Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DSGVO · Fassung November 2026 (Rev. 2)

zwischen

Firma, Rechtsform

Straße, PLZ, Ort

vertreten durch (Name, Funktion)

(nachfolgend „Auftraggeber“ / „Verantwortlicher“)

und

Spruck IT Service GmbH
O7, 6 · 68161 Mannheim
Geschäftsführer: Daniel Spruck
(nachfolgend „Auftragnehmer“ / „Auftragsverarbeiter“)

Diese Vereinbarung gilt für folgende Leistungen des Auftragnehmers:

- ☐ Fernwartung und IT-Support (Remote)
- ☐ Managed IT Services (Full-Service-Betreuung, Administration, Cloud-Management)
- ☐ Remote Monitoring und Management (RMM) mit Softwareagent auf den betreuten Systemen
- ☐ Sonstige:

Zutreffendes ankreuzen oder ergänzen. Es können mehrere Optionen gewählt werden.

Ergänzende Vereinbarung für Berufsgeheimnisträger (optional):

- ☐ Der Auftraggeber ist Berufsgeheimnisträger im Sinne des § 203 StGB (z. B. Arztpraxis, Pflegedienst, Apotheke, Rechtsanwalts-, Steuerberater- oder Wirtschaftsprüferkanzlei). In diesem Fall gilt zusätzlich § 13 dieser Vereinbarung sowie Anlage 4.

Ohne Ankreuzen entfaltet Anlage 4 keine Wirkung; die übrige Vereinbarung gilt unverändert.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien im Zusammenhang mit der Auftragsverarbeitung gemäß Art. 28 DSGVO. Sie gilt für alle Tätigkeiten, bei denen Beschäftigte des Auftragnehmers oder von ihm beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers verarbeiten.

(2) Bei der Betreuung der IT-Systeme des Auftraggebers – insbesondere im Rahmen von Fernwartung und Monitoring – ist eine Kenntnisnahme personenbezogener Daten technisch nicht auszuschließen. Die Leistungen stellen daher eine Auftragsverarbeitung dar; der Abschluss dieser Vereinbarung ist für beide Parteien gesetzlich vorgeschrieben.

(3) Die Vereinbarung ist an die Laufzeit des zugrundeliegenden Servicevertrages gekoppelt. Sie beginnt mit Unterzeichnung und endet automatisch mit Beendigung des Hauptvertrages, sofern nicht eine gesonderte Beendigung vereinbart wird.

(4) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist durch Unionsrecht oder das Recht eines Mitgliedstaates zu einer anderen Verarbeitung verpflichtet.

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung durch den Auftragnehmer umfasst folgende Tätigkeiten:

– Administration und Wartung von IT-Systemen, Cloud-Diensten und Netzwerkinfrastruktur
– Fernwartung und technischer Support (1st/2nd Level)
– Remote Monitoring und Management (RMM) einschließlich automatisierter Inventarisierung, Statusüberwachung und Skriptausführung
– Einrichtung, Konfiguration und Außerbetriebnahme von Endgeräten (Onboarding/Offboarding)
– Verwaltung von Benutzerkonten, Berechtigungen und Sicherheitsrichtlinien
– Monitoring, Patch-Management und Sicherheitsüberwachung
– Verwaltung von E-Mail-, Kollaborations- und Kommunikationssystemen
– Unterstützung bei der Datensicherung und Wiederherstellung
– Beratung zu technischen und organisatorischen Sicherheitsmaßnahmen
– KI-gestützte Analyse und Dokumentation zur Unterstützung der vorgenannten Tätigkeiten nach Maßgabe von § 6a

Die Verarbeitung dient der Sicherstellung der Funktionsfähigkeit und Sicherheit der IT-Infrastruktur des Auftraggebers.

§ 3 Art der personenbezogenen Daten und Kategorien betroffener Personen

Folgende Datenarten können Gegenstand der Verarbeitung sein:

– Stammdaten (Name, Vorname, Anschrift, Geburtsdatum)
– Kontaktdaten (Telefonnummer, E-Mail-Adresse)
– Beschäftigtendaten (Personalnummer, Abteilung, Funktion)
– Vertragsdaten und kaufmännische Daten
– Kommunikationsdaten (E-Mail-Inhalte, Chat-Nachrichten)
– IT-Nutzungsdaten (Logfiles, Zugangsdaten, IP-Adressen)
– Weitere Daten gemäß den Anwendungen des Auftraggebers (z. B. CRM, Buchhaltung, DATEV)

Kategorien betroffener Personen: Beschäftigte, Kunden, Lieferanten, Geschäftspartner und sonstige Kontaktpersonen des Auftraggebers.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)

☐ Es werden keine besonderen Kategorien personenbezogener Daten verarbeitet.
☐ Es können besondere Kategorien verarbeitet werden, insbesondere: _____

Zutreffendes bitte ankreuzen. Werden besondere Kategorien verarbeitet (z. B. Gesundheitsdaten), gelten die erhöhten Schutzmaßnahmen nach Anlage 1 Ziffer 10.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Er verwendet die zur Verarbeitung überlassenen Daten für keine anderen Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung und wahrt die Vertraulichkeit.

(3) Alle Personen, die Zugang zu personenbezogenen Daten des Auftraggebers erhalten können, sind schriftlich zur Vertraulichkeit verpflichtet und werden vor Aufnahme der Tätigkeit mit den relevanten Datenschutzbestimmungen vertraut gemacht. Sensibilisierungsmaßnahmen werden regelmäßig durchgeführt.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei der Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei der Durchführung von Datenschutz-Folgenabschätzungen, soweit die Auftragsverarbeitung betroffen ist.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Betroffenenrechte (Art. 12–22 DSGVO) im erforderlichen Umfang.

(6) Auskünfte an Dritte oder Betroffene erteilt der Auftragnehmer nur nach vorheriger Zustimmung des Auftraggebers. Direkt an den Auftragnehmer gerichtete Anfragen werden unverzüglich weitergeleitet.

(7) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU bzw. des EWR. Soweit einzelne in Anlage 2 genannte Dienstleister Daten außerhalb der EU/des EWR verarbeiten, erfolgt dies ausschließlich auf Grundlage eines Angemessenheitsbeschlusses oder der Standardvertragsklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO nebst, soweit erforderlich, ergänzender Maßnahmen. Eine darüber hinausgehende Verarbeitung in Drittländern bedarf der vorherigen Zustimmung des Auftraggebers in Textform.

(8) Der Auftragnehmer beschäftigt weniger als 20 Personen mit der regelmäßigen automatisierten Verarbeitung personenbezogener Daten und ist daher nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet (§ 38 BDSG). Zentraler Ansprechpartner für alle Datenschutzangelegenheiten ist der Geschäftsführer, Herr Daniel Spruck (datenschutz@spruck-it.de). Sollte eine Bestellpflicht entstehen, wird der Auftraggeber unverzüglich informiert.

(9) Unterstützungsleistungen nach den Absätzen 4 und 5 sowie nach § 9 Abs. 3, die über die Beantwortung einfacher Anfragen hinausgehen, vergütet der Auftraggeber nach den jeweils gültigen Stundensätzen des Auftragnehmers, sofern der Anlass nicht vom Auftragnehmer zu vertreten ist.

§ 4a Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung sowie für die zutreffenden Angaben auf Seite 1 und in § 3 (Berufsgeheimnis, besondere Kategorien personenbezogener Daten) verantwortlich. Ändern sich diese Umstände, teilt er dies dem Auftragnehmer unverzüglich mit.

(2) Der Auftraggeber benennt dem Auftragnehmer Systeme, die besonders schutzbedürftige Daten enthalten.

(3) Die Information seiner Beschäftigten und sonstiger betroffener Personen nach Art. 13 und 14 DSGVO obliegt dem Auftraggeber.

§ 5 Technische und organisatorische Maßnahmen

(1) Anlage 1 beschreibt das vereinbarte, dem Risiko angemessene Schutzniveau gemäß Art. 32 DSGVO. Einzelne Maßnahmen können durch gleichwertige Maßnahmen ersetzt werden.

(2) Die Maßnahmen können im Rahmen des technischen Fortschritts angepasst werden, solange das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber unverzüglich mitzuteilen.

(3) Der Auftragnehmer stellt sicher, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(4) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen im Rahmen der Leistungserbringung.

(5) Die Verarbeitung personenbezogener Daten des Auftraggebers auf Privatgeräten der Beschäftigten des Auftragnehmers ist nicht gestattet. Für Tätigkeiten im Home-Office gelten die gleichen Sicherheitsstandards wie im Büro; der Zugriff erfolgt ausschließlich über gesicherte Verbindungen (VPN) und verwaltete Unternehmensgeräte.

§ 6 Fernwartung, Remote Monitoring und Management

(1) Eingesetzte Systeme. Der Auftragnehmer setzt für die Betreuung der Systeme des Auftraggebers ein:

– Tactical RMM – Managementplattform mit Softwareagent zur Inventarisierung, Überwachung, Patch- und Softwareverteilung sowie Skriptausführung. Die Plattform wird als quelloffene Software ausschließlich im eigenen Rechenzentrum des Auftragnehmers in O7, 6, 68161 Mannheim betrieben. Eine Übermittlung an den Softwarehersteller oder an Cloud-Dienste Dritter findet nicht statt.
– TeamViewer – Software für die interaktive Fernwartung mit Bildschirm- und Dateiübertragung. Die Verarbeitung erfolgt in Deutschland bzw. der EU.

(2) Umfang des Zugriffs. Der Auftraggeber stimmt der Installation der erforderlichen Agenten auf den betreuten Systemen zu. Über den Agenten erfolgen die automatisierte Erhebung von Inventar-, Status- und Telemetriedaten sowie die Ausführung von Wartungsaufgaben, Updates und Skripten mit administrativen Rechten. Ein Zugriff auf Bildschirminhalte über den Agenten erfolgt nur nach Maßgabe von Absatz 3.

(3) Interaktive Fernwartung. Der Zugriff auf Bildschirminhalte von Arbeitsplatzrechnern und mobilen Endgeräten erfolgt ausschließlich nach vorheriger Bestätigung durch den jeweiligen Anwender (attended). Ein unbeaufsichtigter Zugriff (unattended) ist ausschließlich auf Server, Terminalserver sowie Netzwerk- und Infrastrukturkomponenten zulässig, soweit dies für Wartung, Störungsbeseitigung und Sicherheitsmaßnahmen erforderlich ist.

(4) Zweckbindung. Der Zugriff erfolgt ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen. Eine Kenntnisnahme von Inhaltsdaten erfolgt nur, soweit sie dafür unvermeidbar ist.

(5) Zugriffsschutz. Zugriffe erfolgen ausschließlich über personalisierte Benutzerkonten des Auftragnehmers; Sammelkonten sind unzulässig. Die Zugänge zu den Managementplattformen des Auftragnehmers sowie zu Cloud-Diensten sind mit Mehrfaktor-Authentifizierung abgesichert, auf Systemen des Auftraggebers, soweit diese es unterstützen; der Zugriff ist über ein Rollenkonzept auf den erforderlichen Umfang begrenzt. Scheidet ein Mitarbeiter des Auftragnehmers aus, werden dessen Zugänge unverzüglich deaktiviert.

(6) Protokollierung. Fernwartungssitzungen werden mit Zeitpunkt, Dauer, Zielsystem und ausführender Person protokolliert; die Protokolle werden in der Regel zwölf Monate vorgehalten und dem Auftraggeber auf Anforderung zur Verfügung gestellt. Die Dokumentation der Servicevorgänge im Ticketsystem des Auftragnehmers wird nachvollziehbar geführt und im Rahmen der gesetzlichen Aufbewahrungsfristen verwahrt.

(7) Notfallzugriff. Für Störungen mit erheblicher Auswirkung auf den Geschäftsbetrieb hält der Auftragnehmer einen gesondert gesicherten Notfallzugang („Break-Glass“) vor. Dessen Nutzung wird protokolliert und dem Auftraggeber zeitnah, in der Regel am folgenden Werktag, mitgeteilt.

(8) Mitwirkung des Auftraggebers. Der Auftraggeber informiert seine Beschäftigten gemäß Art. 13 DSGVO über die Fernwartung und die dabei erhobenen Daten. Er stellt sicher, dass eine gegebenenfalls erforderliche Beteiligung des Betriebsrats erfolgt ist; die im Rahmen des Monitorings anfallenden Daten (z. B. An- und Abmeldezeiten, installierte und genutzte Software) können objektiv zur Verhaltens- und Leistungskontrolle geeignet sein, sodass der Einsatz solcher Systeme der Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG unterliegen kann.

(9) Keine Leistungskontrolle. Der Auftragnehmer erstellt keine Auswertungen zur Leistungs- oder Verhaltenskontrolle einzelner Beschäftigter des Auftraggebers.

(10) Beendigung. Mit Beendigung des Hauptvertrages entfernt der Auftragnehmer die installierten Agenten, soweit ihm der Zugriff noch möglich ist, und deaktiviert sämtliche Fernzugänge.

§ 6a Einsatz von KI-Diensten

(1) Der Auftragnehmer kann zur Unterstützung der in § 2 genannten Tätigkeiten KI-Sprachmodelle einsetzen, insbesondere zur Auswertung von Tickets, Protokollen und Systemmeldungen, zur Fehleranalyse sowie zur Erstellung von Dokumentationen und Skripten.

(2) Für Daten des Auftraggebers werden ausschließlich geschäftliche Angebote und API-Zugänge der in Anlage 2 genannten Anbieter eingesetzt, mit denen ein Vertrag zur Auftragsverarbeitung besteht. Nach den jeweils geltenden Vertragsbedingungen der Anbieter werden übermittelte Daten nicht zum Training der Modelle verwendet; eine Speicherung beim Anbieter erfolgt nur befristet im Rahmen der Anbieterbedingungen.

(3) Die Anbindung erfolgt über Software, die der Auftragnehmer auf eigener Infrastruktur betreibt. Der Auftragnehmer begrenzt die Übermittlung auf den für die jeweilige Aufgabe benötigten Umfang; eine systematische Übermittlung vollständiger Datenbestände des Auftraggebers findet nicht statt.

(4) Der Einsatz erfolgt in der Verantwortung des Auftragnehmers. Automatisierte Entscheidungen im Einzelfall im Sinne des Art. 22 DSGVO finden nicht statt. Die Information der Beschäftigten des Auftraggebers obliegt dem Auftraggeber (§ 6 Abs. 8 gilt entsprechend).

(5) Patienten-, Mandanten- oder Klientendaten von Berufsgeheimnisträgern sowie besondere Kategorien personenbezogener Daten übermittelt der Auftragnehmer nicht gezielt an KI-Dienste nach Absatz 2; eine gezielte Übermittlung erfolgt nur nach vorheriger Zustimmung des Auftraggebers in Textform. Die Zustimmung erfolgt in Kenntnis, dass sich die Vertraulichkeitspflichten der KI-Anbieter aus deren Auftragsverarbeitungsverträgen ergeben und diese keine gesonderte Erklärung nach § 203 Abs. 4 StGB abgeben.

§ 7 Unterauftragsverhältnisse

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter hinzuzuziehen, zu ersetzen oder zu wechseln (Art. 28 Abs. 2 Satz 1 DSGVO). Die jeweils aktuelle Liste ist Anlage 2 und wird unter www.spruck-it.de/unterauftragsverarbeiter veröffentlicht.

(2) Änderungen werden ausschließlich durch Aktualisierung dieser Liste bekannt gegeben; eine gesonderte Ansprache jedes Auftraggebers erfolgt nicht. Der Auftraggeber kann innerhalb von 14 Tagen nach Veröffentlichung aus einem wichtigen datenschutzrechtlichen Grund in Textform widersprechen; andernfalls gilt die Änderung als genehmigt. Auf Wunsch richtet der Auftragnehmer eine automatische Benachrichtigung per E-Mail ein. Widerspricht der Auftraggeber, kann der Auftragnehmer die betroffene Leistung einstellen oder den Servicevertrag mit einer Frist von drei Monaten kündigen; ein Anspruch auf Leistungserbringung ohne den betroffenen Unterauftragsverarbeiter besteht nicht.

(3) Der Auftragnehmer stellt vertraglich sicher, dass den Unterauftragsverarbeitern mindestens gleichwertige Datenschutzpflichten auferlegt werden (Art. 28 Abs. 4 DSGVO). Der Auftraggeber erhält auf Verlangen Einsicht in die wesentlichen datenschutzrelevanten Inhalte dieser Verträge; Geschäftsgeheimnisse sind ausgenommen.

(4) Der Auftragnehmer wählt Unterauftragsverarbeiter unter besonderer Berücksichtigung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

(5) Nebenleistungen wie Telekommunikation, Post, Transport, Reinigung oder allgemeine Wartung ohne Bezug zu personenbezogenen Daten gelten nicht als Unterauftragsverhältnisse im Sinne dieser Vereinbarung. Gleiches gilt für Software, die der Auftragnehmer ausschließlich auf eigener Infrastruktur betreibt und bei der kein Datenzugriff des Herstellers besteht.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, die Einhaltung der datenschutzrechtlichen Vorschriften und dieser Vereinbarung in angemessenem Umfang zu überprüfen. Dies kann durch Einholung von Auskünften, Einsichtnahme in Dokumentationen und – soweit erforderlich – durch Inspektionen vor Ort erfolgen. Beauftragt der Auftraggeber einen Dritten mit der Prüfung, muss dieser zur Verschwiegenheit verpflichtet sein und darf nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen.

(2) Kontrollen finden nach angemessener Vorankündigung von mindestens zwei Wochen zu den Geschäftszeiten des Auftragnehmers statt und dürfen den Geschäftsbetrieb nicht unverhältnismäßig stören. Routinekontrollen finden nicht häufiger als einmal pro Kalenderjahr statt, sofern kein begründeter Anlass für eine außerordentliche Prüfung besteht.

(3) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen und Nachweise zur Verfügung. Soweit die Kontrolle durch Vorlage aktueller Zertifizierungen, Auditberichte oder der ausgefüllten TOM-Dokumentation erfolgen kann, sind diese Mittel vorrangig zu nutzen. Für den Aufwand einer Vor-Ort-Kontrolle kann der Auftragnehmer eine angemessene Vergütung nach seinen jeweils gültigen Stundensätzen berechnen; ausgenommen sind Kontrollen aus konkretem Anlass, den der Auftragnehmer zu vertreten hat.

§ 9 Meldepflichten bei Datenschutzverletzungen

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich nach Kenntniserlangung über jede Verletzung des Schutzes personenbezogener Daten. Die Information erfolgt so rechtzeitig, dass der Auftraggeber seine Meldepflicht gegenüber der Aufsichtsbehörde nach Art. 33 DSGVO fristgerecht erfüllen kann. Auch begründete Verdachtsfälle sind mitzuteilen.

(2) Die Meldung enthält mindestens: (a) Beschreibung der Art der Verletzung, (b) Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze, (c) Beschreibung der wahrscheinlichen Folgen, (d) Beschreibung der ergriffenen oder vorgeschlagenen Gegenmaßnahmen.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Meldepflichten gemäß Art. 33 und 34 DSGVO.

(4) Erhebliche Störungen der Auftragsverarbeitung, Verstöße gegen datenschutzrechtliche Bestimmungen sowie Kontrollen durch Aufsichtsbehörden sind dem Auftraggeber unverzüglich mitzuteilen.

§ 10 Weisungsrecht

(1) Der Auftraggeber erteilt Weisungen in der Regel in Textform (E-Mail oder Ticketsystem genügt). In Eilfällen können Weisungen mündlich erteilt und unverzüglich in Textform bestätigt werden.

(2) Der Auftragnehmer macht den Auftraggeber unverzüglich darauf aufmerksam, wenn eine Weisung seiner Auffassung nach gegen datenschutzrechtliche Vorschriften verstößt. Er ist berechtigt, die Durchführung der Weisung auszusetzen, bis sie bestätigt oder angepasst wird.

(3) Weisungsberechtigte und -empfangsberechtigte Personen werden in Anlage 3 benannt.

(4) Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, sind nach Aufwand zu vergüten.

§ 11 Berichtigung, Löschung und Rückgabe von Daten

(1) Der Auftragnehmer berichtigt, löscht oder sperrt im Auftrag verarbeitete Daten ausschließlich nach Weisung des Auftraggebers.

(2) Nach Beendigung des Auftragsverhältnisses hat der Auftragnehmer sämtliche im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben. Die Löschung ist dem Auftraggeber in Textform zu bestätigen. Daten in Sicherungskopien werden nicht gesondert gelöscht, sondern mit Ablauf des regulären Sicherungszyklus überschrieben; bis dahin erfolgt kein Zugriff auf sie. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

(3) Dokumentationen, die dem Nachweis der ordnungsgemäßen Auftragsverarbeitung dienen, sind über das Vertragsende hinaus entsprechend den gesetzlichen Aufbewahrungsfristen aufzubewahren.

§ 12 Haftung

Die Haftung gegenüber betroffenen Personen richtet sich nach Art. 82 DSGVO. Im Verhältnis der Parteien zueinander – einschließlich eines Rückgriffs nach Art. 82 Abs. 5 DSGVO – gelten die Haftungsregelungen des zugrundeliegenden Servicevertrages. Gegen den Auftraggeber verhängte Bußgelder übernimmt der Auftragnehmer nicht.

§ 13 Besondere Geheimhaltungspflichten (§ 203 StGB) – gilt nur bei Ankreuzen auf Seite 1

(1) Ist der Auftraggeber Berufsgeheimnisträger im Sinne des § 203 Abs. 1 StGB, wird der Auftragnehmer als sonstige mitwirkende Person nach § 203 Abs. 3 Satz 2 StGB tätig. Der Auftragnehmer verpflichtet sich, über alle ihm bekannt gewordenen fremden Geheimnisse – insbesondere Patienten-, Klienten- und Mandantendaten – Verschwiegenheit zu bewahren und diese weder unbefugt zu offenbaren noch zu verwerten. Die Verpflichtung besteht über die Beendigung des Vertragsverhältnisses hinaus fort.

(2) Der Auftragnehmer stellt sicher, dass alle von ihm eingesetzten Beschäftigten, die Zugang zu geschützten Informationen erhalten können, zuvor nach § 203 Abs. 4 Satz 2 StGB zur Geheimhaltung verpflichtet werden. Unterauftragnehmer, die Zugang zu geschützten Informationen erhalten, werden nur nach vorheriger Zustimmung des Auftraggebers und nach entsprechender Verpflichtung eingesetzt.

(3) Die Erfüllung dieser Pflicht wird in Anlage 4 dokumentiert.

§ 14 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform.

(2) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Mannheim.

(4) Die Anlagen 1–4 sind Bestandteil dieser Vereinbarung. Anlage 4 gilt nur, sofern auf Seite 1 entsprechend gekennzeichnet.

(5) Diese Fassung ersetzt frühere Fassungen der AV-Vereinbarung zwischen den Parteien.

(6) Bei Widersprüchen zwischen dieser Vereinbarung und dem Servicevertrag geht diese Vereinbarung in datenschutzrechtlichen Fragen vor, im Übrigen der Servicevertrag.

Ort, Datum	Mannheim, 01.11.2026 Ort, Datum
SIGN Auftraggeber (Unterschrift, Stempel)	Daniel Spruck Digital unterschrieben von Daniel Spruck Datum: 2026.11.04 10:48:34 +01'00' Auftragnehmer – Spruck IT Service GmbH, Daniel Spruck

Bitte senden Sie das ausgefüllte und unterzeichnete Dokument an nachricht@spruck-it.de. Sie erhalten es gegengezeichnet zurück. Eine digital signierte Fassung des Auftragnehmers steht unter www.spruck-it.de zum Abruf bereit.

Anlage 1: Technische und organisatorische Maßnahmen

gemäß Art. 32 DSGVO · Stand November 2026 (Rev. 2)

1. Zutrittskontrolle

Maßnahmen, die Unbefugten den physischen Zutritt zu den Datenverarbeitungsanlagen verwehren:

– Geschäftsräume und eigenes Rechenzentrum in O7, 6, 68161 Mannheim mit zwei massiven Haustüren und Sicherheitsschlössern
– Videoüberwachung der Eingangstüren auf Grundlage des berechtigten Interesses am Schutz der Räumlichkeiten; Hinweisbeschilderung vorhanden
– Schlüsselregelung mit dokumentierter Ausgabe und Rücknahme
– Besucher werden empfangen und begleitet; kein unbeaufsichtigter Zugang zu Arbeitsplätzen
– Serverraum / Netzwerkschrank mit eingeschränktem Zugang (nur autorisierte Mitarbeiter)

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

– Individuelle Benutzerkonten mit komplexen Passwörtern für alle Systeme
– Multi-Faktor-Authentifizierung (MFA) für Cloud-Dienste sowie für die Management- und Fernwartungsplattformen des Auftragnehmers
– Zentrale Passwortverwaltung über selbst gehosteten Passwortmanager (Vaultwarden) mit verschlüsselter Datenbank
– Automatische Bildschirmsperre nach Inaktivität auf allen Arbeitsplätzen
– Zentral verwalteter Endpoint-Schutz auf allen Systemen des Auftragnehmers: ESET PROTECT Complete einschließlich ESET Inspect (EDR), verwaltet über die ESET PROTECT Cloud Console
– Cisco Meraki MX Security Appliance mit Advanced Security Lizenz und aktiviertem IDS/IPS
– Windows-Firewall auf allen Endgeräten aktiv
– Remote-Zugriffe ausschließlich über verschlüsselte VPN-Verbindungen oder MFA-geschützte Dienste
– Zuordnung von Benutzerrechten nach dem Prinzip der geringsten Privilegien (Least Privilege)

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass Berechtigte nur auf die ihrem Zugriffsprofil unterliegenden Daten zugreifen können:

– Rollenbasiertes Berechtigungskonzept für alle verwalteten Systeme
– Verwaltung der Zugriffsrechte durch den Systemadministrator
– Regelmäßige Überprüfung und Anpassung von Berechtigungen bei Personalveränderungen
– Separate Admin-Konten für administrative Tätigkeiten
– Sichere Aufbewahrung von Datenträgern mit Kundendaten
– Physische Löschung von Datenträgern vor Wiederverwendung oder Entsorgung (DBAN / physische Zerstörung)
– Einsatz von Aktenvernichtern (mindestens Sicherheitsstufe P-4)

4. Weitergabekontrolle / Übertragungssicherheit

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der Übertragung nicht unbefugt gelesen, kopiert oder verändert werden können:

– Verschlüsselte E-Mail-Übertragung (TLS) als Standard für die gesamte geschäftliche Kommunikation
– Nutzung passwortgeschützter, verschlüsselter Übertragungswege für den Austausch sensibler Daten
– VPN-Verschlüsselung für alle Standortvernetzungen und Remote-Zugriffe
– Ende-zu-Ende-verschlüsselte Fernwartungssitzungen; Verarbeitung ausschließlich in Deutschland bzw. der EU
– Ausschließliche Nutzung von HTTPS für Webzugriffe auf verwaltete Systeme
– Keine unverschlüsselte Übertragung personenbezogener Daten über öffentliche Netze

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft werden kann, ob und von wem Daten eingegeben, verändert oder entfernt worden sind:

– Nachvollziehbarkeit von Änderungen durch individuelle Benutzerkonten und Protokollierung
– Ticketsystem für alle Supportvorgänge mit protokolliertem Bearbeitungsverlauf; Aufbewahrung im Rahmen der gesetzlichen Fristen
– Audit-Logs in den verwalteten Cloud-Plattformen (Microsoft Entra, Microsoft 365)
– Protokollierung der Fernwartungssitzungen mit Zeitpunkt, Dauer, Zielsystem und ausführender Person; Aufbewahrung in der Regel zwölf Monate

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten nur entsprechend den Weisungen verarbeitet werden:

– Schriftliche Auftragsverarbeitungsvereinbarung (dieses Dokument) mit eindeutigen Weisungsregelungen
– Schriftliche Verpflichtung aller Beschäftigten auf die Vertraulichkeit und den Datenschutz im Rahmen des Arbeitsvertrages
– Regelmäßige Sensibilisierung der Beschäftigten für Datenschutzthemen
– Sorgfältige Auswahl von Unterauftragsverarbeitern und Prüfung ihrer Nachweise vor Beauftragung
– Sicherstellung und Dokumentation der Datenlöschung nach Auftragsbeendigung

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

– Mehrstufiges Sicherungskonzept nach dem 3-2-1-Prinzip mit lokaler und georedundanter Cloud-Sicherung; unveränderbare Aufbewahrung der Cloud-Sicherungen (Immutable Storage mit Retention Lock) als Schutz vor Ransomware und vor Löschung durch Angreifer
– Einsatz unterbrechungsfreier Stromversorgung (USV) für kritische Systeme
– Endpoint-Schutz mit Echtzeitschutz, EDR-Funktionen und automatischen Updates
– Cisco Meraki Firewall mit IDS/IPS zum Schutz der Netzwerkinfrastruktur
– Regelmäßiges Patch-Management für Betriebssysteme und Anwendungen
– Definierte Wiederanlaufprozesse für kritische Systeme; die Wiederherstellbarkeit wird im laufenden Betrieb verifiziert

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

– Logische Mandantentrennung in den Managementsystemen (RMM, Ticketsystem, Passwortverwaltung)
– Separate Kundenumgebungen mit individuellen Zugangsdaten und Berechtigungen
– Getrennte Ablagestrukturen und Berechtigungskonzepte pro Auftraggeber
– Trennung von Produktiv- und Testsystemen

9. Verschlüsselung

Maßnahmen zur Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO):

– Vollverschlüsselung aller Firmengeräte mittels BitLocker (Windows) bzw. FileVault (macOS)
– Transportverschlüsselung (TLS 1.2/1.3) für alle externen Verbindungen
– VPN-Verschlüsselung für Remote-Zugriffe und Standortvernetzung
– Verschlüsselte Passwortverwaltung (Vaultwarden mit AES-256)
– Cloud-Daten serverseitig verschlüsselt (Microsoft Azure Encryption at Rest, AES-256)

10. Ergänzende Maßnahmen bei besonderen Kategorien personenbezogener Daten

Gelten, sofern in § 3 dieser Vereinbarung entsprechend gekennzeichnet:

– Zugriff auf die betroffenen Systeme nur für einen namentlich festgelegten, eingeschränkten Personenkreis
– Bevorzugt begleiteter Zugriff (attended) nach Anmeldung beim Auftraggeber
– Gesonderte Verpflichtung der eingesetzten Personen nach § 203 Abs. 4 StGB (Anlage 4)
– In der Managementplattform werden keine Inhaltsdaten gespeichert; im Ticketsystem nur, soweit dies zur Bearbeitung des jeweiligen Vorgangs erforderlich ist

11. Einsatz von KI-Diensten

Maßnahmen beim Einsatz von KI-Diensten nach § 6a dieser Vereinbarung:

– Nutzung ausschließlich geschäftlicher Zugänge bzw. API-Zugänge mit Auftragsverarbeitungsvertrag
– KI-Agenten-Software auf eigener Infrastruktur des Auftragnehmers
– Zentrale Verwaltung der API-Schlüssel; Zugriffsrechte nach dem Prinzip der geringsten Privilegien

Anlage 2: Unterauftragsverarbeiter

Stand November 2026 (Rev. 2)

Folgende Unterauftragsverarbeiter sind vom Auftraggeber genehmigt:

Unternehmen	Leistung	Standort
Microsoft Ireland Operations Ltd.	Cloud-Infrastruktur (Microsoft 365, Azure, Entra ID)	EU (Irland/Niederlande)
TeamViewer Germany GmbH	Fernwartungssoftware: Vermittlung und Verschlüsselung der Sitzungen, Geräte- und Kontaktlisten	Deutschland / EU
ESET spol. s r.o.	Endpoint Security (ESET PROTECT Cloud)	EU (Slowakei)
Cisco Meraki (Cisco Systems)	Netzwerk-Management (Meraki Cloud Dashboard)	EU/USA (EU-SCCs)
Hornetsecurity GmbH	Datensicherung des eigenen Microsoft 365 des Auftragnehmers (365 Total Backup)	EU (Deutschland)
Anthropic PBC	KI-Sprachmodelle (Claude) über geschäftliche Zugänge und API	USA (EU-SCCs)
OpenAI Ireland Ltd.	KI-Sprachmodelle (GPT) über geschäftliche Zugänge und API	EU/USA (EU-SCCs)

Nicht als Unterauftragsverarbeitung gilt der Einsatz der Managementplattform Tactical RMM sowie der selbst betriebenen KI-Agenten-Software: Der Auftragnehmer betreibt diese Software ausschließlich auf eigener Infrastruktur; ein Zugriff des Softwareherstellers besteht nicht. Die Übermittlung an KI-Anbieter richtet sich nach § 6a und der vorstehenden Tabelle.

Die jeweils aktuelle Fassung dieser Liste ist unter www.spruck-it.de/unterauftragsverarbeiter abrufbar und maßgeblich. Änderungen werden dort veröffentlicht; ein Widerspruchsrecht besteht nach § 7 dieser Vereinbarung.

Anlage 3: Weisungsberechtigte Personen

Bitte vom Auftraggeber ausfüllen

Weisungsberechtigt auf Seiten des Auftraggebers

Name:

Funktion:

E-Mail:

Telefon:

Vertretung (optional)

Name:

E-Mail:

Weisungsempfangsberechtigt auf Seiten des Auftragnehmers

Name: Daniel Spruck
Funktion: Geschäftsführer
E-Mail: d.spruck@spruck-it.de
Telefon: +49 621 180 600 20
Vertretung: support@spruck-it.de

Änderungen sind der jeweils anderen Partei unverzüglich mitzuteilen.

Anlage 4: Verpflichtung nach § 203 Abs. 4 StGB

Optional · gilt nur für Berufsgeheimnisträger und nur bei Kennzeichnung auf Seite 1

Ist der Auftraggeber Berufsgeheimnisträger im Sinne des § 203 Abs. 1 StGB (z. B. Arztpraxis, Pflegedienst, Apotheke, Rechtsanwalts-, Steuerberater- oder Wirtschaftsprüferkanzlei), darf er fremde Geheimnisse gegenüber mitwirkenden Personen nur offenbaren, soweit dies für deren Tätigkeit erforderlich ist. Die mitwirkenden Personen sind zuvor zur Geheimhaltung zu verpflichten (§ 203 Abs. 4 StGB). Diese Anlage dokumentiert die Erfüllung dieser Pflicht.

1. Erklärung des Auftragnehmers

Die Spruck IT Service GmbH verpflichtet sich, über alle ihr im Rahmen ihrer Tätigkeit bekannt gewordenen fremden Geheimnisse – insbesondere Patienten-, Klienten- und Mandantendaten – Verschwiegenheit zu bewahren. Sie wird solche Geheimnisse weder unbefugt offenbaren noch verwerten. Die Verpflichtung besteht über die Beendigung des Vertragsverhältnisses hinaus fort.

Alle eingesetzten Personen werden vor Aufnahme der Tätigkeit nach § 203 Abs. 4 Satz 2 StGB schriftlich zur Geheimhaltung verpflichtet und über die Rechtsfolgen eines Verstoßes belehrt.

2. Belehrung

Ein Verstoß gegen die Geheimhaltungspflicht kann nach § 203 Abs. 4 StGB mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe geahndet werden. Daneben können zivilrechtliche Schadensersatzansprüche und Sanktionen nach der DSGVO entstehen.

3. Für den Auftraggeber eingesetzte Personen

Sämtliche Beschäftigten des Auftragnehmers, die Zugang zu Systemen des Auftraggebers erhalten können, sind vor Aufnahme ihrer Tätigkeit nach § 203 Abs. 4 Satz 2 StGB schriftlich zur Geheimhaltung verpflichtet und über die Rechtsfolgen belehrt. Eine namentliche Aufstellung mit Verpflichtungsdatum wird dem Auftraggeber auf Anforderung übermittelt.

Ort, Datum · Auftraggeber	Ort, Datum · Spruck IT Service GmbH