Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

zwischen

_____

(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)

☐ Sonstige: _____

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

§ 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) 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.

(3) 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)
- 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

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.

§ 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 ausschließlich innerhalb der EU bzw. des EWR. Eine Verarbeitung in Drittländern bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und ist nur unter Einhaltung der Voraussetzungen des Kapitels V DSGVO zulässig.

(8) Der Auftragnehmer ist derzeit aufgrund der Unternehmensgröße (weniger als 20 Personen mit regelmäßiger automatisierter Datenverarbeitung) nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet (§ 38 BDSG). Sollte sich dies ändern, wird der Auftraggeber unverzüglich informiert.

§ 5 Technische und organisatorische Maßnahmen

(1) Die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO werden als verbindliches Mindestschutzniveau festgelegt.

(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 Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragsverarbeitern ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers zulässig. Die aktuell genehmigten Unterauftragsverarbeiter sind in Anlage 2 aufgeführt.

(2) Der Auftragnehmer stellt vertraglich sicher, dass den Unterauftragsverarbeitern mindestens gleichwertige Datenschutzpflichten auferlegt werden. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge.

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

(4) Nebenleistungen wie Telekommunikation, Post, Transport, Reinigung oder allgemeine Wartung ohne Bezug zu personenbezogenen Daten gelten nicht als Unterauftragsverhältnisse im Sinne dieser Vereinbarung.

§ 7 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.

(2) Kontrollen finden nach angemessener Vorankündigung 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, die zur Durchführung der Kontrolle notwendig sind. Soweit die Kontrolle durch Vorlage aktueller Zertifizierungen, Auditberichte oder der ausgefüllten TOM-Dokumentation erfolgen kann, sind diese Mittel vorrangig zu nutzen.

(4) Der Auftragnehmer kann alternativ die Einhaltung der vereinbarten Maßnahmen durch Vorlage aktueller Prüfberichte, Zertifizierungen oder der dokumentierten technischen und organisatorischen Maßnahmen nachweisen.

§ 8 Meldepflichten bei Datenschutzverletzungen

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung, über jede Verletzung des Schutzes personenbezogener Daten. 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, Verstöße gegen datenschutzrechtliche Bestimmungen sowie Kontrollen durch Aufsichtsbehörden sind dem Auftraggeber unverzüglich mitzuteilen.

§ 9 Weisungsrecht

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

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

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

§ 10 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 schriftlich zu bestätigen. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

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

§ 11 Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des zugrundeliegenden Servicevertrages.

§ 12 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 1–3 sind Bestandteil dieser Vereinbarung.

_____

Ort, Datum

_____

Auftraggeber (Unterschrift, Stempel)

Mannheim, 16.03.2026

Ort, Datum

DS

_____

Auftragnehmer – Spruck IT Service GmbH

Anlage 1: Technische und organisatorische Maßnahmen

gemäß Art. 32 DSGVO — Stand: März 2026

1. Zutrittskontrolle

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

- Geschäftsräume in O7, 6, 68161 Mannheim mit zwei massiven Haustüren und Sicherheitsschlössern
- Elektronische Videoüberwachung der Eingangsbereiche mit Aufzeichnung
- 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 alle Cloud-Dienste und administrativen Zugänge
- Zentrale Passwortverwaltung über selbst gehosteten Passwortmanager (Vaultwarden) mit verschlüsselter Datenbank
- Automatische Bildschirmsperre nach Inaktivität auf allen Arbeitsplätzen
- ESET Endpoint Security auf allen Endgeräten mit zentraler Verwaltung über 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 Cloud-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 alle geschäftliche Kommunikation
- Nutzung passwortgeschützter, verschlüsselter Übertragungswege für den Austausch sensibler Daten
- VPN-Verschlüsselung für alle Standortvernetzungen und Remote-Zugriffe
- Ausschließliche Nutzung von HTTPS für Webzugriffe auf verwaltete Systeme

– Keine unverschlüsselte Übertragung personenbezogener Daten

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 dokumentiertem Bearbeitungsverlauf
– Audit-Logs in den verwalteten Cloud-Plattformen (Microsoft Entra, Microsoft 365)
– Protokollierung administrativer Zugriffe auf Kundensysteme

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
– Sicherstellung und Dokumentation der Datenlöschung nach Auftragsbeendigung

7. Verfügbarkeitskontrolle

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

– Backup-Konzept mit lokaler und Cloud-basierter Sicherung (georedundant)
– Einsatz unterbrechungsfreier Stromversorgung (USV) für kritische Systeme
– ESET Endpoint Security mit Echtzeitschutz und automatischen Signatur-Updates
– Cisco Meraki Firewall mit IDS/IPS zum Schutz der Netzwerkinfrastruktur
– Regelmäßiges Patch-Management für Betriebssysteme und Anwendungen
– Notfallplanung und dokumentierte Wiederherstellungsverfahren

8. Trennungsgebot

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

– Logische Mandantentrennung in allen eingesetzten Systemen
– 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)

Anlage 2: Unterauftragsverarbeiter

Folgende Unterauftragsverarbeiter sind vom Auftraggeber genehmigt:

Unternehmen	Leistung	Standort
Microsoft Ireland Operations Ltd.	Cloud-Infrastruktur (Microsoft 365, Azure, Entra ID)	EU (Irland/Niederlande)
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)
3CX Ltd.	Cloud-Telefonanlage (3CX Hosted PBX)	EU (Deutschland/Irland)

Änderungen an der Liste der Unterauftragsverarbeiter werden dem Auftraggeber vorab mitgeteilt. Der Auftraggeber kann innerhalb von 14 Tagen nach Mitteilung widersprechen.

Stand: März 2026

Anlage 3: Weisungsberechtigte Personen

Weisungsberechtigt auf Seiten des Auftraggebers:

Name: _____
Funktion: _____
E-Mail: _____
Telefon: _____

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.