Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Bezeichnung	Angaben
Auftragnehmer / Auftragsverarbeiter	schober24.com Deutschland – Professionelle IT-Dienstleistungen Einzelunternehmen, vertreten durch den Inhaber Thorsten P. Schober Friedrichsring 44, 68161 Mannheim, Deutschland E-Mail Datenschutz: datenschutz@schober24.com
Auftraggeber / Kunde	Die natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die mit schober24.com Deutschland ein Vertragsverhältnis über IT-Leistungen eingeht und diese Vereinbarung elektronisch, insbesondere durch Zahlung der ausdrücklich als Vertragsangebot bezeichneten ersten Rechnung, annimmt oder in deren Vertragsverhältnis sie wirksam einbezogen wird.
Fassung	Online-Masterfassung | Stand: 23. Juni 2026
Geltungsbeginn	Mit elektronischer Annahme dieser Vereinbarung, insbesondere durch vorbehaltlose Zahlung der ersten ausdrücklich als Vertragsangebot bezeichneten Rechnung, oder mit sonstiger wirksamer Einbeziehung in das jeweilige Vertragsverhältnis über IT-Leistungen.

§ 1 Gegenstand, Rangfolge und Anwendungsbereich

1. Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Zusammenhang mit sämtlichen gegenwärtigen und zukünftigen Vertragsverhältnissen über IT-Leistungen zwischen den Parteien (nachfolgend „Leistungsverhältnis“). Eine gesonderte Bezeichnung, Vertragsnummer oder Nennung des jeweiligen Leistungsverhältnisses in dieser Vereinbarung ist nicht erforderlich.

2. Auftraggeber oder Kunde ist die Person oder Stelle, die IT-Leistungen des Auftragnehmers beauftragt und diese Vereinbarung elektronisch, insbesondere durch vorbehaltlose Zahlung der ersten ausdrücklich als Vertragsangebot bezeichneten Rechnung, annimmt oder in deren Leistungsverhältnis sie sonst wirksam einbezogen wird. Der Auftraggeber muss in dieser Vereinbarung nicht namentlich genannt werden. Seine Identität ergibt sich aus dem Kundenkonto, Bestellvorgang, Angebot, Auftrag, Ticket, Zahlungsvorgang oder sonstigen Vertragsunterlagen des jeweiligen Leistungsverhältnisses.

3. Art und Umfang der tatsächlich beauftragten Leistungen bestimmen sich aus dem jeweiligen Leistungsverhältnis. Anlage 1 beschreibt den möglichen Leistungsrahmen; nur tatsächlich beauftragte oder zur Vertragserfüllung erforderliche Leistungsbausteine werden durchgeführt.

4. Die Vereinbarung gilt nur, soweit der Auftraggeber für die Verarbeitung Verantwortlicher oder seinerseits Auftragsverarbeiter ist und der Auftragnehmer personenbezogene Daten weisungsgebunden verarbeitet. Für private Tätigkeiten einer natürlichen Person außerhalb des Anwendungsbereichs der DSGVO gilt sie nicht.

5. Bei Widersprüchen gehen die datenschutzrechtlichen Regelungen dieser Vereinbarung dem jeweiligen Leistungsverhältnis vor. Individuelle, ausdrücklich als solche bezeichnete Datenschutzvereinbarungen gehen dieser universellen Fassung vor.

6. Die Anlagen sind Bestandteil dieser Vereinbarung. Nicht beauftragte optionale Leistungsbausteine begründen keine Verarbeitungspflicht.

§ 2 Dauer der Verarbeitung

Die Verarbeitung beginnt mit Aufnahme der auftragsbezogenen Leistung und dauert grundsätzlich für die Laufzeit des jeweiligen Leistungsverhältnisses. Bestehen mehrere Leistungsverhältnisse, gilt diese Vereinbarung bis zur Beendigung des letzten Leistungsverhältnisses, in dessen Rahmen eine Auftragsverarbeitung erfolgt. Einzelne Pflichten, insbesondere Vertraulichkeit, Nachweis, Rückgabe und Löschung, bestehen nach dessen Ende fort, soweit dies ihrer Natur nach erforderlich ist.

§ 3 Weisungsgebundene Verarbeitung

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, einschließlich hinsichtlich einer Übermittlung an ein Drittland, soweit keine bindende gesetzliche Verpflichtung entgegensteht. In diesem Fall informiert er den Auftraggeber vor der Verarbeitung, sofern das Recht eine solche Information nicht verbietet.

2. Das jeweilige Leistungsverhältnis, diese Vereinbarung, Supporttickets und nachweisbare Mitteilungen autorisierter Ansprechpartner gelten als dokumentierte Weisungen. Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen.

3. Hält der Auftragnehmer eine Weisung für datenschutzrechtswidrig, informiert er den Auftraggeber

Kontakt Telefonisch: 01805 - 554 887* • Telefax: 01805 - 002 510* • E-Mail: info@schober24.com • Im Internet: http://www.schober24.com
Persönlich: Friedrichsring 44 (nähe Gewerkschaftshaus / Collinicenter) • 68161 Mannheim • E-Mail: friedrichsring@schober24.com
per Post: Verwaltung • S 6, 23 • 68161 Mannheim • E-Mail: verwaltung@schober24.com
Konto Deutsche Bank PGK Mannheim (BLZ: 670 700 24) • Konto: 0152595
IBAN: DE78670700240001525950O • SWIFT/BIC: DEUTDEDBMAN
Rechtliches Geschäftsführung: Thorsten P. Schober (CEO) • Steuernummer: 38408/29494 • USt-ID: DE240222935
Es gelten unsere Allgemeinen Geschäftsbedingungen (siehe auch http://www.schober24.com/agb.php)
*0,14 € / Min. aus dem Festnetz, max. 0,42 € / Min. aus den Mobilfunknetzen.

unverzüglich und darf deren Ausführung bis zur Bestätigung oder Änderung aussetzen.

4. Der Auftragnehmer bestimmt die zur sicheren Leistungserbringung erforderlichen technischen und organisatorischen Mittel, soweit dadurch Zwecke und wesentliche Mittel der Verarbeitung nicht entgegen den Weisungen des Auftraggebers festgelegt werden.

§ 4 Vertraulichkeit und zugriffsberechtigte Personen

1. Der Auftragnehmer gewährleistet, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Zugriff erhalten nur der Inhaber sowie ausdrücklich autorisierte Beschäftigte und Unterauftragnehmer nach dem Erforderlichkeits- und Berechtigungsprinzip.

2. Personenbezogene Inhalte, die bei Fernwartung, Administration oder Fehleranalyse lediglich sichtbar werden, dürfen nicht für eigene Zwecke verwendet werden. Eine Dokumentation solcher Inhalte erfolgt nur, wenn sie zur Fehlerbehebung erforderlich und von der Weisung gedeckt ist.

3. Screenshots, Protokollauszüge oder Dateien dürfen nur erstellt bzw. übertragen werden, soweit dies für Diagnose, Nachweis oder Behebung erforderlich ist. Besonders sensible oder geheimnisgeschützte Inhalte sind soweit praktikabel zu minimieren oder zu schwärzen.

§ 5 Fernzugriff, Monitoring und Kundenkonten

1. Bei Ad-hoc-Leistungen erfolgt der Zugriff nach dem im jeweiligen Leistungsverhältnis oder im Einzelfall vereinbarten Freigabemodell. Eine aktive Freigabe ist nur geschuldet, wenn dies vereinbart wurde oder technisch vorgesehen ist.

2. Bei IT-Betreuungspaketen ist der unbeaufsichtigte Fernzugriff auf die betreuten Systeme Bestandteil der Weisung und darf jederzeit erfolgen, soweit dies für Support, Wartung, Monitoring, Sicherheit, Fehlerbehebung oder die vereinbarte Betriebsführung erforderlich ist. Zugriffe ohne Leistungsbezug oder zu privaten Zwecken sind unzulässig.

3. Fernzugriffe werden im Rahmen der technischen Möglichkeiten protokolliert. Datenübertragungen sind zulässig, soweit sie für die Leistung erforderlich sind. Sitzungsaufzeichnungen erfolgen nicht regelmäßig und nur bei konkretem Bedarf, dokumentierter Weisung oder vorheriger Information.

4. Soweit Kunden eigene Konten oder Freigabelinks erhalten, trägt der Auftraggeber Verantwortung für deren interne Zuweisung und sichere Nutzung. Der Auftragnehmer stellt verfügbare Sicherheitsfunktionen, einschließlich Mehrfaktor-Authentifizierung, bereit; privilegierte Konten des Auftragnehmers und seiner Unterauftragnehmer werden mit Mehrfaktor-Authentifizierung geschützt.

5. Monitoring erfolgt nur, wenn es vereinbart ist. Technische Bestands- und Verbindungsinformationen, die bei einer Fernwartungsverbindung systembedingt anfallen, dürfen auch bei Ad-hoc-Leistungen verarbeitet werden, soweit dies für Verbindung, Sicherheit und Fehleranalyse erforderlich ist.

§ 6 Sicherheit der Verarbeitung

1. Der Auftragnehmer trifft die in Anlage 3 beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Die Maßnahmen berücksichtigen insbesondere die Möglichkeit des Vollzugriffs auf Kundensysteme sowie die Verarbeitung besonderer Kategorien personenbezogener Daten.

2. Die Maßnahmen dürfen dem technischen Fortschritt entsprechend weiterentwickelt werden, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche nachteilige Änderungen teilt der Auftragnehmer dem Auftraggeber mit.

§ 7 Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen angemessen bei der Erfüllung von Betroffenenrechten, bei der Sicherheit der Verarbeitung, bei Meldungen und Benachrichtigungen von Datenschutzverletzungen sowie bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen. Anfragen betroffener Personen leitet er unverzüglich an den Auftraggeber weiter und beantwortet sie nicht eigenständig, sofern keine Weisung oder gesetzliche Pflicht besteht.

§ 8 Datenschutzverletzungen

Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit dem Auftrag bekannt geworden ist. Die Meldung enthält, soweit verfügbar, Art und Umfang des Vorfalls, betroffene Daten und Personen, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Maßnahmen sowie eine Kontaktstelle. Noch fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht.

§ 9 Unterauftragsverarbeiter

1. Der Auftraggeber erteilt die allgemeine Genehmigung zum Einsatz der in Anlage 4 aufgeführten Unterauftragsverarbeiter. Der Auftragnehmer informiert den Auftraggeber mindestens 14 Kalendertage vor der beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform, soweit nicht ein dringender Sicherheits- oder Ausfallfall eine kürzere Frist erfordert.

2. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund innerhalb der Informationsfrist widersprechen. Die Parteien bemühen sich um eine zumutbare Alternative. Ist keine Lösung möglich, kann der betroffene Leistungsbaustein unter Einhaltung der vertraglichen Regelungen beendet werden.

3. Der Auftragnehmer verpflichtet Unterauftragsverarbeiter mindestens zu den Datenschutzpflichten, die für ihre Leistungen relevant und inhaltlich dieser Vereinbarung gleichwertig sind. Er bleibt gegenüber dem Auftraggeber für deren Pflichterfüllung verantwortlich.

4. Reine Nebenleistungen ohne Zugriffsmöglichkeit auf auftragsbezogene personenbezogene Daten gelten nicht als Unterauftragsverarbeitung.

Kontakt Telefonisch: 01805 - 554 887* • Telefax: 01805 - 002 510* • E-Mail: info@schober24.com • Im Internet: http://www.schober24.com
Persönlich: Friedrichsring 44 (nähe Gewerkschaftshaus / Collinicenter) • 68161 Mannheim • E-Mail: friedrichsring@schober24.com
per Post: Verwaltung • S 6, 23 • 68161 Mannheim • E-Mail: verwaltung@schober24.com
Konto Deutsche Bank PGK Mannheim (BLZ: 670 700 24) • Konto: 0152595
IBAN: DE78670700240001525950O • SWIFT/BIC: DEUTDEDBMAN
Rechtliches Geschäftsführung: Thorsten P. Schober (CEO) • Steuernummer: 38408/29494 • USt-ID: DE240222935
Es gelten unsere Allgemeinen Geschäftsbedingungen (siehe auch http://www.schober24.com/agb.php)
*0,14 € / Min. aus dem Festnetz, max. 0,42 € / Min. aus den Mobilfunknetzen.

§ 10 Drittlandübermittlungen

1. Verarbeitung außerhalb des Europäischen Wirtschaftsraums erfolgt nur auf dokumentierte Weisung und unter Einhaltung der Art. 44 ff. DSGVO. Vorrangig werden Angemessenheitsbeschlüsse genutzt; andernfalls sind geeignete Garantien, insbesondere Standardvertragsklauseln und erforderlichenfalls ergänzende Maßnahmen, zu vereinbaren.

2. Die Schweiz gilt aus Sicht der Europäischen Union als Staat mit angemessenem Datenschutzniveau. Soweit der Auftraggeber dem schweizerischen Datenschutzrecht unterliegt, wirken die Parteien bei der Erfüllung der dort anwendbaren Pflichten angemessen zusammen.

3. Der bloße Aufenthalt eines Mitarbeiters oder Ansprechpartners des Auftraggebers in einem Drittland ist keine vom Auftragnehmer veranlasste Drittlandübermittlung. Fernzugriffe des Auftragnehmers oder seiner Unterauftragnehmer aus einem Drittland bedürfen dagegen einer datenschutzrechtlichen Grundlage und sind in Anlage 4 auszuweisen.

§ 11 Nachweise und Kontrollen

1. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung von Art. 28 DSGVO zur Verfügung und ermöglicht angemessene Überprüfungen einschließlich Inspektionen durch den Auftraggeber oder einen zur Verschwiegenheit verpflichteten Prüfer.

2. Kontrollen sind grundsätzlich mit angemessener Frist anzukündigen, während üblicher Geschäftszeiten durchzuführen und auf das Erforderliche zu begrenzen. Betriebs- und Geschäftsgeheimnisse sowie Daten anderer Kunden sind zu schützen. Bei konkretem Verdacht auf einen erheblichen Verstoß oder nach einem relevanten Sicherheitsvorfall kann die Ankündigungsfrist angemessen verkürzt werden.

3. Nachweise durch aktuelle Prüfberichte, Zertifikate, Protokollauszüge oder Selbstauskünfte können eine Vor-Ort-Prüfung ersetzen, soweit sie den Prüfzweck erfüllen.

§ 12 Rückgabe, Löschung und Aufbewahrung

1. Nach Ende der Leistung gibt der Auftragnehmer auf Weisung alle personenbezogenen Daten und Datenträger zurück oder löscht sie, sofern keine gesetzliche Aufbewahrungspflicht besteht. Produktivdaten werden grundsätzlich spätestens innerhalb von 60 Tagen gelöscht.

2. Zugangsdaten und IT-Dokumentationen werden nach einer vereinbarten Übergabe unwiederbringlich aus den produktiven, vom Auftragnehmer zugänglichen Systemen gelöscht. Daten in kundeneigenen, für den Auftragnehmer nicht freigegebenen Tresoren bleiben unter Kontrolle des Kunden.

3. Fernwartungs-, Monitoring-, Support- und technische Protokolldaten werden grundsätzlich für 60 Tage gespeichert, soweit nicht eine kürzere Frist, eine dokumentierte Weisung, ein Sicherheitsvorfall oder eine gesetzliche bzw. vertragliche Nachweispflicht eine abweichende Frist erfordert.

4. Daten in laufenden Sicherungen werden nicht allein zur Einzeldateilöschung reaktiviert. Sie werden mit dem regulären Sicherungszyklus überschrieben oder gelöscht und dürfen bei einer Wiederherstellung nur zu Sicherungs- und Wiederanlaufzwecken verarbeitet werden.

5. Gesetzlich aufzubewahrende Daten werden gesperrt und nur für den gesetzlichen Zweck verarbeitet. Der Auftragnehmer bestätigt die Löschung auf angemessene Anfrage.

§ 13 Berufs- und besondere Geheimnisse

1. Soweit der Auftragnehmer bei Leistungen für Ärzte, Rechtsanwälte oder andere Berufsgeheimnisträger Kenntnis von Geheimnissen im Sinne des § 203 StGB erlangen kann, wird er als mitwirkende Person tätig und wahrt die fremden Geheimnisse auch über das Vertragsende hinaus.

2. Der Auftragnehmer unterrichtet mitwirkende Beschäftigte und sonstige mitwirkende Personen über ihre Geheimhaltungspflicht und verpflichtet sie in geeigneter Form. Weitere Personen werden nur eingesetzt, soweit dies für die Leistung erforderlich und vom Auftraggeber nach dieser Vereinbarung genehmigt ist.

3. Der Auftraggeber bleibt dafür verantwortlich, dass die Einbeziehung des Auftragnehmers berufsrechtlich zulässig ist, und erteilt die erforderlichen Informationen und Weisungen. Gesetzlich strengere Geheimhaltungs-, Beschlagnahmeschutz- oder Berufsregeln bleiben unberührt.

§ 14 Verantwortlichkeit und Mitwirkung des Auftraggebers

Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung, die Rechtsgrundlagen, Informationspflichten, Weisungen und die Wahrung der Rechte betroffener Personen verantwortlich. Er informiert den Auftragnehmer über besondere Schutzbedarfe und konfiguriert kundenseitige Berechtigungen sorgfältig. Er darf keine Weisungen erteilen, die gegen anwendbares Datenschutzrecht verstoßen.

§ 15 Schlussbestimmungen

1. Änderungen und Ergänzungen dieser Vereinbarung einschließlich Weisungen bedürfen mindestens der Textform, soweit nicht gesetzlich eine strengere Form verlangt wird.

2. Soweit eine Regelung unwirksam ist oder wird, bleibt die Wirksamkeit der übrigen Regelungen unberührt. An ihre Stelle tritt die gesetzliche Regelung.

3. Es gilt das im jeweiligen Leistungsverhältnis vereinbarte Recht und der dort vereinbarte Gerichtsstand, soweit zulässig. Zwingendes Datenschutzrecht bleibt unberührt.

Kontakt Telefonisch: 01805 - 554 887* • Telefax: 01805 - 002 510* • E-Mail: info@schober24.com • Im Internet: http://www.schober24.com
Persönlich: Friedrichsring 44 (nähe Gewerkschaftshaus / Collinicenter) • 68161 Mannheim • E-Mail: friedrichsring@schober24.com
per Post: Verwaltung • S 6, 23 • 68161 Mannheim • E-Mail: verwaltung@schober24.com
Konto Deutsche Bank PGK Mannheim (BLZ: 670 700 24) • Konto: 0152595
IBAN: DE78670700240001525950O • SWIFT/BIC: DEUTDEDBMAN
Rechtliches Geschäftsführung: Thorsten P. Schober (CEO) • Steuernummer: 38408/29494 • USt-ID: DE240222935
Es gelten unsere Allgemeinen Geschäftsbedingungen (siehe auch http://www.schober24.com/agb.php)
*0,14 € / Min. aus dem Festnetz, max. 0,42 € / Min. aus den Mobilfunknetzen.

Anlage 1 – Gegenstand und Leistungsbausteine
Die konkrete Auswahl ergibt sich aus dem jeweiligen Leistungsverhältnis oder aus der tatsächlich angeforderten und erbrachten Leistung. Eine gesonderte Zuordnung dieser Anlage zu einer Vertragsnummer ist nicht erforderlich. Alle Bausteine können Zugriff auf personenbezogene Daten einschließlich besonderer Kategorien und geheimnisgeschützter Inhalte ermöglichen.

Leistungsbaustein	Verarbeitung / Systeme
IT-Support und Ad-hoc-Fernwartung	Fehleranalyse, Unterstützung und Fernsteuerung; Verbindung je nach Vereinbarung mit aktiver Freigabe oder vorhandenem unbeaufsichtigtem Zugriff. Primär MeshCentral, hilfsweise TeamViewer oder RustDesk.
IT-Betreuung / Managed Services	Unbeaufsichtigter Zugriff auf vereinbarte Geräte und Systeme; Wartung, Administration, Sicherheit, Patch- und Störungsbearbeitung.
Monitoring	MeshCentral, GLPI, Tactical RMM. Erfassung technischer Gerätedaten, IP-Adressen, Softwarebestand, Protokolle, Patchstatus, Sicherheitsmeldungen, Registry-Informationen, Benutzernamen und Power-Status. Keine Überwachung von Browseraktivitäten oder Eingaben.
Passwort- und IT-Dokumentation	Psono, lokal auf Synology NAS: Zugangsdaten, 2FA-Daten, Geräte, Netzwerkstrukturen, Provider- und Dienstleisterzugänge sowie sonstige MSP-relevante Dokumentation in einer Baumstruktur.
Ticket- und Kommunikationsbearbeitung	osTicket sowie selbst gehostete E-Mail-Systeme zur Aufnahme, Bearbeitung und Dokumentation von Supportvorgängen.
Datensicherung	Lokale Sicherungen und verschlüsselte bzw. zugriffsgeschützte externe Sicherungen nach Anlage 3.

Art und Zweck der Verarbeitung
Erheben durch technischen Anfall, Auslesen, Erfassen, Ordnen, Speichern, Anpassen, Übertragen, Abfragen, Einsehen, Verwenden, Abgleichen, Einschränken und Löschen – jeweils ausschließlich zur Erbringung, Absicherung, Dokumentation und Abrechnung der vereinbarten IT-Leistungen.

Anlage 2 – Datenarten und betroffene Personen

Kategorie	Beispiele
Stamm- und Kontaktdaten	Namen, Anschriften, Kommunikationsdaten, Firmenzugehörigkeit, Ansprechpartner
Benutzer- und Identifikationsdaten	Benutzernamen, IDs, Rollen, Berechtigungen, Gerätezuordnungen
Authentifizierungs- und Geheimnisdaten	Kennwörter, Schlüssel, Tokens, 2FA-Daten, Zugangsdaten
IT- und Protokolldaten	IP-Adressen, Geräte-, Hardware-, Software-, Netzwerk-, Registry-, Ereignis-, Sicherheits- und Verbindungsdaten
Kommunikations- und Supportdaten	E-Mails, Tickets, Fehlerbeschreibungen, Screenshots, Protokollauszüge, übertragene Dateien
Inhalts- und Geschäftsdaten	Dateien, Datenbanken, Dokumente, Vertrags-, Kunden-, Beschäftigten-, Mandats- und Behandlungsinformationen
Besondere Kategorien nach Art. 9 DSGVO	Insbesondere Gesundheitsdaten; je nach Kundensystem weitere besonders geschützte Daten
Berufsgeheimnisse	Patienten-, Mandanten- und sonstige nach § 203 StGB oder Berufsrecht geschützte Informationen

Betroffene Personengruppen
Beschäftigte, Bewerber, freie Mitarbeiter und Organmitglieder des Auftraggebers
Kunden, Interessenten, Lieferanten, Partner und sonstige Ansprechpartner
Patienten, Mandanten, Klienten und deren Angehörige oder Vertreter
Nutzer, Websitebesucher und Kommunikationspartner
Sonstige Personen, deren Daten sich in den betreuten Systemen befinden

Kontakt Telefonisch: 01805 - 554 887* • Telefax: 01805 - 002 510* • E-Mail: info@schober24.com • Im Internet: http://www.schober24.com
Persönlich: Friedrichsring 44 (nähe Gewerkschaftshaus / Collinicenter) • 68161 Mannheim • E-Mail: friedrichsring@schober24.com
per Post: Verwaltung • S 6, 23 • 68161 Mannheim • E-Mail: verwaltung@schober24.com
Konto Deutsche Bank PGK Mannheim (BLZ: 670 700 24) • Konto: 0152595
IBAN: DE78670700240001525950O • SWIFT/BIC: DEUTDEDBMAN
Rechtliches Geschäftsführung: Thorsten P. Schober (CEO) • Steuernummer: 38408/29494 • USt-ID: DE240222935
Es gelten unsere Allgemeinen Geschäftsbedingungen (siehe auch http://www.schober24.com/agb.php)
*0,14 € / Min. aus dem Festnetz, max. 0,42 € / Min. aus den Mobilfunknetzen.

Anlage 3 – Technische und organisatorische Maßnahmen

Unternehmen: schober24.com Deutschland
Branche: IT-Dienstleistungen
Stand: 23. Juni 2026
Rechtsgrundlage: Art. 25 und Art. 32 DSGVO

Die nachfolgenden Maßnahmen beschreiben das zum angegebenen Stand implementierte Schutzniveau. Sie sind risikoorientiert anzuwenden, regelmäßig auf Wirksamkeit zu überprüfen und bei technischen, organisatorischen oder rechtlichen Änderungen fortzuschreiben.

1. Zutrittskontrolle – Schutz der Betriebs- und Infrastrukturstandorte

Zutritt zum Büro-/Wohnbereich nur mit Schlüssel.
Alarmanlage vorhanden.
Videoüberwachung am Eingang.
Kein separates Laden- oder Büroobjekt; die Leistungserbringung erfolgt überwiegend mobil. Lokale Server- und Speicherinfrastruktur befindet sich im gesicherten Büro-/Wohnbereich.

2. Zutrittskontrolle – Unterlagen und Datenträger
Vorrangig digitale und papierarme Ablage.
Aktenvernichter mit Sicherheitsstufe P-4 oder höher für schutzbedürftige Papierunterlagen.
Datenträger und IT-Systeme werden innerhalb des zugangsgeschützten Bereichs aufbewahrt.

3. Zugangskontrolle – IT-Systeme
Zwei-Faktor-Authentifizierung für privilegierte Konten des Inhabers und eingesetzter Unterauftragnehmer.
Automatische Bildschirmsperre nach Inaktivität.
Biometrische Authentifizierung, insbesondere Fingerabdruck oder Face ID, auf unterstützten Geräten.
Passwort-Manager zur sicheren Verwaltung von Zugangsdaten.

4. Zugangskontrolle – Benutzer- und Berechtigungsverwaltung
Regelzugriff durch den Inhaber des Einzelunternehmens.
Getrennte Konten für private und geschäftliche Nutzung.
Temporäre und zweckgebundene Zugänge für Freelancer und Dienstleister.
Dokumentation der vergebenen Zugänge und Berechtigungen.
Kundenzugänge werden auf den jeweiligen Kundenbereich beschränkt; Mehrfaktor-Authentifizierung ist für Kundenkonten technisch zuschaltbar.

5. Zugriffskontrolle – Datenzugriff
Verschlüsselung der eingesetzten Festplatten und SSDs.
Zusätzlicher Passwortschutz für sensible Dateien, soweit erforderlich.
Strukturierte Ablage mit rollen- und aufgabenbezogenen Zugriffsrechten.
Mandantenbezogene Freigaben in Psono; kundeneigene, nicht freigegebene Tresore sind für den Auftragnehmer nicht zugänglich.

6. Übertragungskontrolle – sichere Datenübertragung
E-Mail-Verschlüsselung mittels S/MIME oder PGP, soweit vom Kommunikationspartner unterstützt und für den Übermittlungsvorgang eingesetzt.
HTTPS/TLS für Webseiten, Verwaltungsoberflächen und Portale.
Fernwartungs- und Administrationsverbindungen erfolgen über verschlüsselte Verbindungen der eingesetzten Systeme.

7. Eingabekontrolle – Nachvollziehbarkeit
Zeitstempel und systemseitige Protokollierung bei Einträgen und administrativen Vorgängen, soweit die eingesetzten Systeme dies unterstützen.
Protokollierung von Fernzugriffen in MeshCentral; Regelspeicherdauer 60 Tage.
Sicherung vor wichtigen Änderungen, soweit Art und Risiko der Änderung dies erfordern.

8. Weitergabekontrolle
Keine Weitergabe personenbezogener Daten ohne Rechtsgrundlage, dokumentierte Weisung oder vertragliche Erforderlichkeit.
Datenübertragungen im Support werden auf den für Diagnose und Fehlerbehebung erforderlichen Umfang beschränkt.
Unterauftragnehmer erhalten nur die für den jeweiligen Auftrag erforderlichen Zugriffe.

9. Verfügbarkeitskontrolle und Wiederherstellbarkeit
Tägliche automatische Datensicherungen.
Zusätzliche externe Sicherung auf einer Storage Box neben lokalen Sicherungen.
Unterbrechungsfreie Stromversorgung (USV) für lokale Infrastruktur.
Wiederherstellung aus Sicherungen nach Bedarf und im Rahmen der technischen Möglichkeiten.

10. Trennungskontrolle

Kontakt Telefonisch: 01805 - 554 887* • Telefax: 01805 - 002 510* • E-Mail: info@schober24.com • Im Internet: http://www.schober24.com
Persönlich: Friedrichsring 44 (nähe Gewerkschaftshaus / Collinicenter) • 68161 Mannheim • E-Mail: friedrichsring@schober24.com
per Post: Verwaltung • S 6, 23 • 68161 Mannheim • E-Mail: verwaltung@schober24.com
Konto Deutsche Bank PGK Mannheim (BLZ: 670 700 24) • Konto: 0152595
IBAN: DE78670700240001525950O • SWIFT/BIC: DEUTDEDBMAN
Rechtliches Geschäftsführung: Thorsten P. Schober (CEO) • Steuernummer: 38408/29494 • USt-ID: DE240222935
Es gelten unsere Allgemeinen Geschäftsbedingungen (siehe auch http://www.schober24.com/agb.php)
*0,14 € / Min. aus dem Festnetz, max. 0,42 € / Min. aus den Mobilfunknetzen.

Separate E-Mail-Konten für unterschiedliche Zwecke.
Logische Mandantentrennung in den eingesetzten Software-Systemen.
Kundenbezogene Baum-, Tresor-, Geräte- und Berechtigungsstrukturen.
Trennung privater und geschäftlicher Benutzerkonten.

11. Integrität und Authentizität
Digitale Signaturen für wichtige Dokumente, soweit im jeweiligen Geschäftsprozess eingesetzt.
PDF/A für Dokumente, die zur Langzeitarchivierung vorgesehen sind.
Verschlüsselte Übertragungswege und zugriffsgeschützte Ablagen zum Schutz gegen unbefugte Änderung.

12. Pseudonymisierung und Datenminimierung
Verwendung von Kundennummern statt Namen in Analysen, soweit der jeweilige Zweck dies erlaubt.
Beschränkung von Screenshots, Protokollauszügen und übertragenen Dateien auf das für die Fehlerbehebung erforderliche Maß.

13. Belastbarkeit und Resilienz
Aktivierte und konfigurierte Firewalls.
Regelmäßige Sicherheits- und Softwareupdates.
Redundante Internetverbindung.
Mehrfaktor-Authentifizierung für privilegierte Zugänge.

14. Löschungskontrolle
Löschung nach dokumentierten Regelfristen und Weisungen; Regelfrist für auftragsbezogene operative Daten 60 Tage, soweit keine abweichende Pflicht oder Vereinbarung besteht.
Sichere, dem jeweiligen Medium angemessene Löschverfahren; Überschreiben, soweit technisch geeignet, ansonsten insbesondere kryptographisches Löschen, Herstellerverfahren oder physische Vernichtung.
Aussonderung und sichere Vernichtung nicht mehr benötigter Papierunterlagen und Datenträger.

15. Überprüfung und Evaluierung
Mindestens jährliche Überprüfung der technischen und organisatorischen Maßnahmen.
Anlassbezogene Anpassung bei neuen Risiken, Sicherheitsvorfällen, Systemwechseln oder geänderten rechtlichen Anforderungen.
Kontrolle der Wirksamkeit gemäß Art. 32 Abs. 1 Buchst. d DSGVO.

16. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
Opt-in statt Opt-out, soweit eine Verarbeitung auf Einwilligung gestützt wird.
Minimale Berechtigungen für neue Nutzer und Zugänge.
Datenminimierung und mandantenbezogene Freigaben bei der Systemkonfiguration.

17. Auftragskontrolle
Verarbeitung nur im Rahmen dokumentierter Weisungen.
Regelmäßige, risikoorientierte Kontrolle eingesetzter Dienstleister und Unterauftragnehmer.
Vertraulichkeitsverpflichtung und zweckbezogene Berechtigungen für eingesetzte Personen.
Dokumentation der Unterauftragnehmer und Durchführung des vertraglichen Änderungsverfahrens.

Prüfung und Freigabe der TOM
Diese Dokumentation ist regelmäßig zu überprüfen und bei Bedarf zu aktualisieren. Die Wirksamkeit der Maßnahmen wird gemäß Art. 32 Abs. 1 Buchst. d DSGVO regelmäßig evaluiert.

Freigabe	Angaben
Ort / Datum	_____
Name / Funktion	Thorsten P. Schober, Inhaber
Unterschrift	_____

Anlage 4 – Unterauftragnehmer und Betriebsumgebung

Nur Anbieter, die auftragsbezogene personenbezogene Daten verarbeiten können, sind Unterauftragsverarbeiter. Selbst betriebene Software ist zur Transparenz als Betriebsumgebung aufgeführt.

Anbieter / System	Leistung und Ort	Status
STRATO AG	V-Server für MeshCentral und selbst gehosteten RustDesk-Connection-Server; Betrieb innerh. EU	Unterauftragnehmer
IONOS SE	Dedicated Server für osTicket und E-Mail; Betrieb innerh. EU	Unterauftragnehmer
Hetzner Online GmbH	Storage Box für Datensicherungen; Betrieb innerh. EU	Unterauftragnehmer

Kontakt Telefonisch: 01805 - 554 887* • Telefax: 01805 - 002 510* • E-Mail: info@schober24.com • Im Internet: http://www.schober24.com
Persönlich: Friedrichsring 44 (nähe Gewerkschaftshaus / Collinicenter) • 68161 Mannheim • E-Mail: friedrichsring@schober24.com
per Post: Verwaltung • S 6, 23 • 68161 Mannheim • E-Mail: verwaltung@schober24.com
Konto Deutsche Bank PGK Mannheim (BLZ: 670 700 24) • Konto: 0152595
IBAN: DE78670700240001525950O • SWIFT/BIC: DEUTDEDBMAN
Rechtliches Geschäftsführung: Thorsten P. Schober (CEO) • Steuernummer: 38408/29494 • USt-ID: DE240222935
Es gelten unsere Allgemeinen Geschäftsbedingungen (siehe auch http://www.schober24.com/agb.php)
*0,14 € / Min. aus dem Festnetz, max. 0,42 € / Min. aus den Mobilfunknetzen.

Anbieter / System	Leistung und Ort	Status
TeamViewer Germany GmbH / maßgebliche Konzerngesellschaft	TeamViewer Corporate für hilfsweise Fernwartung bis Vertragsende	Unterauftragnehmer
Externe IT-Partner	Bundes-IT Verbund, u.a. Bodenmüller IT-Dienstleistungen, Mannheim ONIG OpenNetworkIT-Group, München	Unterauftragnehmer
Psono	Lokal innerhalb der Geschäftsinfrastruktur	Betriebsumgebung
MeshCentral / RustDesk	Selbst gehostete Fernwartung auf STRATO-V-Server / EU	Betriebsumgebung
GLPI	Monitoring/IT-Management; Betrieb innerhalb der EU	Betriebsumgebung
Tactical RMM	Nur bei künftiger Einführung; Hosting und etwaige Anbieter sind vor Einsatz nach dem Änderungsverfahren aufzunehmen.	Noch nicht eingesetzt
Lokaler Exchange Server	Innerhalb der geschäftlichen Infrastruktur	Betriebsumgebung

Anlage 5 – Kommunikation und Weisungsberechtigung
Weisungsberechtigt sind die vom Auftraggeber über sein Kundenkonto, im Bestell- oder Beauftragungsprozess, in einem Supportticket oder in sonstiger nachweisbarer Kommunikation benannten Personen. Der Auftragnehmer darf bei Zweifeln an Identität oder Berechtigung eine angemessene Bestätigung verlangen. Weisungs- und Datenschutzkontakt des Auftragnehmers ist Thorsten P. Schober, datenschutz@schober24.com, +49 (621) 15699977.

Elektronischer Abschluss und Einbeziehung

1. Diese Vereinbarung wird ohne handschriftliche Unterschrift elektronisch geschlossen. Die Annahme kann insbesondere durch Aktivieren einer nicht vorangekreuzten Checkbox, Betätigen einer eindeutig beschrifteten Schaltfläche, elektronische Bestätigung eines Angebots oder Auftrags, Registrierung bzw. Bestätigung in einem Kundenportal, vorbehaltlose Zahlung der ausdrücklich als Vertragsangebot bezeichneten ersten Rechnung oder eine sonstige eindeutige elektronische Annahmeerklärung erfolgen.

2. Soll der Vertrag durch Zahlung der ersten Rechnung zustande kommen, stellt die erste Rechnung zusammen mit der vollständigen Leistungsbeschreibung und den beigefügten Vertragsunterlagen das Vertragsangebot des Auftragnehmers dar. Die Rechnung muss eindeutig darauf hinweisen, dass der Kunde durch vorbehaltlose Zahlung den IT-Betreuungsvertrag einschließlich dieser Vereinbarung und ihrer Anlagen annimmt. Sämtliche einbezogenen Unterlagen sind dem Kunden vor der Zahlung vollständig und in dauerhaft speicherbarer Form bereitzustellen.

3. Eine Rechnung, die lediglich eine bereits anderweitig begründete Zahlungspflicht abrechnet, bewirkt für sich allein keine Annahme dieser Vereinbarung. Gleiches gilt für eine Zahlung, wenn der Hinweis auf die Vertragswirkung oder die vollständigen Vertragsunterlagen dem Kunden erst nach der Zahlung zugehen.

4. Alternativ kann diese Vereinbarung wirksam in ein Leistungsverhältnis einbezogen werden, wenn der Auftraggeber vor Abgabe seiner Vertragserklärung klar auf ihre Geltung hingewiesen wird, die vollständige Fassung über einen unmittelbar erreichbaren Link einsehen und dauerhaft speichern kann und der Geltung zustimmt.

5. Die Annahme gilt für alle gegenwärtigen und zukünftigen Leistungsverhältnisse zwischen den Parteien, soweit darin eine Auftragsverarbeitung erfolgt. Ein erneuter Abschluss für jeden Einzelauftrag, jedes Supportticket oder jedes Betreuungspaket ist nicht erforderlich.

6. Der Auftragnehmer dokumentiert die Identität des Auftraggebers, Versand und Inhalt des Vertragsangebots, die beigefügten oder verlinkten Unterlagen, die jeweilige Fassungs- oder Versionsnummer, den Zahlungseingang sowie den verwendeten Annahmeweg. Die versandte und angenommene Fassung wird beweissicher aufbewahrt.

7. Wesentliche Änderungen dieser Vereinbarung, insbesondere Änderungen des Verarbeitungsgegenstands, des Schutzniveaus oder der Rechte des Auftraggebers, werden dem Auftraggeber in Textform mitgeteilt und bedürfen einer erneuten wirksamen Einbeziehung oder Annahme, soweit die Änderung nicht bereits durch ein vereinbartes Änderungsverfahren gedeckt ist. Das Verfahren für Unterauftragnehmer nach § 9 bleibt unberührt.

Kontakt Telefonisch: 01805 - 554 887* • Telefax: 01805 - 002 510* • E-Mail: info@schober24.com • Im Internet: http://www.schober24.com
Persönlich: Friedrichsring 44 (nähe Gewerkschaftshaus / Collinicenter) • 68161 Mannheim • E-Mail: friedrichsring@schober24.com
per Post: Verwaltung • S 6, 23 • 68161 Mannheim • E-Mail: verwaltung@schober24.com
Konto Deutsche Bank PGK Mannheim (BLZ: 670 700 24) • Konto: 0152595
IBAN: DE78670700240001525950O • SWIFT/BIC: DEUTDEDBMAN
Rechtliches Geschäftsführung: Thorsten P. Schober (CEO) • Steuernummer: 38408/29494 • USt-ID: DE240222935
Es gelten unsere Allgemeinen Geschäftsbedingungen (siehe auch http://www.schober24.com/agb.php)
*0,14 € / Min. aus dem Festnetz, max. 0,42 € / Min. aus den Mobilfunknetzen.