Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen

Besteller/Vertragspartner/Lizenzierter Nutzer der C&S CareWare

.....

.....

- Verantwortlicher - nachstehend **Auftraggeber** genannt -

und

Firmenverbund C&S AG und der C&S Computer und Software GmbH

86153 Augsburg, Wolfsgäßchen 1

- Auftragsverarbeiter - nachstehend **Auftragnehmer** genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Überprüfung Dateneingabe, Einweisung in die Bedienung Software oder Hotline Service, dieser umfasst die Behandlung, nicht notwendigerweise die Behebung von Störungen oder kleineren Fehlern per Telefon oder mittels Mailbeantwortung oder per Fernwartung.

(2) Dauer

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit der vereinbarten Frist gemäß den Festlegungen aus dem Vertrag Allgemeine Pflegebedingungen für Softwareprogramme der C&S AG gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben im Vertrag Allgemeine Pflegebedingungen für Softwareprogramme der C&S AG.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

☒ Personenstammdaten
☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
☒ Kundenhistorie
☒ Vertragsabrechnungs- und Zahlungsdaten
☒ Planungs- und Steuerungsdaten
☒ Pflegedokumentationsdaten und medizinische Daten
☒ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☒ Kunden
☒ Interessenten
☒ Bewohner, Patienten, Klienten
☒ Beschäftigte
☒ Lieferanten und Dienstleister, Ärzte, Apotheken, gesetzliche Betreuer
☒ Ansprechpartner, Angehörige
☒ Externe Dienstleister des Auftraggebers

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].
(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Daten Portabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.
   Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen,

Post-/Transportdienstleistungen, Wartung und Benutzerservice oder sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung	Vertragsbezug/vertragliche Grundlage
basis software GmbH	28355 Bremen, Ludwig-Sütterlin-Str. 5	Hotline für das Softwareprodukt WinLine (Hersteller: mesonic Datenverarbeitung GmbH)	Softwarebetreuungsvertrag mit Auftragnehmer für WinLine
Microsoft Deutschland GmbH	80807 München, Walter-Gropius-Straße 5	Cloud-Computing-Dienste	Microsoft Azure Mircosoft Office 365 und dynamics

b) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
   - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
   - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
   - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

☒ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) -entfällt-

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Sonstiges

Diese Vereinbarung unterliegt Anpassungen. Die jeweils aktuelle Version ist auf unserer Webseite *managingcare.de* veröffentlicht. Die Vereinbarung kann heruntergeladen und unterzeichnet werden.
Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen der Vereinbarung nicht.

Augsburg, 24.02.2020 *Ort, Datum .....*

Bruno Ristok *Vorname Name Unterschrift*
Vorstandsvorsitzender
C&S AG

Bruno Ristok
Geschäftsführer
C&S Computer und Software GmbH

Anlage 1 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

  - Automatisches Zugangskontrollsystem
  - Chipkarten-/Transponder- oder manuelles Schließsystem
  - Sicherheitsschlösser
  - Schlüsselregelung
  - Personenkontrolle Empfang
  - Protokollierung der Besucher
  - Sorgfältige Auswahl von Reinigungspersonal
  - Tragepflicht von Besucherausweisen

- **Zugangskontrolle**
  Keine unbefugte Systembenutzung

  - Zuordnung von Benutzerrechten
  - Erstellen von Benutzerprofilen
  - Passwortvergabe
  - Authentifikation mit Benutzername / Passwort
  - Zuordnung von Benutzerprofilen zu IT-Systemen
  - Einsatz von VPN-Technologie
  - Sperren von externen Schnittstellen (USB)
  - Schlüsselregelung
  - Sorgfältige Auswahl von Reinigungspersonal
  - Tragepflicht von Besucherausweisen
  - Einsatz von Intrusion-Detection-Systemen
  - Einsatz von Anti-Viren-Software
  - Einsatz einer Hardware-Firewall
  - Einsatz einer Software-Firewall bei allen mobilen Arbeitsplätzen

- **Zugriffskontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

  - Erstellen eines Berechtigungskonzepts
  - Verwaltung der Rechte durch Systemadministrator
  - Anzahl der Administratoren auf das „Notwendigste“ reduziert
  - Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
  - Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
  - sichere Aufbewahrung von Datenträgern
  - physische Löschung von Datenträgern vor Wiederverwendung
  - ordnungsgemäße Vernichtung von Datenträgern
  - Einsatz von Aktenvernichtern bzw. Dienstleistern
  - Protokollierung der Vernichtung, wenn vorgeschrieben

- **Trennungskontrolle**
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

  - physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
  - logische Mandantentrennung (softwareseitig)
  - Erstellung eines Berechtigungskonzepts
  - Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
  - Versehen der Datensätze mit Zweckattributen/Datenfeldern

- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

- **Pseudonymisierung** (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- sichere Transportbehälter/-verpackungen

- **Eingabekontrolle**
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

- Unterbrechungsfreie Stromversorgung (USV)
- Klimatisierung in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management (IT Störungsmanagement);
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

  - Datenschutz Management nach EU DSGVO
  - Incident-Response-Management (IT Störungsmanagement)
  - Notfallplan
  - Datenschutzfreundliche Voreinstellungen
  - Berechtigungskonzept
  - Löschbarkeit von Daten
  - Überprüfung des Auftragnehmers und seiner Tätigkeiten
  - Wirksame Kontrollrechte

Anlage 2 Übersicht von Verarbeitungstätigkeiten Auftragsverarbeiter als Ergänzung zur Vereinbarung

Übersicht von Verarbeitungstätigkeiten Auftragsverarbeiter	001b
Angaben zum Auftragsverarbeiter	
Firmengruppe	☒ ja ☐ nein
Name	C&S AG
Straße	Wolfsgäßchen 1
PLZ	86153
Ort	Augsburg
Telefon	+49 821 25 82-0
E-Mail	info(at)cs-ag.de
Internet-Adresse	---
Angaben zu ggf. einem weiteren gemeinsamen Auftragsverarbeiter	
Name	C&S Computer und Software GmbH
Straße	Wolfsgäßchen 1
PLZ	86153
Ort	Augsburg
Telefon	+49 821 25 82-0
E-Mail	www.managingcare.de
Angaben zum Vertreter des Auftragsverarbeiters	
Name, Vorname	Ristok, Bruno
Straße	Wolfsgäßchen 1
PLZ	86153
Ort	Augsburg
Telefon	+49 821 25 82-0
E-Mail	brunoristok(at)cs-ag.de
Angaben zur Person des Datenschutzbeauftragten	
Anrede	Herr
Name, Vorname	Rautenberg, René
Anschrift	C&S Computer und Software GmbH c/o René Rautenberg
Straße	Wolfsgäßchen 1
PLZ	86153
Ort	Augsburg
E-Mail	info(at)cs-ag.de
Angaben zum Datenschutzkoordinator innerhalb C&S	
Anrede	Herr
Name, Vorname	Backhaus, Hagen
Straße	Wolfsgäßchen 1
PLZ	86153
Ort	Augsburg
Telefon	+49 821 25 82-0
E-Mail	info(at)cs-ag.de
Datum Einführung und letzte Änderung	
Datum Einführung: **18.05.2018**	Datum der letzten Änderung: 25.02.2019
Kategorien von Verarbeitungen, die im Auftrag durchgeführt werden	
C&S führt ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO. Gegenstand ist die Entwicklung, die Wartung und der Vertrieb von Softwareprodukten der Sozialwirtschaft sowie damit im Zusammenhang stehender Dienstleistungen (Vertrieb und	

<table>
<tr><td colspan="2">Verkauf, Kundenbetreuung, Marketing, Pflege der Softwareprodukte und entsprechender Dienstleistungen zur Vertragserfüllung). Die Datenerhebung, -verarbeitung und -nutzung erfolgt zur Ausführung der vorgenannten Zwecke. Die Zweckbestimmung umfasst die Abwicklung und Durchführung von Verträgen im Zusammenhang mit Vertrieb, Verkauf und Produktbetreuung der Vertragssoftware (Schulung vor Ort oder online, Installation und Fehlerbehebung vor Ort oder online per Fernwartung und Dienstleistungen zur Softwareeinführung (Organisationsberatung, Parametrisierung und Installation der Vertragssoftware mit User-Einweisung vor Ort oder online per Fernwartung. Die Datenverarbeitung von personenbezogenen Daten erfolgt für eigene Zwecke der Nachweisführung/Dokumentation und zum Zwecke der Vertragsdurchführung.
○ Hotline Support
○ Fehlersuche
○ Softwareinstallation und Patch
○ Softwarewartung
○ Fehlersuche
○ Schulung</td></tr>
<tr><td colspan="2">Kirchendatenschutz
Wir erfüllen die Auflagen der kirchlichen Datenschutzgesetze gem.
○ §31 des Gesetzes über den Kirchlichen Datenschutz (KDG) des Verbandes der Diözesen Deutschlands und
○ § 30 Absatz 5 Satz 3 Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD) - Unterwerfung erstreckt sich auf die Aufgaben und Befugnisse der kirchlichen Datenschutzaufsicht nach §§ 43, 44 EKD-Datenschutzgesetz.</td></tr>
<tr><td>Übermittlung von personenbezogenen Daten an Drittland oder eine internationale Organisation</td><td>☐ Datenübermittlung findet nicht statt und ist auch nicht geplant
☒ Datenübermittlung findet wie folgt statt
C&S übermittelt grundsätzlich keine Kunden- und Mitarbeiterdaten in Drittländer. Allerdings ist eine Übermittlung von personenbezogenen Daten in ein Drittland auch beim Einsatz von Microsoft Office 365 und Microsoft Dynamics 365 gegeben. Wir nutzen die europäische Lösung, hier werden die Daten nach Irland und in die Niederlande übertragen und per Fernzugriffsrechte in die USA transferiert, sodass ein Datentransfer in Drittländer vorliegt.

☒ Drittland oder internationale Organisation (Name):
Microsoft - USA
☒Dokumentation geeigneter Garantien:
○ EU-Standardvertragsklauseln
○ EU-US Privacy Shield (Angemessenheitsbeschluss EU 2016/1250) vom 12. Juli 2016
○ Vereinbarung Auftragsverarbeitung mit Microsoft https://www.managing-care.de/wp-content/uploads/2018/07/ADV_MircosoftOnlineServiceTermsGerman_CUNDSJuly2018.pdf
○ Trust Center Microsoft unter https://products.office.com/de-de/business/office-365-trust-center-top-10-trust-tenets-cloud-security-and-privacy</td></tr>
</table>

Technische und Organisatorische Maßnahmen (TOM) gem. Art. 32 DS-GVO	siehe TOM Beschreibung in der Anlage 1 zur Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO in digitaler Form unter http://www.managing-care.de/agb/ An diese dort in der jeweils aktuellen Veröffentlichung der TOM halten wir uns gebunden.
Rechte als Betroffener	Sie haben die Rechte aus den Art. 15 – 22 DS-GVO: – Recht auf Auskunft (Art. 15 DS-GVO) – Recht auf Berichtigung (Art. 16 DS-GVO) – Recht auf Löschung (Art. 17 DS-GVO) – Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) – Widerspruchsrecht gegen die Verarbeitung (Art. 21) – Recht auf Datenübertragbarkeit (Art. 20 DS-GVO) Wenden Sie sich hierzu an die vorgenannten Verantwortlichen.
Zuständige Datenschutzbehörde/Aufsichtsbehörde	Die für uns zuständige Datenschutzaufsichtsbehörde ist: Bayerisches Landesamt für Datenschutzaufsicht 91522 Ansbach, Promenade 27 Telefon: 0981 53-1300 Telefax: 0981 53-5300 E-Mail: poststelle@lda.bayern.de Homepage: http://www.lda.bayern.de

Anlage 3 Änderungsübersicht

Version	Datum	Grund	Beschreibung der Änderung	Bearbeiter
1.0	27.03.2018	Veröffentlichung		hb
1.1	27.03.2018	Änderung bei Unterauftragnehmer	Fa. Comramo gelöscht	hb
2.0	22.05.2018	Vertragspartner Unterauftragnehmer 6 (1) und 6 (2) Kontrollrechte des Auftraggebers 7 (4) Anlage 2 Übersicht von Verarbeitungstätigkeiten Auftragsverarbeiter Anlage 3 Änderungsübersicht	Titelblatt C&S AG hinzugefügt gelöscht wurde: „oder die Entsorgung von Datenträgern“ gelöscht wurde: „Comramo …“ gelöscht wurde der gesamte Punkt 7 (4): „Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen“ Anlage hinzugefügt mit Nennung der Verantwortlichen und DSB etc. Anlage hinzugefügt zum Nachweis von Änderungen (Historie)	hb
3.0	13.06.2018	11 Sonstiges NEUER Absatz Anlage 2 Aktualisierung Anlage 2 Neu Anlage 2 Ergänzung Anlage 2 Neu Anlage 2 Änderung	Es gilt immer die jeweils auf der Website managingcare.de veröffentlichte Version dieser Vereinbarung. - Angaben zur Person Datenschutzbeauftragter der C&S GmbH aktualisiert- Datum Einführung und Änderung hinzugefügt als Rubrik Ergänzung am Beginn unter **Kategorien von Verarbeitungen, die im Auftrag durchgeführt werden**: „C&S führt ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO.“ Festlegungen zu den Kirchendatenschutzgesetzen Übermittlung von personenbezogenen Daten an Drittland oder eine internationale Organisation wurde aktiviert	hb
3.1	11.07.2018	Deckblatt (Seite 1) 3. TOM, Punkt (2) Änderung	2 Zeilen für handschriftlichen Eintrag Firma eingefügt nach „Besteller/Vertragspartner/Lizenzierter Nutzer der C&S CareWare“	hb

		Nach 11 Sonstiges (Seite 6) Neu Anlage 2 Ergänzung	Anlage 1. 1 wurde geändert in Anlage 1 Unterschrift Verantwortlicher C&S (Sie können damit die Vereinbarung ausdrucken, unterzeichnen und ablegen) Übermittlung von personenbezogenen Daten an Drittland oder eine internationale Organisation: ergänzt wurde Link zur Anzeige der Auftragsverarbeitungsvereinbarung mit Microsoft	
3.2	25.02.2019	Anlage 2, Seite 10: Besetzung Funktionsstelle Datenschutzkoordinator Anlage 2, Datum der letzten Änderung aktualisiert Global: Fußzeile links, Version aktualisert Seite 6 Unterschriftenabschnitt, Monat und Jahr aktualisiert	Datenschutzkoordinator gelöscht wurde der Eintrag: Benedikt Ristok und ersetzt durch: Hagen Backhaus Gelöscht wurde 11.07.2018 und aktualisiert auf 25.02.2019 Gelöscht wurde Version 3.1 vom 13.07.2018 und aktualisiert auf: Version 3.2 vom 25.02.2019 Gelöscht: Juli 2018 und aktualisiert auf: Februar 2019	
3.3	08.10.2019	Seite 5, Punkt 8 (2) Seite 6, Unterschriftenabschnitt links, Tag, Monat, Jahr aktualisiert Fußzeile links	Ergänzung #angemessene#, nun NEU: (2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung beanspruchen. Gelöscht: Februar und aktualisiert auf: 08.Oktober 2019 Gelöscht: 3.2 vom 25.02.2019 und aktualisiert auf: 3.3 vom 08.10.2019	
3.4	20.02.2020	7 (3) abgewählt wurden:	☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO; ☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).	DRAFT

		11 Sonstiges löschen und Neueintrag Unterschriftenabschnitt, Monat und Jahr aktualisiert Unterschriften erweitert/ergänzt Fußzeile links	Diese Vereinbarung unterliegt Anpassungen. Die jeweils aktuelle Version ist auf unserer Webseite *managingcare.de* veröffentlicht. Die Vereinbarung kann heruntergeladen und unterzeichnet werden. ~~Es gilt immer die jeweils auf der Website managingcare.de veröffentlichte Version dieser Vereinbarung~~. Gelöscht: 08.Oktober 2019, neu 20.02.2020 Bruno Ristok, Vorstandsvorsitzender C&S AG Bruno Ristok, Geschäftsführer C&S Computer und Software GmbH Gelöscht: 3.3 vom 08.10.2019 und aktualisiert auf: 3.4 vom 20.02.2020	
3.5	24.02.2020	6 (2) Unterauftragsverhältnisse Unterschriftenabschnitt, Tag aktualisiert	Ergänzt wurde: Microsoft mit seinen Coud-Diensten 24.02.2020	