Vertrag zur Auftragsverarbeitung

nach Art. 28 DSGVO

Auftragsverarbeiter (nachfolgend „Auftragnehmer“)	
Firma / Inhaber	Tobias Möller, Einzelunternehmer, handelnd unter „PC Service aus Schaumburg“
Anschrift	Riepacker Str. 19, 31691 Helpsen, Deutschland
Telefon	+49 (0)5724 / 98449
Mobil	+49 (0)171 / 5318613
Fax	+49 (0)5724 / 98450
E-Mail	info@pc-service-aus-schaumburg.de
Website	https://www.pc-service-aus-schaumburg.de

Verantwortlicher (nachfolgend „Auftraggeber“)	
Firma / Name	_____
Vertreten durch	_____
Anschrift	_____
Telefon	_____
E-Mail	_____

Auftragnehmer und Auftraggeber – nachstehend gemeinsam „die Parteien“ – schließen den folgenden Vertrag über die Verarbeitung personenbezogener Daten im Auftrag.

Präambel

Der Auftragnehmer erbringt für den Auftraggeber IT-Dienstleistungen rund um Computer, Notebook, Server, Netzwerk, Internet, Smart Home, Datensicherung und Fernwartung. Im Rahmen dieser Tätigkeiten kann der Auftragnehmer Zugriff auf personenbezogene Daten erhalten, für die der Auftraggeber datenschutzrechtlich Verantwortlicher im Sinne der Datenschutz-Grundverordnung (DSGVO) ist. Mit dem vorliegenden Vertrag regeln die Parteien diese Auftragsverarbeitung gemäß Art. 28 DSGVO.

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand: Auftragsverarbeitung im Rahmen aller vom Auftragnehmer erbrachten IT-Dienstleistungen, insbesondere:

- Computerreparatur und Hardware-Service vor Ort oder in der Werkstatt
- Softwareinstallation, Datenmigration, Einrichtung von Windows, macOS, Office und Anwendungssoftware

- DSL-, WLAN- und Netzwerkkonfiguration
- Smart-Home-Einrichtung und Funk-Nachrüstung
- Fernwartung (Remote-Support per Bildschirmübertragung)
- Backup- und Datensicherungs-Dienstleistungen, einschließlich verwalteter Cloud-Backups
- Beratung und laufende Betreuung im Rahmen von Wartungspaketen

(2) Dauer: Der Vertrag beginnt mit Unterzeichnung und läuft auf unbestimmte Zeit. Er endet mit Beendigung aller zugrundeliegenden Hauptverträge bzw. mit der vollständigen Erledigung der zuletzt beauftragten Leistung. Eine Kündigung mit Frist von einem Monat zum Monatsende ist jederzeit möglich.

(3) Hauptvertrag: Maßgeblich sind die jeweiligen Einzelaufträge (Auftragsformulare, Angebote, E-Mail-Bestätigungen) sowie die Allgemeinen Geschäftsbedingungen des Auftragnehmers.

§ 2 Konkretisierung der Verarbeitung

(1) Art und Zweck: Die Verarbeitung umfasst die Erbringung der unter § 1 Abs. 1 genannten IT-Dienstleistungen. Zwecke sind insbesondere Wartung, Fehlerbeseitigung, Einrichtung, Datenrettung und -migration, Backup, Sicherheitsmaßnahmen und Support.

(2) Art der personenbezogenen Daten:

- Stamm- und Kontaktdaten (Name, Anschrift, E-Mail, Telefon) – des Auftraggebers, seiner Mitarbeiter, Kunden, Lieferanten
- Kommunikationsdaten (E-Mails, Chats, gespeicherte Korrespondenz)
- Anmelde- und Zugangsdaten (Benutzernamen, soweit unvermeidbar Passwörter)
- Inhaltsdaten (Dokumente, Tabellen, Fotos, Datenbanken)
- Nutzungs- und Protokolldaten (Logfiles, Verbindungsdaten)
- Bei Privatkunden ggf. Daten von Familienmitgliedern
- Ggf. besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO, sofern diese auf den vom Auftraggeber bereitgestellten Systemen vorhanden sind

(3) Kategorien betroffener Personen:

- Auftraggeber und – sofern juristische Person – dessen gesetzliche Vertreter und Mitarbeiter
- Kunden, Interessenten, Lieferanten und sonstige Geschäftspartner des Auftraggebers
- Sonstige natürliche Personen, deren Daten auf den vom Auftraggeber bereitgestellten Systemen gespeichert sind

§ 3 Pflichten des Auftragnehmers

(1) Weisungsbindung: Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen dieses Vertrags und auf dokumentierte Weisung des Auftraggebers. Mündliche Weisungen werden vom Auftragnehmer unverzüglich (z. B. per E-Mail) bestätigt. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt.

(2) Vertraulichkeit: Der Auftragnehmer unterliegt der Verschwiegenheitspflicht gemäß Art. 28 Abs. 3 lit. b DSGVO. Er gewährleistet, dass jede Person, die Zugang zu den verarbeiteten Daten hat, sich zur Vertraulichkeit verpflichtet hat. Dies gilt insbesondere für etwaige Subunternehmer und gelegentlich beauftragte Aushilfskräfte.

(3) Datensicherheit: Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Eine Beschreibung dieser Maßnahmen findet sich in Anlage 1 zu diesem Vertrag.

(4) Datenschutzbeauftragter: Der Auftragnehmer ist als Einzelunternehmer mit weniger als 20 mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten Personen nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet (§ 38 BDSG). Ansprechpartner für Datenschutzfragen ist Herr Tobias Möller persönlich, erreichbar unter info@pc-service-aus-schaumburg.de.

(5) Unterstützung: Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Wahrnehmung der Rechte betroffener Personen (Art. 12–22 DSGVO), bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO sowie auf Anfrage bei einer Datenschutz-Folgenabschätzung. Der Aufwand kann nach den jeweils gültigen Stundensätzen des Auftragnehmers abgerechnet werden, soweit er nicht auf einem Verschulden des Auftragnehmers beruht.

(6) Meldepflichten: Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Kenntniserlangung, über jede Verletzung des Schutzes personenbezogener Daten („Datenpanne“) im Zuständigkeitsbereich des Auftragnehmers. Die Meldung enthält die in Art. 33 Abs. 3 DSGVO genannten Angaben, soweit beim Auftragnehmer bekannt.

(7) Nachweise: Der Auftragnehmer weist die Einhaltung seiner Pflichten gegenüber dem Auftraggeber in geeigneter Weise nach, insbesondere durch die Beschreibung der TOMs (Anlage 1) und auf Anforderung durch zusätzliche schriftliche Auskünfte.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen allein verantwortlich („Verantwortlicher“ im Sinne von Art. 4 Nr. 7 DSGVO).

(2) Der Auftraggeber teilt dem Auftragnehmer das Ergebnis von Kontrollen, Anfragen von Aufsichtsbehörden oder Betroffenen unverzüglich mit, soweit dies die Auftragsverarbeitung betrifft.

(3) Der Auftraggeber benennt – sofern erforderlich – seinen Datenschutzbeauftragten oder eine sonstige für Datenschutzfragen zuständige Person und teilt deren Kontaktdaten dem Auftragnehmer mit.

(4) Bei Fernwartung gibt der Auftraggeber die jeweilige Sitzung ausdrücklich frei und kann sie jederzeit beenden. Während der Sitzung verfolgt der Auftraggeber die durchgeführten Aktionen am Bildschirm mit.

§ 5 Unterauftragsverhältnisse

(1) Allgemeine Genehmigung: Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zur Hinzuziehung der nachstehend genannten weiteren Auftragsverarbeiter („Sub-Auftragsverarbeiter“). Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen mit einer Vorlauffrist von mindestens vier Wochen. Der Auftraggeber kann der Änderung aus berechtigtem Grund widersprechen.

(2) Aktuelle Sub-Auftragsverarbeiter:

Sub-Auftragsverarbeiter	Leistung / Zweck	Sitz / Datenort
N-able International Ltd.	Remote-Monitoring-and-Management-Plattform (N-able Take Control / N-central) für Fernwartung und Patch-Management	Irland (EU). Rechenzentren EU/UK. Standardvertragsklauseln, sofern UK-Transfer.
Google Ireland Limited	Chrome Remote Desktop, sofern auf ausdrücklichen Wunsch des Auftraggebers eingesetzt	Irland (EU). Datenübermittlung in Drittländer auf Basis EU-Standardvertragsklauseln + EU-U.S. Data Privacy Framework.
STRATO AG	Hosting der Website pc-service-aus-schaumburg.de inkl. E-Mail-Postfächer (info@…)	Deutschland.

(3) Verpflichtung: Der Auftragnehmer verpflichtet die Sub-Auftragsverarbeiter schriftlich oder in dokumentierter elektronischer Form zur Einhaltung der Datenschutzvorschriften nach Art. 28 Abs. 2 und 4 DSGVO.

(4) Drittlandübermittlung: Soweit Sub-Auftragsverarbeiter Daten außerhalb des EWR verarbeiten, stellt der Auftragnehmer sicher, dass geeignete Garantien nach Art. 44 ff. DSGVO bestehen (z. B. EU-Standardvertragsklauseln, Angemessenheitsbeschluss).

(5) Keine Sub-Auftragsverarbeitung sind: Telekommunikations-, Post-, Reinigungs- oder Bewachungsdienstleistungen sowie Beratungs- und Sachverständigenleistungen, soweit kein Zugriff auf personenbezogene Daten erfolgt.

§ 6 Rechte der Betroffenen

Wenden sich Betroffene mit Anfragen oder Anträgen (z. B. auf Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Widerspruch) unmittelbar an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter. Der Auftragnehmer beantwortet solche Anfragen nicht selbst, es sei denn, der Auftraggeber weist ihn dazu an.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, die Einhaltung der vertraglichen und gesetzlichen Verpflichtungen des Auftragnehmers in angemessenem Umfang zu überprüfen, insbesondere durch Einholung schriftlicher Auskünfte.

(2) Inspektionen vor Ort sind nach vorheriger Anmeldung mit einer Frist von mindestens 14 Tagen, während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs zulässig. Der Auftragnehmer kann den Nachweis auch durch aktuelle Testate, Zertifikate oder Auditberichte (z. B. ISO 27001, BSI C5) erbringen, soweit verfügbar.

(3) Der für den Auftragnehmer durch eine Kontrolle entstehende Aufwand ist nach den jeweils gültigen Stundensätzen zu vergüten, sofern die Kontrolle nicht aus einem konkreten Anlass beim Auftragnehmer (etwa nach einer Datenschutzverletzung) erforderlich wird.

§ 8 Löschung und Rückgabe nach Beendigung

Nach Beendigung der Auftragsverarbeitung hat der Auftragnehmer alle ihm überlassenen personenbezogenen Daten nach Wahl des Auftraggebers zurückzugeben oder zu löschen, einschließlich aller im Auftragsverhältnis erstellten Kopien. Die Löschung wird auf Verlangen schriftlich oder per E-Mail bestätigt. Gesetzliche Aufbewahrungspflichten bleiben unberührt; in diesem Fall werden die Daten weiterhin gegen unbefugten Zugriff geschützt und nur zur Erfüllung der jeweiligen gesetzlichen Pflicht verwendet.

§ 9 Haftung

Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Innenverhältnis haftet jede Partei dem Anteil ihres Verschuldens entsprechend; im Übrigen gelten die Haftungsregelungen des Hauptvertrags bzw. der Allgemeinen Geschäftsbedingungen des Auftragnehmers.

§ 10 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform (z. B. unterzeichnetes PDF, E-Mail mit ausdrücklicher Zustimmung). Dies gilt auch für die Aufhebung dieses Formerfordernisses.

(2) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt eine Regelung, die dem wirtschaftlichen Zweck am nächsten kommt.

(3) Bei Widersprüchen zwischen diesem Vertrag und Regelungen aus dem Hauptvertrag oder den Allgemeinen Geschäftsbedingungen des Auftragnehmers gehen die Regelungen dieses Vertrags vor.

(4) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist – soweit gesetzlich zulässig – der Sitz des Auftragnehmers.

Unterschriften

Ort, Datum

____.____._____

_____

Auftragnehmer
Tobias Möller
PC Service aus Schaumburg

Ort, Datum

____.____._____

_____

Auftraggeber
Firma / Name
Vertretungsberechtigte Person

Anlage 1 — Technische und organisatorische Maßnahmen (TOMs)

gemäß Art. 32 DSGVO

Der Auftragnehmer trifft folgende technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten. Die Maßnahmen werden regelmäßig überprüft und an den Stand der Technik angepasst.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Zutrittskontrolle:** Geschäftsräume sind durch abschließbare Türen gesichert; Zugang nur für Tobias Möller persönlich. Aufbewahrung von Kundengeräten in einem abschließbaren Raum.
- **Zugangskontrolle:** Alle Arbeitsgeräte des Auftragnehmers sind mit individuellen Benutzerkonten, starken Passwörtern (mindestens 12 Zeichen) und Festplatten-Vollverschlüsselung (BitLocker bzw. FileVault) versehen. Bildschirmsperre nach maximal 10 Minuten Inaktivität.
- **Zugriffskontrolle:** Berechtigungen auf Kundendaten werden nur im Rahmen des konkreten Auftrags vergeben (Need-to-know). Administrative Zugriffe nur mit Multi-Faktor-Authentifizierung, soweit von den Zielsystemen unterstützt.
- **Trennungskontrolle:** Kundendaten verschiedener Auftraggeber werden logisch und – wo möglich – physisch getrennt verarbeitet (separate Arbeitsverzeichnisse, separate Backup-Datenträger).
- **Pseudonymisierung:** Für Test- und Reproduktionszwecke werden, wo praktikabel, anonymisierte oder pseudonymisierte Daten verwendet.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- **Weitergabekontrolle:** Übertragung personenbezogener Daten ausschließlich über verschlüsselte Verbindungen (TLS, SSH, SFTP, verschlüsselte E-Mail-Anhänge). Mobile Datenträger sind verschlüsselt.
- **Eingabekontrolle:** Wesentliche Aktionen werden in Tickets, E-Mails oder Auftragsformularen dokumentiert. Bei N-able liegen Protokolle der Fernwartungssitzungen vor.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Verfügbarkeitskontrolle:** Systeme des Auftragnehmers sind durch Firewall, aktuelle Endpoint-Protection und regelmäßige Updates gegen Schadsoftware geschützt.
- **Datensicherung:** Eigene Geschäftsdaten werden täglich verschlüsselt gesichert. Sicherungsdaten von Kunden werden im Rahmen beauftragter Backup-Pakete getrennt verwahrt.
- **Notfallplan:** Definierte Schritte zur Wiederherstellung bei Hardware-Ausfall innerhalb von 24 Stunden bei Standardfehlern.

4. Verfahren zur Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- **Datenschutz-Management:** Jährliche Überprüfung der TOMs und der eingesetzten Sub-Auftragsverarbeiter. Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO wird geführt.
- **Auftragskontrolle:** Verarbeitung nur auf Weisung des Auftraggebers; Weisungen werden dokumentiert.

- **Datenschutzfreundliche Voreinstellungen:** Es werden nur die für den jeweiligen Auftrag erforderlichen Daten verarbeitet. Nach Abschluss werden Daten zeitnah gelöscht.
- **Vorfallreaktion:** Datenschutzverletzungen werden unverzüglich – spätestens 48 Stunden nach Kenntnis – an den Auftraggeber gemeldet.

5. Spezifische Maßnahmen Fernwartung

- Fernwartung ausschließlich über N-able Take Control bzw. – auf ausdrücklichen Kundenwunsch – Chrome Remote Desktop.
- Sitzung wird ausschließlich auf aktive Freigabe des Auftraggebers gestartet (One-Time-Code bzw. ausdrückliche Bestätigung am Endgerät).
- Während der Sitzung sieht der Auftraggeber alle Aktionen am Bildschirm mit und kann die Sitzung jederzeit beenden.
- Es findet keine Aufzeichnung der Sitzung statt. Aktivitätsprotokolle werden nur in dem für Abrechnung und Fehleranalyse erforderlichen Umfang vorgehalten.
- Übertragung erfolgt Ende-zu-Ende-verschlüsselt.

Hinweis: *Dieses Dokument ist eine Vertragsvorlage und kein Ersatz für eine individuelle Rechts- oder Datenschutzberatung. Vor Verwendung empfiehlt sich – insbesondere bei größeren Auftraggebern oder bei Verarbeitung besonderer Datenkategorien – die Prüfung durch einen Rechtsanwalt oder Datenschutzbeauftragten.*

Stand: 23.05.2026 · Erstellt für PC Service aus Schaumburg · Tobias Möller