euregon®

Vertrag über Auftragsverarbeitung i. S. d. Art. 28 DSGVO

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem Vertrag zur Softwareüberlassung, Softwarebetreuung und/oder über Hostingleistungen bzw. Online-Services ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit den Leistungen der euregon AG, Walchstr. 2, 86157 Augsburg (nachfolgend „Auftragnehmer") in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Für Einrichtungen in kirchlicher Trägerschaft - bzw. in der Trägerschaft von Caritas oder Diakonie - werden die Anforderungen des kirchlichen Datenschutzes nach DSG-EKD 2018 (evangelische/diakonische Träger) bzw. KDG (katholische Träger und Caritas) berücksichtigt.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsdatenverarbeitung

Der Vertragsumfang und die Geltungsdauer sowie Umfang und Art der Datenverarbeitung werden durch die zugrunde liegenden Verträge zwischen und Auftraggeber festgelegt. .

Zweck der Verarbeitung nach Art. 4 Abs. 1 DSGVO :

- Bei Verträgen zur Softwareüberlassung (Kauf oder Miete) oder zur Softwarebetreuung die Softwarebetreuung und –unterstützung von Mitarbeitern des Auftraggebers sowie Analyse und Behebung von Fehlerzuständen der Software mittels Telefon, Fernwartung und Datenbankkopien des Auftraggebers.
- Bei Verträgen zum Hosting zusätzlich die Bereitstellung und den Betrieb eines vollständigen Datenverarbeitungssystems (Server und Terminalserver/Client) zur Nutzung der vertraglich vereinbarten Software des Auftragnehmers.
- Bei Verträgen zur Softwareüberlassung und Softwarebetreuung für Produkte die Online-Services beinhalten (d.h. insbesondere .snap MDA, .snap Assist, .snap Home…) die Bereitstellung und den Betrieb der zentralen Serverkomponente für diese Softwareprodukte.

Im Zuge der Leistungserbringung kann ein Zugriff auf personenbezogene Daten durch den Auftragnehmer nicht ausgeschlossen werden. 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 Art. 44 ff. DS-GVO erfüllt sind.

Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung

Kategorien von betroffenen Personen	Daten oder Datenkategorien
Klienten des Auftraggebers	Anschrifts-/Kontaktdaten, Persönliche Informationen, Bezugspersonen, Religionsdaten, Gesundheitsdaten, Angaben über pflegerischen/medizinischen Zustand und Diagnosen, erbrachte Leistungen, Leistungsträger, Ärzte, Sonstige Dienstleister, Rechnungslegung, Kontakthistorie und Dokumente für .snap PPC/PPS zusätzlich: Anamnesedaten; Pflegeplanung und –dokumentation, Pflegeberichte und ergänzende Dokumentation
Bezugspersonen des Klienten	Anschrifts-/Kontaktdaten, Verwandtschaftsgrad
Ärzte	Anschrifts-/Kontaktdaten, Verwaltungsdaten
Mitarbeiter des Auftraggebers	Anschrifts-/Kontaktdaten, Angaben zu Ausbildung/Qualifikation, Angaben zum Beschäftigungsverhältnis, Dienst- und Einsatzplan Arbeitszeiterfassung und –auswertung, Dokumente Supportfälle und Teilnahmen an Schulungen/Veranstaltungen

Dienstleister und deren Ansprechpartner	Anschrifts-/Kontaktdaten, Kontakthistorie

Empfänger, denen die Daten mitgeteilt werden können, sind Mitarbeiter in den Bereichen Support/Kundenbetreuung und Softwareentwicklung des Auftragnehmers.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer erbringt im Auftrag des Auftraggebers Supportdienstleistungen im Rahmen der zugrundeliegenden Verträge. Zusätzlich erbringt er je nach Beauftragung weitere Leistungen wie Hostingleistungen, das Einspielen von Updates, Anpassung von Datenbanken oder die Bereitstellung von Onlinediensten. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis von diesen erlangt. Nach Art. 28 DS-GVO ist daher der Abschluss einer Vereinbarung zur Verarbeitung im Auftrag erforderlich.

(2) Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 DSGVO als Dienstleister ausgewählt. Er regelt mit diesem Vertrag zur Auftragsverarbeitung i.S. d. Art. 28 Abs. 3 DSGVO die Rechte und Pflichten der Parteien zum Datenschutz im Zusammenhang mit der Erbringung von Supportdienstleistungen.

(3) Der Auftraggeber ist im Rahmen der Auftragsdatenverarbeitung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie die Rechtmäßigkeit der Datenverarbeitung primär verantwortlich („verantwortliche Stelle" im Sinne des § 3 Abs. 7 BDSG).

§ 3 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 zur Erledigung durch diesen weiterleiten.

(2) Die Umsetzung der Rechte auf Löschung, Berichtigung, Datenübertragbarkeit und Auskunft sind nur nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

(3) 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 oder aufgrund gerichtlicher oder behördlicher Anordnung erforderlich sind.

(4) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber - spätestens jedoch mit Beendigung der Leistungsvereinbarung - hat der Auftragnehmer nach Wahl des Auftraggebers sämtliche Daten, die unter die DSGVO fallen zurückzugeben oder diese zu löschen, sofern nicht andere Rechtspflichten entgegenstehen.

(5) 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.

§ 4 Pflichten des Auftragnehmers

(1) Eine Verarbeitung personenbezogener Daten, die sich nicht auf die Erbringung von Supportdienstleistungen im Rahmen der zugrundeliegenden Verträge bezieht, ist dem Auftragnehmer untersagt. Dies gilt je nach Auftragsumfang auch für die Hosting- oder Onlinedienstleistungen. Es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer bestätigt, dass er - soweit dieser gesetzlich dazu verpflichtet ist - einen betrieblichen Datenschutzbeauftragten i.S. d. Art. 38, 39 DS-GVO bestellt hat.
Als Datenschutzbeauftragter ist beim Auftragnehmer bestellt:
Herr Rico Bautsch
Walchstr. 2, 86157 Augsburg
dsb@euregon.de
Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

(4) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz Grundverordnung (Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Der Auftragnehmer hat die erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung dokumentiert (insbes. Anlage A) und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz/Beauftragung durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung oder ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen und zu dokumentieren.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten des Auftraggebers.

(6) Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete personenbezogene Daten einer Verletzung des gesetzlichen Schutzes personenbezogener Daten gem. Art. 33 DS-GVO (Datenschutzverstoß bzw. Datenpanne) unterliegen, z.B. indem diese unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls bzw. der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Meldung an den Auftraggeber muss mindestens folgende Informationen enthalten:

a. Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze.

b. Den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen.

c. Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.

d. Eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

(7) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der personenbezogenen Daten des Auftraggebers befassten Mitarbeiter gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO zur Wahrung der Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugriff auf personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in dieser Vereinbarung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Diese Vertraulichkeitsverpflichtung besteht auch nach Beendigung der Tätigkeit fort.

(8) Der Auftragnehmer hat alle Mitarbeiter zur Wahrung des Sozialgeheimnisses (§78 Abs. 1 SGB X) und zur Wahrung des Berufsgeheimnisses (§203 StGB) zu verpflichten.

(9) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.

(10) Des Weiteren verpflichtet sich der Auftragnehmer den Auftraggeber gemäß Art. 28 Abs. 3 lit. f DS-GVO bei der Einhaltung der in Art. 34 - 36 DS-GVO genannten Pflichten zu unterstützen:

a. Im Rahmen seiner Informationspflicht gegenüber den betroffenen Personen und dem Auftraggeber in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

b. Bei der Durchführung seiner Datenschutz-Folgenabschätzung.

c. Im Rahmen einer vorherigen Konsultation mit der Aufsichtsbehörde.

(11) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(12) Der Auftragnehmer hat den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, zu informieren. 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. Eine Information erfolgt nicht, soweit dies gerichtlich oder behördlich untersagt ist.

(13) 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 durch den Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(14) 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.

§ 5 Rechte und Pflichten des Auftraggebers

(1) Jeder Mitarbeiter des Auftraggebers ist im Rahmen des zugrundeliegenden Vertrags zur Unterstützung per Fernwartung durch den Auftragnehmer berechtigt. Die Unterstützung erfolgt unter Aufsicht des Mitarbeiters des Auftraggebers und nur mit dessen Rechten im System.

Einzelweisungen für darüber hinausgehende Aufgaben (Datenbankoperationen, Datenanpassungen per Script, Bearbeitung von Datensicherungen etc.) dürfen nur von der verantwortlichen Person oder weiteren weisungsberechtigten Personen erteilt werden, die der Auftragnehmer schriftlich mitteilt.
(Das Formular hierzu finden Sie unterhttps://www.euregon.de/info/AVV-Nachtrag.pdf)
Weisungen sind in Textform (auch E-Mail, FAX) zu übermitteln – ausnahmsweise mündlich erteilte Weisungen sind unverzüglich in Textform zu bestätigen.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Dem Auftraggeber obliegen die aus Art. 33 Abs. 1 DS-GVO resultierenden Meldepflichten.

(4) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten personenbezogenen Daten nach Beendigung des Auftrages durch Weisung fest.
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.
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.
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

(5) Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

§ 6 Wahrung von Rechten der betroffenen Person

(1) Der Auftraggeber ist für die Wahrung der Rechte der betroffenen Person verantwortlich.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Einschränkung, Datenübertragbarkeit oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

(3) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Löschung oder Einschränkung oder Datenübertragbarkeit seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(4) Entsteht durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer wesentlicher Mehraufwand, so kann der Auftragnehmer hierfür eine angemessene Vergütung verlangen wenn Leistungen erforderlich sind, die
a) nicht nach den Regelungen der DSGVO kostenfrei zu erbringen sind und
b) über den Umfang der vertraglich genutzten Software hinausgehen.

§ 7 Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen sowie die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Abs. 1 erforderlich ist.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Abs. 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, so dass die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht gestört werden.
Der Auftragnehmer darf diese Kontrollen von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich im Rahmen der Prüfung ggf. berührter Betriebs- und Geschäftsgeheimnisse des Auftragnehmers abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(4) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DS-GVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen.

(5) Der Auftragnehmer erbringt den Nachweis technischer und organisatorischer Maßnahmen, die nicht nur den konkreten Auftrag betreffen. Dabei kann dies erfolgen durch:

a. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO.

b. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO.

c. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Datenschutzauditoren.

d. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO27001 oder BSI-Grundschutz).

(6) Werden durch eine Kontrolle entgegen der Regelungen in Abs. 3 Betriebsabläufe gestört oder entsteht nicht nur unwesentlicher Mehraufwand durch Kontrollen, die über den erforderlichen Umfang hinausgehen, so kann der Auftragnehmer hierfür eine angemessene Vergütung verlangen.

§ 8 Unterauftragsverhältnisse

(1) Der Auftragnehmer nimmt für die Erbringung von Hosting-Leistungen im Auftrag des Auftraggebers nur Leistungen von den in Anlage B genannten Dritten in Anspruch, die in seinem Auftrag Daten gem. Art. 28 DS-GVO verarbeiten ("Unterauftragnehmer").

(2) Der Auftraggeber stimmt zu, dass der Auftragnehmer bestehende Subunternehmer wechselt oder weitere Subunternehmer hinzuzieht. Dies ist zulässig, soweit:
• der Auftragnehmer einen solchen Wechsel bzw. eine solche Auslagerung auf Subunternehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform mit dem Termin des geplanten Vertragsbeginns anzeigt und
• der Auftraggeber nicht bis zum Vertragsbeginn des Unterauftragsverhältnisses gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung bzw. den Wechsel erhebt und
• zwischen dem Auftragnehmer und dem Subunternehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 EU-DSGVO zugrunde gelegt wird.

Die Weiterleitung von Daten an einen Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtung nach § 32 EU-DSGVO erfüllt hat.

Wenn der Auftraggeber Einspruch gegen die Beauftragung des Subunternehmers einlegt, was nur aus wichtigem Grund zulässig ist, dieser aber für die Durchführung des Auftrages oder des Produktes erforderlich ist, ist der Auftragnehmer berechtigt, dem Auftraggeber den zugrundeliegenden Vertrag ohne Fristeinhaltung zu kündigen.

(3) Im Falle einer Beauftragung hat der Auftragnehmer den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen

einhalten kann.
Der Auftragnehmer hat insbesondere vorab sicherzustellen, dass der Unterauftragnehmer die nach Art. 28 Abs. 3 lit. c, 32 DS-GVO i.V.m. Art. 5 Abs. 1, Abs. 2 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.
Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen Datenschutzbeauftragten i.S.d. Art. 37-39 DS-GVO bestellt hat.

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(5) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

(6) Ein zustimmungspflichtiges Unterauftragsverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externen Telekommunikations-, Post- und Versanddienstleistungen oder Wartungsarbeiten.
Der Auftragnehmer wird mit diesem Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

§ 9 Sonderregelungen für Einrichtungen in kirchlicher Trägerschaft

Soweit es sich beim Auftraggeber um Einrichtungen in der **Trägerschaft der katholischen Kirche** handelt, so gelten die Regelungen des KDG.
Wird in dieser Vereinbarung incl. Anhang auf die DSGVO Bezug genommen, erfolgt die Bezugnahme entsprechend auf die anwendbare kirchenrechtliche Regelung, die den jeweiligen Vorschriften der DSGVO entspricht. Etwaige Regelungen in dieser Vereinbarung und der Anlage, die zu Gunsten des Auftraggebers über die jeweils anwendbaren kirchenrechtlichen Regelungen hinausgehen, bleiben zu Gunsten des Auftraggebers hiervon unberührt.
Hinsichtlich von Einrichtungen in der Trägerschaft der katholischen Kirche finden insbesondere die kirchenrechtlichen Vorschriften zur Auftragsdatenverarbeitung nach § 29 KDG (Gesetz über den kirchlichen Datenschutz) Anwendung.

Handelt es sich beim Auftraggeber um eine Einrichtung in der **Trägerschaft der evangelischen Kirche** besteht gemäß § 30 Abs. 5 DSG-EKD n.F. die Möglichkeit, Verträge mit Auftragsverarbeitern abzuschließen, auf die die kirchlichen Datenschutzbestimmungen keine Anwendung finden, wenn sich die Inhalte des AV-Vertrages an Artikel 28 Datenschutz-Grundverordnung orientieren. Voraussetzung ist, dass sich der Auftragsverarbeiter der kirchlichen Datenschutzaufsicht unterwirft.
Der Auftragnehmer unterwirft sich der Kontrolle durch den zuständigen kirchlichen Datenschutzbeauftragten gemäß 30 Abs. 5 DSG-EKD.

§ 10 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlichen« im Sinne der DSGVO liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei Unwirksamkeit einer Bestimmung in diesen Vertragsbedingungen bleiben die übrigen Bestimmungen gleichwohl wirksam. Die Vertragsparteien verpflichten sich, eine unwirksame Bestimmung oder eine planwidrig fehlende Bestimmung nach Treu und Glauben durch eine Bestimmung zu ersetzen, die dem gemeinsam verfolgten Zweck der Vertragsparteien am nächsten kommt.

(4) Es gilt deutsches Recht.

Anhang A über technische und organisatorische Maßnahmen nach Art. 32 DSGVO

1) Vertraulichkeit

a) Zutrittskontrolle

Unbefugte Personen haben keinen Zutritt zu den Datenverarbeitungsanlagen. Gäste im Hause sind in sicherheitsrelevanten Bereichen (Entwicklung, Support) stets in Begleitung.

Der Zutritt zum Gebäude und den Büroräumen ist mit einem Schließsystem mit unterschiedlichen Zutrittsbereichen gesichert, welches für befugte Personen nur mit einem elektronisch codierten Schlüssel zugänglich ist. Es existiert ein Schlüsselverzeichnis.

Die zentralen Datenverarbeitungsanlagen (Server) sind in einem separaten verschlossenen Raum. Nur wenige ausgewählte Personen haben hier Zutritt.

Das Gebäude ist weiterhin mit einer Alarmanlage gesichert.

b) Zugangskontrolle

Zugang zu Computern ist nur mit gültigem Benutzerkonto und Passwort gemäß Passwortrichtline möglich.

Organisatorische Regelungen zum Sperren von Computern bei Inaktivität (Screensaver) bzw. Verlassen des Arbeitsplatzes.

Benutzeranmeldung für Zugriff auf Netzwerk zwingend erforderlich.

Einsatz von Firewall und Antivirussoftware.

c) Remote Zugänge nur über verschlüsselte Verbindung möglich. Zugriffskontrolle

Der Zugriff auf die Datenverarbeitungssysteme ist durch eine Nutzer- und

Rechteverwaltung abgesichert.

Zentrale Verwaltung und Festlegung für Zugriffsbefugnisse im Netzwerk und bei Kunden/Supportdaten.

Fernwartung nur unter Aufsicht des Auftraggebers und mit individuellem Zugangscode.

Datenschutzkonforme Vernichtung bzw. Löschung von Datenträgern und vertraulichen Unterlagen:

Optische Datenträger:	Schredder
USB-Stick:	Low-Level Formatierung
Dateien/FTP:	Überschreiben der Datei mit Zufallsdaten und anschließendes Löschen auf Betriebssystemebene

d) Trennungskontrolle

Daten werden entsprechend ihrem Verwendungszweck getrennt gespeichert und verarbeitet.

Eine Vermischung von Daten mit unterschiedlichem Verwendungszweck findet nicht statt.

Trennung von Test- und Produktivsystemen.

e) Verschlüsselung

Verschlüsselte Datenbanken für Kunden und Supportdaten.

2) Integrität

a) Eingabekontrolle

Protokollierung der Nutzer von Kunden/Supportsystem.

Protokollierung von Fernwartungsvorgängen (nur Zeit, Nutzer, Zweck) und Datenaustausch mit dem Auftraggeber.

Protokollierung von kritischen Änderungen von Systemdaten im Systemprotokoll.

b) Weitergabekontrolle

Daten werden nur im privaten Netzwerk bzw. im VPN verarbeitet.

Versand von Daten auf Speichermedien per Post oder verschlüsselt über das Internet.

3) Verfügbarkeit und Belastbarkeit

a) Verfügbarkeitskontrolle

Regelmäßige Datensicherung von Support/Kundendaten (Datensicherung auf externe Festplatten in vom Serverraum getrennten Räumlichkeiten in einem getrennten Brandabschnitt).

Einsatz einer unterbrechungsfreien Stromversorgung für zentrale Serversysteme.

Einsatz von Firewall und Virenscanner.

Automatische Produktupdates für eingesetzte Client-Betriebssysteme.

b) Belastbarkeit der Systeme

Funktions- und Stresstests in sogenannten Staging-Umgebungen (Software-gleiche Umgebung wie die produktive Umgebung).

Kontinuierliches Monitoring der Systeme.

Alerting, wenn fehlerhafter oder anormaler Systemzustand erkannt wird.

4) Weitere Maßnahmenbereiche

a) Auftragskontrolle

Sorgfältige Auswahl von Dienstleistern aufgrund von Standort und Datenschutz-Maßnahmen.

Abschluss von Verträgen zur Auftragsdatenverarbeitung mit allen aufgeführten Subauftragnehmern.

b) Datenschutz Managementsystem

Zentrale Dokumentation aller Verfahrensanweisungen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für alle Mitarbeiter im Intranet.

Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen von Betroffenen ist vorhanden.

Alle Mitarbeiter sind geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet.

Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt.

Anhang B –Verzeichnis der Subunternehmer und Teilleistungen

Beschreibung der Teilleistungen	Name und Anschrift des Subunternehmers
Spamfilter und Virenschutz für eingehende Mails Mailserver für ausgehende Mails	abtis GmbH Wilhelm-Becker-Str. 11b 75179 Pforzheim
Bereitstellung von Produktversionen als Download Up- und Download für Datensicherungen bzw. Datenbanken von Kunden	STRATO AG Pascalstr. 10 10587 Berlin
Bereitstellung von Cloud Services und Hosting von Serverlösungen wie z.B. .snap Assist, .snap MDA, .snap home	1&1 IONOS SE Elgendorfer Str. 57 56410 Montabaur
Bereitstellung von Cloud Services und Hosting von Serverlösungen wie z.B., .snap MDA, .snap home	MD Systec GmbH Fraundorf 9c 84335 Mitterskirchen
Bereitstellung von Cloud Services und Hosting von Serverlösungen wie z.B. .snap MDA, .snap Home	PlusServer GmbH Hohenzollernring 72 50672 Köln
Anzeige und Berechnung von Fahrtrouten in .snap ambulant Tourenvorschläge und Routenoptimierung in .snap Assist	LOGIBALL GmbH Westring 303 44629 Herne
Bereitstellung von Software für die Fernwartung Zentraler Server für die Vermittlung von Fernwartungssitzungen	pcvisit Software AG Manfred-von-Ardenne-Ring 20, D-01099 Dresden
Versand von Newslettern Onlineerfassung von Supportanfragen	Mittwald CM Service GmbH & Co. KG Königsberger Straße 4-6 32339 Espelkamp
Versand von Newslettern	CleverReach GmbH & Co. KG Schafjückenweg 2 26180 Rastede
Versand von Mailings an Kunden	HR Com Tec GmbH Karl-Marx-Str. 16 68199 Mannheim
CRM-ERP Systemsupport	SMC Informationstechnologien AG Koblenzer Str. 2 86157 Augsburg
Helpdesk Hosting	Zendesk Inc. 989 Market Street San Francisco, CA 94103
Helpdesksystemsupport	Leafworks GmbH Travestieg 2 22851 Norderstedt
Optional – nur für Hosting	CONET Services GmbH Theodor-Heuss-Allee 19 53773 Hennef/Sieg
Optional – nur für Hosting	CIS Computer & Internet Services Gesellschaft mbH Daimlerstr. 37 76185 Karlsruhe
Optional – nur für TI Telematikinfrastruktur Anbindung	MEDKONNEKT GmbH Landsberger Str. 155 80687 München