Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO

Muster für das Verhältnis JS Consulting ↔ Lizenznehmerin

zwischen

[Firmenname/Name der Lizenznehmerin], [Anschrift], [ggf. FN/Gewerbeberechtigung] – im Folgenden „**Verantwortliche**" –

und

JS Consulting, Jürgen Spiegel, Parkstraße 18, 8700 Leoben, Österreich – im Folgenden „**Auftragsverarbeiter**" –

im Zusammenhang mit dem Lizenzvertrag über die Software **Betreuungsplaner** bzw. **CareGap** vom [Datum] (im Folgenden „**Lizenzvertrag**").

Präambel

Der Auftragsverarbeiter stellt der Verantwortlichen eine lokal zu betreibende Offline-Software zur Verwaltung von Klienten-/Patientendaten zur Verfügung. Die Software wird **ausschließlich auf Geräten der Verantwortlichen betrieben**; es besteht **keine Cloud-Anbindung und kein Server des Auftragsverarbeiters, über den im Normalbetrieb personenbezogene Daten der Verantwortlichen laufen**.

Die Parteien gehen davon aus, dass **im Regelbetrieb der Software keine Auftragsverarbeitung im Sinne des Art. 28 DSGVO stattfindet**, da die personenbezogenen Daten ausschließlich auf den Systemen der Verantwortlichen gespeichert und verarbeitet werden und dem Auftragsverarbeiter ohne Mitwirkung der Verantwortlichen nicht zugänglich sind. **Dieser Vertrag wird vorsorglich abgeschlossen**, um jene Fälle abzudecken, in denen der Auftragsverarbeiter im Rahmen von Support-, Wartungs- oder Fehlerbehebungsleistungen aufgrund einer ausdrücklichen Weisung und Freigabe der Verantwortlichen Zugang zu personenbezogenen Daten erhalten kann (näher geregelt in § 6). Er regelt außerdem die sonstigen Pflichten nach Art. 28 DSGVO, die für diesen Ausnahmefall gelten – unabhängig davon, wie häufig er tatsächlich eintritt.

---

§ 1 Gegenstand und Dauer

1. Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag der Verantwortlichen im Zusammenhang mit der Bereitstellung, Wartung und dem Support der Software Betreuungsplaner bzw. CareGap.
2. Dieser Vertrag gilt für die Dauer des Lizenzvertrags. Er endet automatisch mit dessen Beendigung, unbeschadet der Nachwirkungen aus § 8 (Löschung/Rückgabe).

§ 2 Art und Zweck der Verarbeitung

1. Die Verarbeitung erfolgt ausschließlich zum Zweck der **technischen Unterstützung und Fehlerbehebung** (Support) im Einzelfall, wenn die Verantwortliche dies wünscht und die Voraussetzungen des § 4 vorliegen.
2. Der Auftragsverarbeiter verarbeitet die Daten **nicht** zu eigenen Zwecken, insbesondere nicht zu Marketing-, Analyse- oder Trainingszwecken (etwa für KI-Modelle), und nicht darüber hinausgehend als in diesem Vertrag und den dokumentierten Weisungen der Verantwortlichen festgelegt.
3. Art und Weise: punktueller, manueller Zugriff über den individuellen Systemadmin-Zugang der jeweiligen Installation (siehe § 6). Kein automatisierter, dauerhafter oder fernwartungsartiger Standardzugriff.

Verarbeitungsort: Supportleistungen des Auftragsverarbeiters erfolgen grundsätzlich in Österreich bzw. innerhalb der EU/des EWR. Eine Verarbeitung oder Übermittlung in ein Drittland oder an eine internationale Organisation erfolgt nur auf dokumentierte Weisung der Verantwortlichen und unter Einhaltung der Voraussetzungen der Art. 44 ff. DSGVO; der Sonderfall einer optionalen KI-Funktion richtet sich ergänzend nach § 5.

§ 3 Kategorien betroffener Personen und Datenkategorien

Betroffene Personen: - Klientinnen/Patientinnen der Verantwortlichen - Personenbetreuerinnen/Pflegepersonal bzw. Mitarbeiterinnen der Verantwortlichen

Datenkategorien: - Stammdaten (Name, Anschrift, Geburtsdatum, Kontaktdaten) - Vertrags- und Abrechnungsdaten - Besondere Kategorien nach Art. 9 DSGVO: Gesundheits- und Pflegedaten, Diagnosen, Medikamente, Behandlungs-/Betreuungspläne, Pflegeprotokolle, Fotos/Dateianhänge, elektronische Unterschriften - Bei Personenbetreuerinnen/Pflegepersonal: Qualifikationsnachweise, Meldedaten sowie gegebenenfalls personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO (z. B. Inhalte einer Strafregisterbescheinigung), soweit diese rechtmäßig verarbeitet werden dürfen.

§ 4 Pflichten des Auftragsverarbeiters (Art. 28 Abs. 3 DSGVO)

Der Auftragsverarbeiter

1. verarbeitet die personenbezogenen Daten ausschließlich auf dokumentierte Weisung der Verantwortlichen (Art. 28 Abs. 3 lit. a), einschließlich Weisungen zu einer Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. Dieser Vertrag sowie konkrete Supportanfragen der Verantwortlichen per E-Mail, Ticketsystem, Fernwartungseinladung oder sonstiger nachvollziehbarer Kommunikation gelten als dokumentierte Weisungen. Ist der Auftragsverarbeiter aufgrund von Unionsrecht oder dem Recht eines Mitgliedstaats zu einer Verarbeitung verpflichtet, informiert er die Verantwortliche vor der Verarbeitung über diese rechtliche Verpflichtung, sofern das betreffende Recht eine solche Information nicht aus wichtigen Gründen des öffentlichen Interesses untersagt. Die Weisungsdokumentation wird für Nachweiszwecke mindestens drei Jahre aufbewahrt;

2. gewährleistet, dass zur Verarbeitung befugte Personen **auf Vertraulichkeit verpflichtet** sind (lit. b);
1. trifft die in **Anlage 2 (TOM)** beschriebenen technischen und organisatorischen Maßnahmen (Art. 32 DSGVO, lit. c);
2. beachtet die Bedingungen für die Hinzuziehung eines weiteren Auftragsverarbeiters gemäß § 5 (lit. d);
3. unterstützt die Verantwortliche im Rahmen des Möglichen bei der Erfüllung von Betroffenenrechten (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) mittels geeigneter technischer und organisatorischer Maßnahmen (lit. e) – praktisch: die Verantwortliche kann diese Rechte in aller Regel selbst unmittelbar in der lokal installierten Software umsetzen (Datenhoheit liegt bei ihr); der Auftragsverarbeiter unterstützt auf Anfrage bei technischen Fragen hierzu;
4. unterstützt die Verantwortliche unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO (TOM, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation) (lit. f). Insbesondere informiert der Auftragsverarbeiter die Verantwortliche unverzüglich nach Kenntniserlangung über eine Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Auftragsverarbeitung. Soweit die Informationen verfügbar sind, enthält die Meldung mindestens Art und Umfang des Vorfalls, betroffene Daten-/Personenkategorien, bekannte oder wahrscheinliche Folgen sowie bereits ergriffene oder vorgeschlagene Abhilfemaßnahmen. Fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht. Eine interne Zielmarke von 48 Stunden darf nicht dazu führen, eine früher mögliche Meldung zu verzögern;
5. löscht oder gibt nach Wahl der Verantwortlichen nach Beendigung der Erbringung von Verarbeitungsleistungen sämtliche personenbezogenen Daten zurück und löscht vorhandene Kopien, soweit nicht eine gesetzliche Aufbewahrungspflicht entgegensteht (lit. g, siehe § 8);
6. stellt der Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen, die von der Verantwortlichen oder einem anderen von ihr beauftragten Prüfer durchgeführt werden, und trägt hierzu bei (lit. h); der Auftragsverarbeiter informiert die Verantwortliche unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder sonstige Datenschutzbestimmungen verstößt (Art. 28 Abs. 3 UAbs. 2).

§ 4a Pflichten und Rechte der Verantwortlichen

1. Die Verantwortliche bleibt für die Rechtmäßigkeit der Verarbeitung, insbesondere für das Vorliegen einer Rechtsgrundlage nach Art. 6 DSGVO und – soweit besondere Kategorien oder Daten nach Art. 10 DSGVO betroffen sind – der zusätzlichen gesetzlichen Voraussetzungen verantwortlich. Sie erfüllt insbesondere Informationspflichten gegenüber betroffenen Personen und stellt sicher, dass nur erforderliche Daten verarbeitet werden.

2. Die Verantwortliche erteilt Weisungen in dokumentierter Form und stellt sicher, dass diese rechtmäßig, eindeutig und auf die vereinbarten Zwecke beschränkt sind. Sie benennt

dem Auftragsverarbeiter auf Anfrage die zur Erteilung von Weisungen berechtigten Ansprechpersonen.

3. Die Verantwortliche ist für die Sicherheit der von ihr betriebenen Geräte, Betriebssysteme, Benutzerkonten, lokalen Netzwerke und Sicherungskopien verantwortlich. Sie schützt insbesondere Systemadmin-Zugangsdaten vor unbefugter Kenntnisnahme und aktiviert die in der Software angebotenen Sicherheitsfunktionen entsprechend ihrer eigenen Risikobewertung.

4. Die Verantwortliche informiert den Auftragsverarbeiter unverzüglich über Umstände, Änderungen oder Weisungen, die für die vertragsgemäße und sichere Erbringung der Auftragsverarbeitung wesentlich sind, und wirkt bei der Aufklärung von Sicherheitsvorfällen sowie bei Betroffenenanfragen mit, soweit dies erforderlich ist.

5. Der Verantwortlichen stehen die in diesem Vertrag geregelten Weisungs-, Informations-, Kontroll- und Wahlrechte zu. Sie kann insbesondere Auskunft über die Verarbeitung verlangen, Weisungen ändern oder widerrufen und nach Maßgabe von § 8 die Rückgabe oder Löschung von im Rahmen des Supports beim Auftragsverarbeiter entstandenen personenbezogenen Daten verlangen.

§ 5 Unterauftragsverhältnisse

1. Der Auftragsverarbeiter setzt derzeit für die in diesem AVV beschriebene Support-Auftragsverarbeitung keine weiteren Auftragsverarbeiter ein. Die Software ist im Normalbetrieb eine Offline-Anwendung ohne Cloud-Backend; eine automatische Datenübermittlung an Dritte findet nicht statt.
2. Die Hinzuziehung eines weiteren Auftragsverarbeiters bedarf der vorherigen spezifischen Genehmigung der Verantwortlichen in Schriftform einschließlich elektronischer Form (Art. 28 Abs. 2 DSGVO). Vor der Genehmigung informiert der Auftragsverarbeiter über Identität und Sitz des Unterauftragsverarbeiters, Gegenstand und Zweck der Verarbeitung, betroffene Datenkategorien, Verarbeitungsort sowie – bei Drittlandbezug – die vorgesehene Grundlage nach Kapitel V DSGVO.
    - Sonderfall optionale KI-Funktion: Sofern künftig eine Anbindung an einen KI-Dienst (derzeit vorgesehen: Anthropic/Anthropic API) mit personenbezogenen Echtdaten genutzt werden soll, bleibt diese Funktion standardmäßig deaktiviert und wird erst nach ausdrücklicher Aktivierung durch die Verantwortliche sowie nach deren spezifischer Genehmigung des Unterauftragsverarbeiters freigeschaltet. Diese Genehmigung nach Art. 28 Abs. 2 DSGVO ersetzt weder eine erforderliche Rechtsgrundlage nach Art. 6 DSGVO noch zusätzliche Voraussetzungen für besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO.
    - Vor einer Aktivierung mit personenbezogenen Daten stellt der Auftragsverarbeiter der Verantwortlichen die für deren Prüfung erforderlichen Informationen zur Verfügung, insbesondere zu Datenkategorien, Verarbeitungszwecken, Speicher-/Löschfristen, Unterauftragsverarbeitern des KI-Dienstes und Verarbeitungsorten.
    - Ohne die vorstehende ausdrückliche Freigabe und ohne Erfüllung der datenschutzrechtlichen Voraussetzungen werden keine personenbezogenen Daten der Verantwortlichen an den KI-Dienst übermittelt.

- Vor tatsächlicher Aktivierung mit personenbezogenen Echtdaten stellt der Auftragsverarbeiter sicher, dass mit dem Unterauftragsverarbeiter eine Vereinbarung besteht, die diesem im Wesentlichen dieselben Datenschutzpflichten auferlegt, die für den Auftragsverarbeiter nach diesem AVV gelten (Art. 28 Abs. 4 DSGVO). Bei Drittlandübermittlungen wird zusätzlich eine gültige Grundlage nach Art. 44 ff. DSGVO eingesetzt, insbesondere ein anwendbarer Angemessenheitsbeschluss oder – sofern erforderlich – Standardvertragsklauseln der Europäischen Kommission einschließlich einer gegebenenfalls erforderlichen Prüfung und ergänzender Schutzmaßnahmen.
- Bis zur Erteilung der ausdrücklichen Freigabe durch die Verantwortliche und zur Erfüllung der vorstehenden Voraussetzungen bleibt die KI-Funktion technisch deaktiviert (Opt-in-Schalter/Konfigurationsflag).

Haftung für Unterauftragsverarbeiter: Der Auftragsverarbeiter bleibt gegenüber der Verantwortlichen für die Erfüllung der Pflichten eines von ihm eingesetzten weiteren Auftragsverarbeiters nach Maßgabe des Art. 28 Abs. 4 DSGVO verantwortlich.

§ 6 Support-Zugriffsregelung (Systemadmin-Zugang)

1. Jede Installation von Betreuungsplaner bzw. CareGap erhält ein **einmalig generiertes, individuelles Systemadmin-Passwort**, das ausschließlich als Hashwert lokal auf dem Gerät der Verantwortlichen gespeichert und dieser bei Einrichtung einmalig angezeigt wird. Der Auftragsverarbeiter selbst speichert dieses Passwort **nicht** und hat **keinen standardmäßigen oder dauerhaften Zugriff** auf die mit der Software verarbeiteten Daten der Verantwortlichen.
2. Ein Zugriff des Auftragsverarbeiters auf den Datenbestand der Verantwortlichen ist **ausschließlich** in folgendem Fall möglich und zulässig:
   - Die Verantwortliche wendet sich mit einem konkreten technischen Anliegen an den Support des Auftragsverarbeiters;
   - die Verantwortliche stellt dem Auftragsverarbeiter den für den konkreten Supportfall erforderlichen Zugang freiwillig und möglichst über einen angemessen geschützten Kommunikationsweg zur Verfügung. Zugangsdaten dürfen nicht in Supportprotokollen, Tickets oder sonstigen Dokumentationen im Klartext dauerhaft gespeichert werden;
   - der Zugriff beschränkt sich auf das zur Bearbeitung des konkreten Anliegens erforderliche Ausmaß und die erforderliche Dauer.

Soweit zur Fehleranalyse Kopien, Screenshots, Logdateien oder Datenbankauszüge mit Personenbezug erforderlich sind, sind diese auf das notwendige Minimum zu beschränken, angemessen gegen unbefugten Zugriff zu schützen und ausschließlich für den konkreten Supportzweck zu verwenden. Eine Weitergabe an Dritte ist nur nach Maßgabe dieses Vertrags zulässig.

3. Der Auftragsverarbeiter protokolliert jeden derartigen Zugriff mit **Zeitpunkt, Anlass, Umfang und den durchgeführten Handlungen** und stellt diese Protokolle der Verantwortlichen auf Verlangen zur Verfügung.
4. Der Auftragsverarbeiter empfiehlt der Verantwortlichen, das Systemadmin-Passwort nach Abschluss des Supportfalls zu ändern (technisch durch die Software zu ermöglichen).

5. **Es besteht kein Anspruch und keine Verpflichtung der Verantwortlichen, das Passwort mitzuteilen.** Support kann auch ohne Zugriff auf den Datenbestand erfolgen (z. B. durch Fehlerbeschreibung, Logfiles ohne Personenbezug, Screenshots ohne Klientendaten), soweit dies zur Problemlösung ausreicht.

§ 7 Kontrollrechte der Verantwortlichen

1. Die Verantwortliche ist berechtigt, sich von der Einhaltung der in diesem Vertrag festgelegten Pflichten des Auftragsverarbeiters, insbesondere der getroffenen technischen und organisatorischen Maßnahmen, vor Beginn der Verarbeitung und danach regelmäßig zu überzeugen. Der Auftragsverarbeiter stellt hierfür auf Anfrage die aktuellen TOM-Unterlagen (Anlage 2) sowie – soweit vorhanden – Protokolle nach § 6 Abs. 3 zur Verfügung.
2. Inspektionen und Vor-Ort-Prüfungen sind mit angemessener Vorankündigung von mindestens **zehn Werktagen** durchzuführen und haben während der üblichen Geschäftszeiten zu erfolgen. Die Prüfungen dürfen den Geschäftsbetrieb des Auftragsverarbeiters nicht unverhältnismäßig beeinträchtigen und müssen auf datenschutzrechtlich relevante Bereiche beschränkt sein. Soweit möglich, können Nachweise zunächst durch Dokumentationen, Selbstauskünfte oder technische Unterlagen erbracht werden, bevor eine Vor-Ort-Prüfung erforderlich wird. Das Recht der Verantwortlichen, im Einzelfall auf einer Vor-Ort-Prüfung zu bestehen, bleibt hiervon unberührt; die Regelung dient der praktikablen Ausgestaltung, nicht der Einschränkung des Kontrollrechts nach Art. 28 Abs. 3 lit. h DSGVO.

§ 8 Löschung und Rückgabe nach Vertragsende

1. Da die Datenhoheit vollständig bei der Verantwortlichen liegt (lokale Speicherung auf deren Geräten) und der Auftragsverarbeiter im Regelbetrieb keine eigene Kopie der Daten führt, betrifft diese Regelung in erster Linie etwaige im Rahmen von Supportfällen (§ 6) kurzzeitig entstandene Kopien/Auszüge (z. B. Diagnosedateien, Screenshots).
2. Nach Abschluss des jeweiligen Supportfalls werden solche Kopien/Auszüge nach Wahl der Verantwortlichen zurückgegeben oder gelöscht. Liegt keine abweichende dokumentierte Weisung vor, löscht der Auftragsverarbeiter sie unverzüglich, spätestens innerhalb von 30 Tagen nach Abschluss des Supportfalls. Soweit Unionsrecht oder österreichisches Recht eine weitere Speicherung bestimmter Daten zwingend verlangt, werden nur die gesetzlich erforderlichen Daten für die gesetzlich vorgeschriebene Dauer gesperrt bzw. ausschließlich zu diesem Zweck weiter gespeichert und anschließend gelöscht.
3. Nach Beendigung des Lizenzvertrags bestätigt der Auftragsverarbeiter auf Verlangen schriftlich, dass keine personenbezogenen Daten der Verantwortlichen mehr bei ihm vorhanden sind.
4. Die vollständige Datenhoheit über den in der Software gespeicherten Datenbestand selbst verbleibt ohnehin ausschließlich bei der Verantwortlichen; diese kann den Datenbestand jederzeit ohne Mitwirkung des Auftragsverarbeiters exportieren und sichern.

§ 9 Haftung

Es gelten die Haftungsregelungen des Lizenzvertrags sowie ergänzend Art. 82 DSGVO. Der Auftragsverarbeiter haftet für Schäden, die durch eine Verarbeitung entstanden sind, bei der er den speziell für Auftragsverarbeiter geltenden Pflichten der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Weisungen der Verantwortlichen gehandelt hat.

§ 10 Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform einschließlich elektronischer Form. Dokumentierte Einzelweisungen im Rahmen der vereinbarten Verarbeitung können insbesondere per E-Mail, Ticketsystem oder sonstiger nachvollziehbarer elektronischer Kommunikation erteilt werden.
2. Sollte eine Bestimmung dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
3. Es gilt österreichisches Recht.
4. Im Fall von Widersprüchen zwischen diesem AVV und dem Lizenzvertrag geht dieser AVV hinsichtlich datenschutzrechtlicher Fragen vor.

Anlage 1 – Übersicht der Verarbeitung (Kurzform)

Punkt	Angabe
Gegenstand	Support/Fehlerbehebung im Einzelfall
Dauer	Laufzeit Lizenzvertrag
Art/Zweck	Punktueller, manueller Support-Zugriff auf ausdrücklichen Wunsch der Verantwortlichen
Betroffene	Klientinnen/Patientinnen, Personenbetreuerinnen/Pflegepersonal
Datenkategorien	Stamm-, Vertrags-, Abrechnungsdaten; Art. 9-Gesundheits-/Pflegedaten; Qualifikations-/Meldedaten Personal
Empfänger	Keine (kein Standard-Subauftragsverarbeiter)
Drittland	Keine im Normalbetrieb; Sonderfall KI-Funktion siehe § 5
Verarbeitungsort	Grundsätzlich Österreich/EU/EWR; Drittland nur nach dokumentierter Weisung und Art. 44 ff. DSGVO; Sonderfall KI-Funktion siehe § 5
Weisungsberechtigung	Verantwortliche; konkrete Supportanfragen und sonstige dokumentierte Weisungen gemäß § 4 und § 4a

Punkt	Angabe
Löschung/Rückgabe	Supportkopien nach Wahl der Verantwortlichen; ohne abweichende Weisung Löschung spätestens 30 Tage nach Supportabschluss

Anlage 2 – Technische und organisatorische Maßnahmen (TOM)

Diese Anlage beschreibt die für die vereinbarte Auftragsverarbeitung maßgeblichen technischen und organisatorischen Maßnahmen. Sie ist regelmäßig sowie bei wesentlichen technischen oder organisatorischen Änderungen zu überprüfen und erforderlichenfalls zu aktualisieren. Stand: 07.08.2026; technische Kernangaben beruhen auf dem Prüfbericht vom 29.07.2026 und der internen Statusmeldung vom 05.08.2026.

Ist-Zustand (technische und organisatorische Maßnahmen, aktuell umgesetzt):

- Verschlüsselung der lokalen Datenbankfunktion: AES-256-GCM mit frischem Zufalls-IV je Vorgang; Schlüsselableitung PBKDF2 mit 600.000 Iterationen (SHA-256). Derzeit opt-in – die Verantwortliche entscheidet im Rahmen ihrer eigenen Risikobewertung über die Aktivierung bei Einrichtung; der Auftragsverarbeiter empfiehlt die Aktivierung bei Verarbeitung von Gesundheitsdaten dringend. Unabhängig davon sind beim Auftragsverarbeiter im Rahmen eines Supportfalls vorübergehend entstehende personenbezogene Dateien/Kopien angemessen gegen unbefugten Zugriff zu schützen und nach § 8 zu löschen bzw. zurückzugeben.
- **Zugriffskontrolle:** Benutzerbezogene Konten mit abgestuften Rechten; individuelles, einmalig generiertes Systemadmin-Passwort je Installation (kein herstellerweiter Master-Zugang mehr).
- **Rollen- und Berechtigungskonzept:** Abgestufte Benutzerrechte für Benutzerkonten der Verantwortlichen; wirken innerhalb der lokal installierten Software (Hinweis: bei einer reinen Offline-Einzelplatzanwendung wirkt dies primär als Bedienhilfe, nicht als serverseitig durchgesetzte Sicherheitsgrenze – dies ist der Verantwortlichen bei der Vergabe von Zugriffsrechten an eigenes Personal bekannt zu geben).
- **Keine Telemetrie/kein Tracking/kein CDN**, keine automatische Cloud-Anbindung im Normalbetrieb.
- **Lizenzprüfung** vollständig offline (ECDSA P-256), kein Hersteller-Zugriff über die Lizenzierung.
- **Signierte Installer** (Authenticode) – in Umsetzung; bis zum Vorliegen des Zertifikats werden SHA-256-Prüfsummen zu jedem Installer bereitgestellt.
- **Wiederherstellungsschlüssel** ohne Hersteller-Hintertür (Recovery Key mit ausreichender Entropie).
- **Protokollierung von Support-Zugriffen** gemäß § 6 Abs. 3.

• Datenminimierung im Support: Personenbezogene Screenshots, Logdateien, Exporte oder Datenbankauszüge werden nur angefordert oder übernommen, wenn eine Fehleranalyse

mit anonymisierten bzw. nicht personenbezogenen Informationen nicht ausreichend möglich ist.

• Vertraulichkeit und Need-to-know-Prinzip: Zugriff auf personenbezogene Supportdaten erhalten nur Personen, die diesen Zugriff für den konkreten Supportfall benötigen und zur Vertraulichkeit verpflichtet sind.

• Sicherer Umgang mit Zugangsdaten: Systemadmin-Zugangsdaten werden nicht dauerhaft im Klartext dokumentiert oder in Supporttickets gespeichert; nach Abschluss eines Supportfalls wird der Verantwortlichen ein Wechsel des temporär offengelegten Passworts empfohlen.

• Löschkonzept für Supportdaten: Vorübergehend übernommene personenbezogene Daten werden nach § 8 zurückgegeben oder sicher gelöscht; nicht mehr benötigte lokale Arbeitskopien und temporäre Dateien werden in den Löschvorgang einbezogen.

- **Sicherheitsupdates:** Der Auftragsverarbeiter aktualisiert die Software und die darin eingesetzten Komponenten/Bibliotheken bei bekannt werdenden Sicherheitslücken (Art. 32 Abs. 1 lit. b DSGVO); ein formalisierter, turnusmäßiger Update- und Schwachstellenmanagementprozess (u. a. automatisierte Abhängigkeits-/Versionsprüfung) befindet sich im Aufbau.
- **Verfahren zur Wiederherstellung** der Verfügbarkeit und des Zugangs zu personenbezogenen Daten nach einem technischen Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO): Die Software bietet der Verantwortlichen eine verschlüsselte Datensicherungs-/Exportfunktion, mit der sie ihren Datenbestand eigenständig sichern und wiederherstellen kann. Ein vom Auftragsverarbeiter dokumentierter, turnusmäßiger Restore-Test steht noch aus; der Verantwortlichen wird empfohlen, eigene Restore-Tests durchzuführen (siehe auch Empfehlung unten).
- **Überprüfung und Bewertung** der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO): erfolgt im Rahmen von durch den Auftragsverarbeiter beauftragten unabhängigen Prüfungen (zuletzt 29.07.2026 und 05.08.2026); ein festgelegter, wiederkehrender Prüfturnus befindet sich im Aufbau.
- **Dokumentierter Prozess für den Umgang mit Sicherheitsvorfällen** einschließlich der Meldung an die Verantwortliche gemäß § 4 Abs. 6 dieses Vertrags (Art. 33 DSGVO).
- **Empfehlung an die Verantwortliche:** zusätzlich Geräteverschlüsselung (BitLocker/FileVault), Bildschirmsperre, regelmäßige verschlüsselte und örtlich getrennte Datensicherung mit Restore-Test.

Hinweis zur geplanten Weiterentwicklung (noch nicht als Ist-TOM umgesetzt):

> Die nachfolgende Regelung beschreibt eine künftige, angestrebte datenschutzfreundliche Voreinstellung der Software. Sie ist keine Beschreibung des derzeitigen technischen Ist-Zustands. Für die Beurteilung der aktuell umgesetzten TOM gelten ausschließlich die vorstehenden Angaben. Die Umsetzung darf das bestehende Schutzniveau nicht absenken.

- Der Auftragsverarbeiter verpflichtet sich, die Verschlüsselung neu eingerichteter Datenbanken künftig standardmäßig (Privacy by Default, Art. 25 Abs. 2 DSGVO) mit AES-256-GCM zu aktivieren. Eine Deaktivierung der Verschlüsselung soll nach

Umsetzung dieser Maßnahme ausschließlich auf ausdrücklichen Wunsch der Verantwortlichen möglich sein. Der Auftragsverarbeiter wird die Verantwortliche in diesem Fall darauf hinweisen, dass eine Deaktivierung insbesondere bei Gesundheitsdaten das Datenschutz- und Sicherheitsniveau reduziert.

- **Umsetzungsstand:** Zum Zeitpunkt des Vertragsabschlusses **noch nicht umgesetzt** – Verschlüsselung bleibt bis dahin opt-in (siehe oben). Umsetzungsdatum: **[von JS Consulting einzutragen, sobald feststehend]**. Bis zum Eintritt dieses Datums gilt ausschließlich der oben beschriebene Ist-Zustand.

Ort, Datum: _____

Für die Verantwortliche: _____

Für den Auftragsverarbeiter (JS Consulting): _____

Quellen/Prüfgrundlagen (Stand: 07.08.2026): - Art. 28, 32, 33 und 44 ff. DSGVO (EUR-Lex) - Standardvertragsklauseln der Europäischen Kommission für Verantwortliche und Auftragsverarbeiter gemäß Art. 28 Abs. 7 DSGVO - EDPB Guidelines 07/2020 zu den Begriffen Verantwortlicher und Auftragsverarbeiter - Anthropic Data Processing Addendum/Commercial Terms (nur relevant bei tatsächlicher Aktivierung der optionalen KI-Funktion; vor Aktivierung tagesaktuell zu prüfen) - Prüfbericht Sicherheit/Datenschutz/Compliance vom 29.07.2026 (JS Consulting, intern) - Interne Statusmeldung „Vertriebsfähigkeit – Umsetzung Sofortmaßnahmen" vom 05.08.2026 (JS Consulting, intern).

Prüfhinweis 07.08.2026: Ergänzt wurden insbesondere die gesetzlichen Ausnahmefälle von Weisungen, Verarbeitungsorte/Drittlandregelung, Pflichten und Rechte der Verantwortlichen, die Unterauftragsverarbeiter-Haftung, Inhalt und Unverzüglichkeit von Datenschutzverletzungsmeldungen, sichere Supportdaten-Handhabung sowie präzisierte Rückgabe-/Löschregeln.

Vorbehalt: Dieses Muster deckt die typischen Pflichtinhalte nach Art. 28 DSGVO ab, ersetzt aber keine anwaltliche Prüfung des Einzelfalls, insbesondere nicht hinsichtlich Haftungsverteilung, branchenspezifischer Besonderheiten und der Formulierung im Fall einer künftigen Aktivierung der KI-Funktion (Drittlandübermittlung).

Interne Arbeitsfassung von JS Consulting, Stand 07.08.2026 – ergänzt um Regelungen zu Drittlandübermittlung, Pflichten der Verantwortlichen, Unterauftragsverarbeiter-Haftung, Inhalt/Unverzüglichkeit von Datenschutzverletzungsmeldungen sowie Rückgabe-/Löschregeln. Eine gesonderte Bestätigung durch eine externe Rechtsanwältin/einen Rechtsanwalt liegt nicht vor; vor dem Einsatz mit echten Kundinnen/Kunden wird eine anwaltliche Durchsicht weiterhin empfohlen.