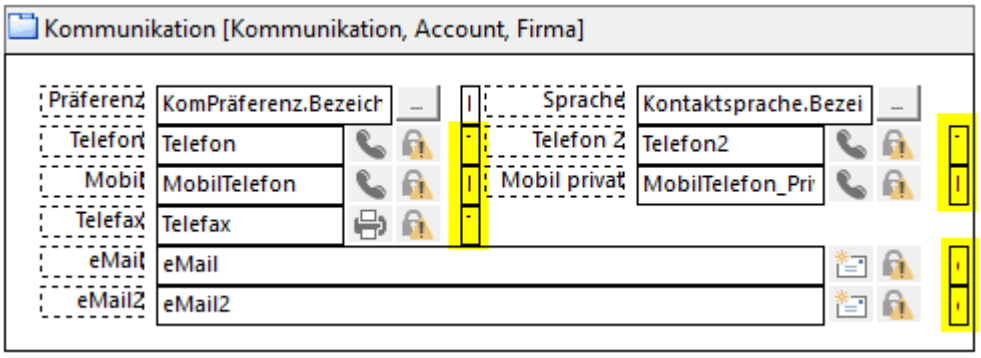
3. Öffnen Sie in der zweiten combit Relationship Manager Instanz die Ansicht "Kontakte_DSGVO" im Eingabemaskendesigner.
4. Markieren Sie nun oben rechts im Reiter "Kommunikation" alle Elemente außer den beiden oberen Feldern "Präferenz" und "Sprache" und kopieren diese.

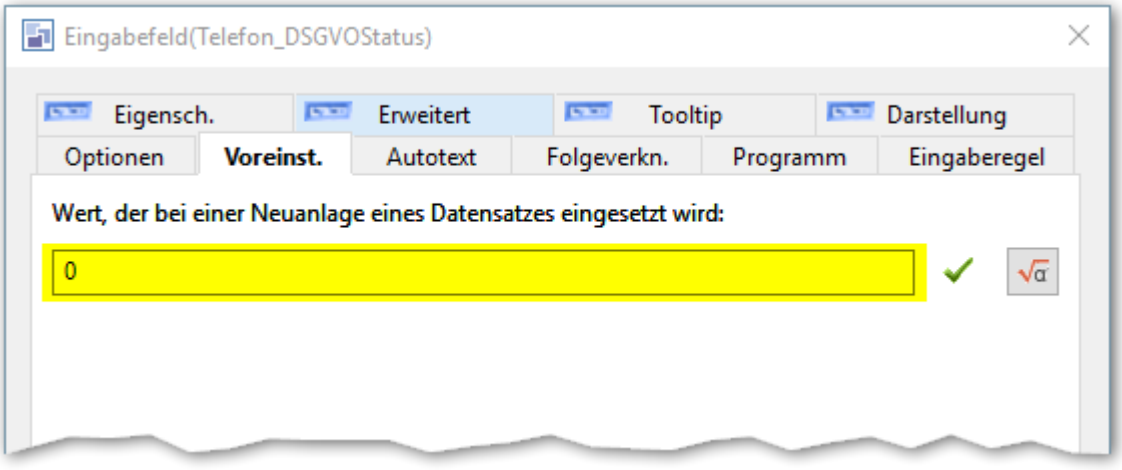


5. Fügen Sie diese nun in der Ansicht "Kontakte" an die Stelle der zuvor gelöschten Elemente ein (STR+V).



8. Ziehen Sie nun noch die Voreinstellung für die in der Abbildung markierten Eingabefelder wie folgt nach:





9. Speichern Sie und Schließen anschließend den Eingabemaskendesigner.

Hintergrundinformation: Die einzelnen Symbole für den jeweiligen Status sind bereits so angelegt, dass sich diese überlagern. Nicht überlagert und wenn diese auseinandergezogen werden, sieht dies folgendermaßen aus:

Export-Aktionen protokollieren

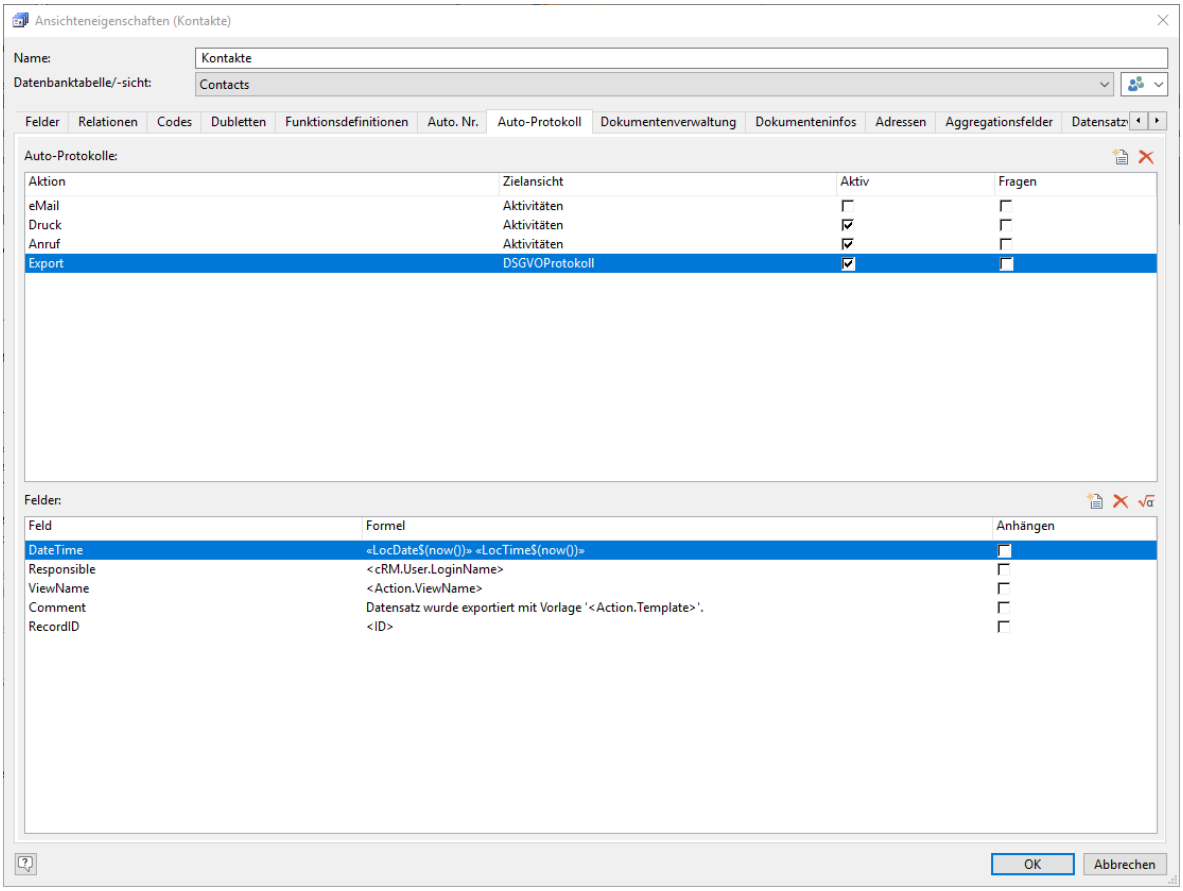
Die Auto-Protokoll-Funktion im combit Relationship Manager war schon immer ein starkes und bei unseren Kunden beliebtes Feature. Damit können Sie selbst beliebige Auto-Protokoll-Aufgaben im combit Relationship Manager definieren und frei über die Oberfläche einstellen.

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.

Ansichten Kontakte und Kampagnenzuordnungen

1. Öffnen Sie die Ansichteneigenschaften der Ansicht "Kontakte" über "Rechtsklick > Eigenschaften" in der Projektnavigation.
2. Legen Sie im Reiter "Auto-Protokoll" über die Schaltfläche "Neu" ein neues Auto-Protokoll für die Aktion "Export" an. Wählen Sie in der Spalte Zielansicht "DSGVOProtokoll". Stellen Sie sicher, dass das Häkchen bei "Aktiv" gesetzt ist.



3. Im Bereich "Felder" und "Formel" wählen und fügen Sie folgende Einträge ein:

DateTime	«LocDate$(now())» «LocTime$(now())»
Responsible	<cRM.User.LoginName>
ViewName	<Action.ViewName>
Comment	Datensatz wurde exportiert mit Vorlage '<Action.Template>'.
RecordID	<ID>

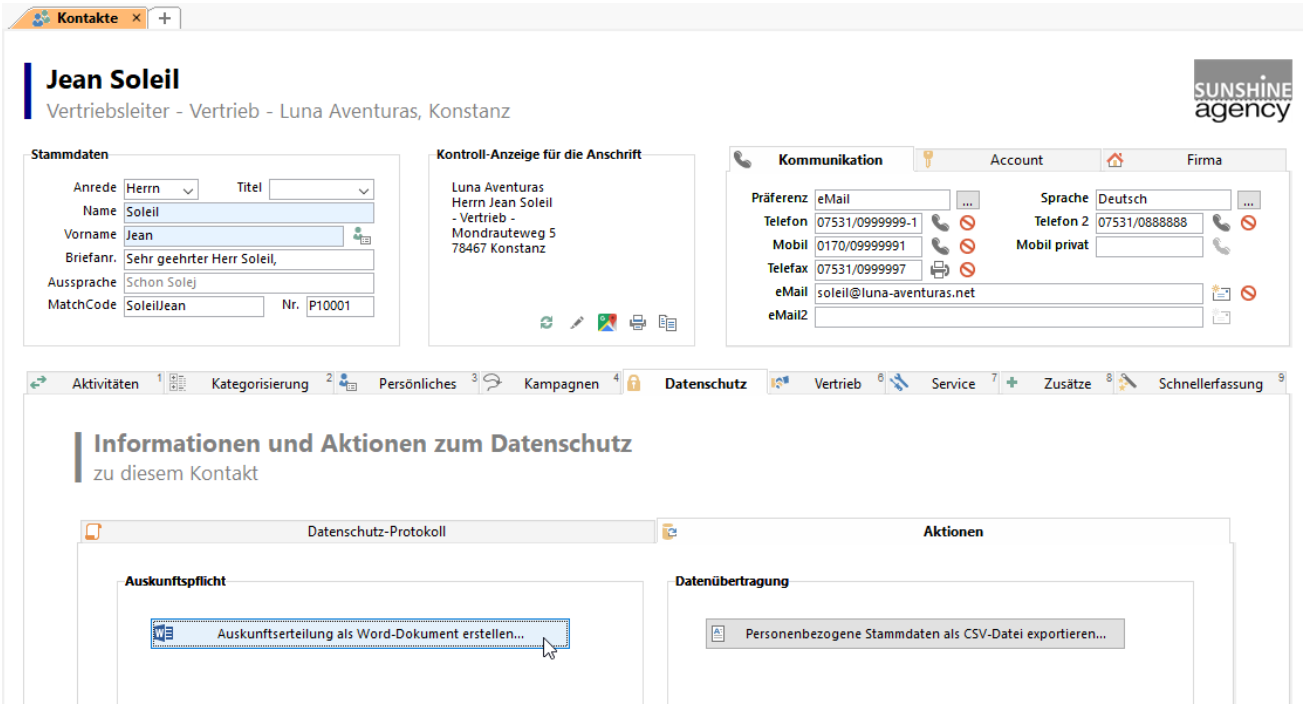
4. Schließen Sie die Ansichteneigenschaften mit "OK".
5. Wiederholen Sie die Schritte 1-5 für die Ansicht "Kampagnenzuordnungen".
6. Speichern Sie das Projekt über "DATEI > Speichern".

Auskünfte erteilen

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 combit 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.

Diese Funktion steht Ihnen durch die zuvor in Ihrer Kontakte-Ansicht angelegte Registerkarte "Datenschutz" im Reiter "Aktionen" zur Verfügung.



Prüfen Sie diese Druckvorlage im Druckvorlagen-Designer vor der ersten Verwendung.

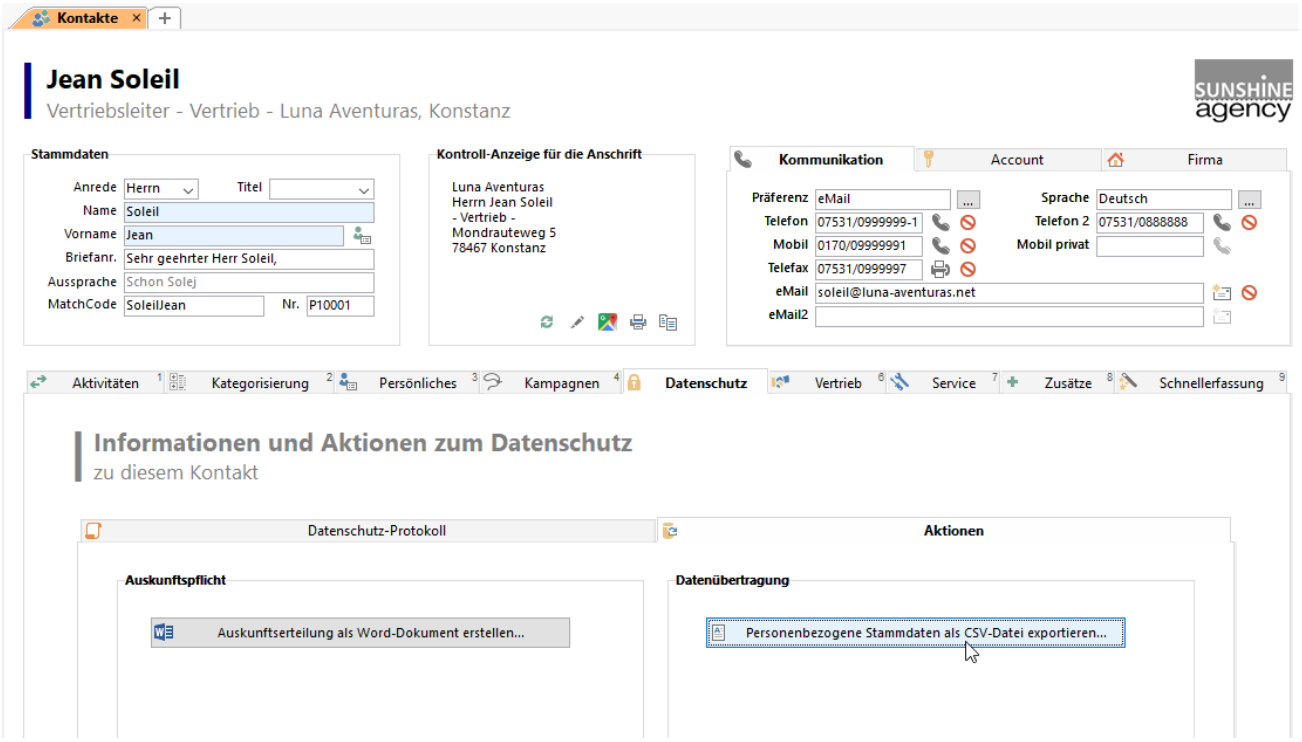
1. Öffnen Sie dazu die Ansicht "Kontakte".
2. Öffnen Sie nun die Druckvorlage "Kontakte - Auskunftserteilung nach DSGVO.lst" über "KONFIGURIEREN > Vorlagen > Listen/Berichte" im Druckvorlagen-Designer.
3. Prüfen Sie nun, ob die dort verwendeten Felder und Container vorhanden sind und drucken Sie den Bericht einmal auf die Vorschau. Passen Sie ggf. Felder an oder löschen diese aus der Druckvorlage.
4. Sobald der Bericht fehlerfrei auf die Vorschau gedruckt werden kann, können Sie diese kontrollieren und ggf. nachbearbeiten. Speichern Sie anschließend den Bericht und schließen den Druckvorlagen-Designer.

Daten übertragen

Mit einem simplen Klick auf die entsprechende Schaltfläche wird direkt eine in der globalen Exportvorlage "Kontakte - Datenübertragung nach DSGVO" hinterlegte Auswahl an Stammdaten-Feldern für den

aktuellen Kontakt als CSV-Datei erzeugt. Machen Sie diese DSGVO-Standard-Export-Vorlage zu Ihrer eigenen Export-Vorlage. Sie können diese Vorlage entweder 1:1 verwenden oder an Ihre individuellen Felder anpassen.

Auch diese Funktion steht Ihnen durch die zuvor in Ihrer Kontakte-Ansicht angelegte Registerkarte "Datenschutz" im Reiter "Aktionen" zur Verfügung.



Öffnen Sie den Assistenten für den Daten-Export über "DATEN > Exportieren" und wählen Sie die Exporvorlage "Globale Vorlagen > Kontakte - Datenübertragung nach DSGVO" um diese CSV-Datei an Ihre Anforderungen anzupassen. Alle weiteren Informationen hierzu finden Sie im combit Relationship Manager Handbuch im Kapitel "Export von Daten".

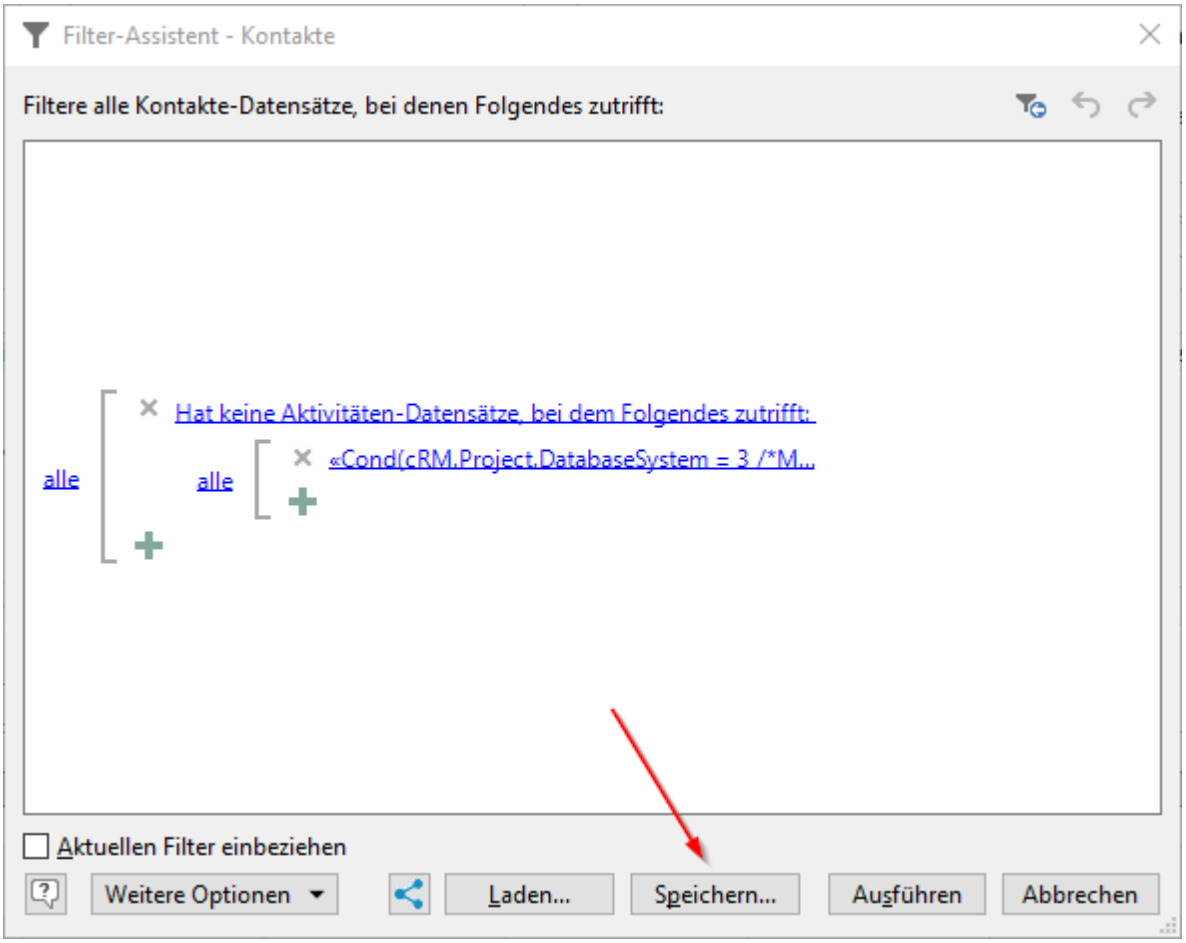
Löschfristen einhalten

Für personenbezogene Daten ist mit der Ansicht "DSGVOCenter" ein Löschkonzept implementiert. Zu Ihren eigenen Verarbeitungstätigkeiten lässt sich direkt eine über unseren mächtigen Filter-Assistenten frei definierbare Löschfrist hinterlegen.

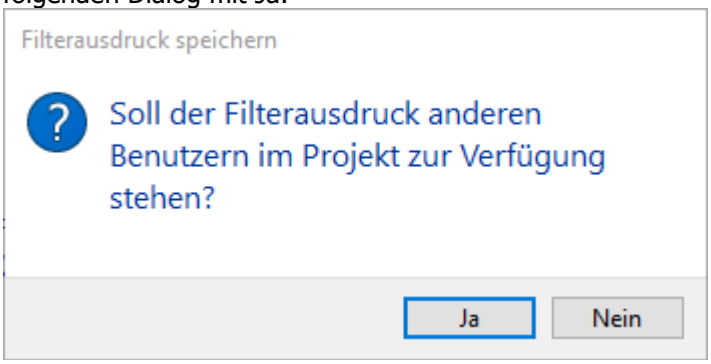
Filter setzen

Übertragen und erstellen Sie sich nun für Ihre Kontakte-Ansicht die wichtigen Filter für Ihr Löschkonzept.

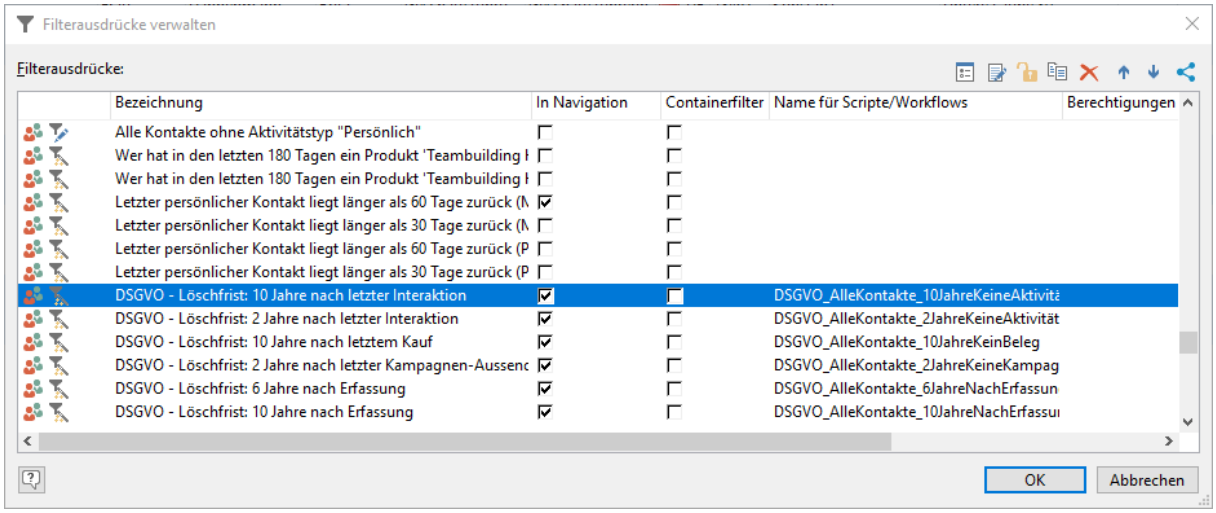
1. Wechseln Sie im Windows Explorer in das "Large_DSGVO" Verzeichnis.
2. Doppelklicken Sie den ersten als .crx Datei mit dem Präfix "DSGVO" mitgelieferten Filter.
3. Es öffnet sich der Filter-Assistent. Klicken Sie nun auf Speichern.



4. Wenn dieser Filter anderen Benutzern auch zur Verfügung stehen soll, beantworten Sie den folgenden Dialog mit Ja.



5. Bestätigen Sie den "Filterausdruck speichern" Dialog mit "OK".
6. Bestätigen Sie den Filter-Assistent Dialog mit "Schließen".
7. Wiederholen Sie die Schritte 2-6 bis Sie am Ende alle 7 Filter übernommen haben.
8. Speichern Sie das Projekt über "DATEI > Speichern" ab.

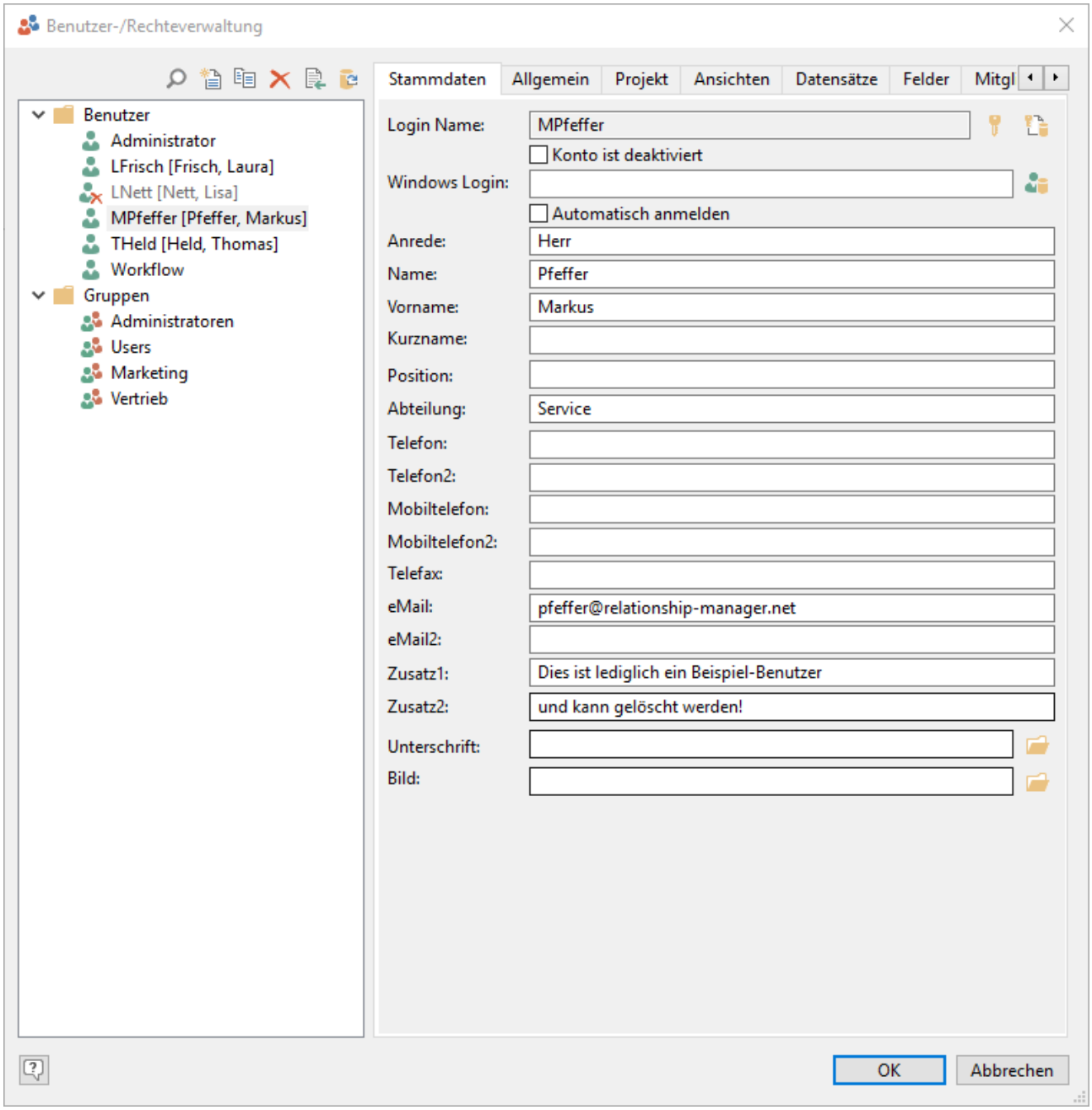


Zugriff autorisieren und Daten einschränken

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.

Über den Menüpunkt "DATEI > Optionen > Benutzerverwaltung" gelangen Sie in die Benutzer- und Rechteverwaltung. Legen Sie hier die verschiedenen Benutzer fest und definieren Sie die jeweiligen Rechte. Alle weiteren Informationen zur Benutzer- und Rechteverwaltung finden Sie im Handbuch im Kapitel "Benutzer- und Rechteverwaltung".



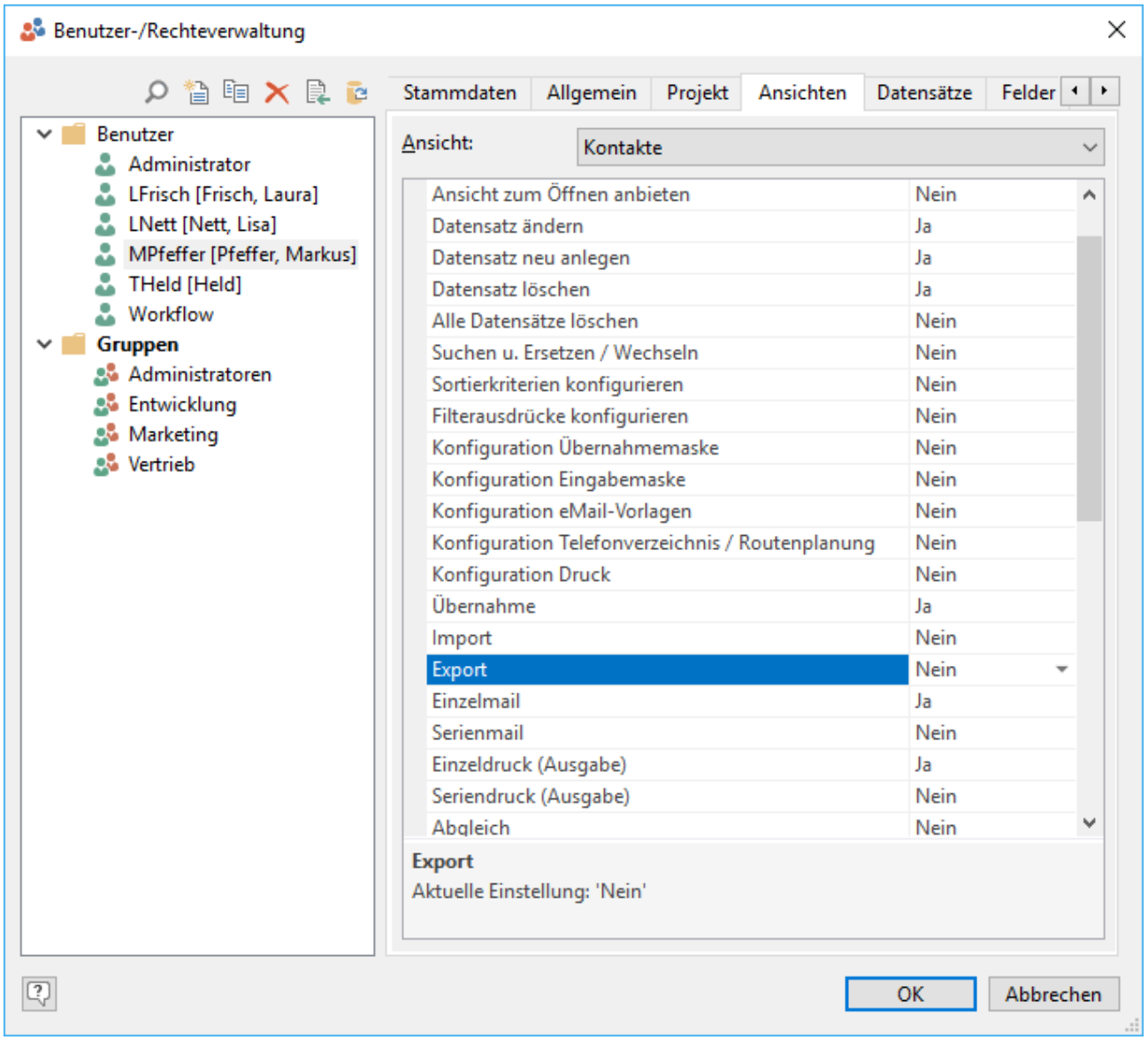
Der combit Relationship Manager hat eine sehr ausgeklügelte und granulare Benutzerverwaltung. Sie haben hier die Möglichkeit, für einzelne Benutzer oder ganze Gruppen u. a. das Folgende freizugeben oder ganz zu sperren:

- 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.



Abschließende Schritte

1. Löschen Sie die Ansichten "Kontakte_DSGVO", "Kampagnen_DSGVO" und "Kampagnenzuordungen_DSGVO" über Rechtsklick auf die Ansicht in der Projektnavigation und Auswahl von "Löschen".
2. Erzeugen Sie für die Sortierungen in den Ansichten "Kontakte" und "Kampagnen" jeweils die Datenbank-Indizes neu. Wählen Sie dazu "KONFIGURIEREN > Sortierungen" und klicken die Schaltfläche oben rechts an. Beenden Sie den Dialog nun mit "OK".
3. Aktualisieren Sie die DSGVO-Protokollierung für die erste Verwendung. Öffnen Sie dazu die Ansicht "DSGVOCenter" und betätigen Sie die Schaltfläche "DSGVO Protokollierung aktualisieren...".
4. Setzen Sie in der Benutzerverwaltung die Berechtigungen für die Sperrliste.

combit GmbH Bücklestr. 3-5 78467 Konstanz Deutschland

combit.net