

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO, zwischen dem Kunden von SmoovOps ("Verantwortlicher") und der Northwood UG (haftungsbeschränkt) ("Auftragsverarbeiter")

Präambel

Dieser Auftragsverarbeitungsvertrag ("Vertrag" oder "AVV") konkretisiert die datenschutzrechtlichen Pflichten der Parteien im Zusammenhang mit der Nutzung von SmoovOps und ergänzt die Allgemeinen Geschäftsbedingungen (AGB) zwischen den Parteien. Er gilt für sämtliche Verarbeitungen personenbezogener Daten, die der Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der Bereitstellung von SmoovOps vornimmt.

Im Fall von Widersprüchen zwischen diesem AVV und den AGB gehen die Regelungen dieses AVV in Bezug auf die Verarbeitung personenbezogener Daten vor.

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der Bereitstellung der SmoovOps-Anwendung, insbesondere der Module Partner (CRM), Produktkatalog, Verträge, Dokumente (einschließlich Rechnungen, Angebote, Lieferscheine, Briefe und Belege), Notizen, Zahlungen und Dashboard.

(2) Einzelheiten zu Art, Umfang und Zweck der Verarbeitung, der Art der personenbezogenen Daten sowie der Kategorien betroffener Personen ergeben sich aus **Anlage 1**.

(3) Die Laufzeit dieses Vertrags entspricht der Laufzeit des zwischen den Parteien bestehenden Hauptvertrags (Nutzungsvertrag über SmoovOps gemäß AGB). Er endet automatisch mit Beendigung des Hauptvertrags, vorbehaltlich fortbestehender Pflichten nach § 10.

§ 2 Weisungsrecht des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach dem Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung verpflichtet; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Nutzung von SmoovOps gemäß der vertraglich vereinbarten Funktionen sowie die vom Verantwortlichen über die Benutzeroberfläche vorgenommenen Konfigurationen und Dateneingaben gelten als Weisung im Sinne dieses Vertrags. Darüberhinausgehende Weisungen bedürfen der Textform (z. B. E-Mail an info@northwood.de).

(3) Hält der Auftragsverarbeiter eine Weisung des Verantwortlichen für rechtswidrig, informiert er den Verantwortlichen unverzüglich hierüber. Der Auftragsverarbeiter ist berechtigt, die Ausführung einer solchen Weisung bis zu ihrer Bestätigung oder Änderung durch den Verantwortlichen auszusetzen.

§ 3 Vertraulichkeit

Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, und dass diese Personen nur im erforderlichen Umfang Zugang zu den betreffenden personenbezogenen Daten haben.

§ 4 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen (TOM), um ein dem Risiko angemessenes Schutzniveau gemäß Art. 32 DSGVO zu gewährleisten.

(2) Der Auftragsverarbeiter ist berechtigt, die TOM anzupassen, sofern das ursprünglich vereinbarte Schutzniveau dadurch nicht unterschritten wird. Wesentliche Änderungen werden dem Verantwortlichen mitgeteilt.

§ 5 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich, unter Berücksichtigung der Art der Verarbeitung, den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen (Art. 28 Abs. 3 lit. e DSGVO). Erhält der Auftragsverarbeiter eine solche Anfrage direkt von einer betroffenen Person, leitet er diese unverzüglich an den Verantwortlichen weiter, ohne sie selbst zu beantworten, sofern der Verantwortliche nichts anderes weisungsgemäß festlegt.

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten (u. a. Sicherheit der Verarbeitung, Meldung von Verletzungen des Schutzes personenbezogener Daten, Datenschutz-Folgenabschätzung).

§ 6 Meldung von Datenschutzverletzungen

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO unverzüglich, spätestens jedoch innerhalb von **48 Stunden** nach Bekanntwerden.

(2) Die Meldung enthält, soweit dem Auftragsverarbeiter bekannt, mindestens die Angaben gemäß Art. 33 Abs. 3 DSGVO und wird an die im Kundenkonto hinterlegte Kontaktadresse übermittelt.

(3) Der Verantwortliche bleibt für die Beurteilung, ob eine Meldepflicht gegenüber der Aufsichtsbehörde nach Art. 33 DSGVO bzw. eine Benachrichtigungspflicht gegenüber betroffenen Personen nach Art. 34 DSGVO besteht, sowie für die entsprechende Umsetzung selbst verantwortlich.

§ 7 Unterauftragsverhältnisse

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung zur Beauftragung von Unterauftragsverarbeitern im Sinne von Art. 28 Abs. 2 DSGVO. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in **Anlage 3** aufgeführt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern mit einer Frist von mindestens 14 Tagen vor der geplanten Änderung, z. B. per E-Mail oder über das Kundenkonto bzw. eine entsprechende Statusseite. Der Verantwortliche kann der Änderung innerhalb dieser Frist aus berechtigtem, sachlich nachvollziehbarem Grund widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt.

(3) Der Auftragsverarbeiter verpflichtet die Unterauftragsverarbeiter vertraglich zu Datenschutzpflichten, die den in diesem Vertrag vereinbarten Pflichten gleichwertig sind, insbesondere hinsichtlich angemessener technischer und organisatorischer Maßnahmen.

(4) Sofern Unterauftragsverarbeiter Daten außerhalb der EU/des EWR verarbeiten, stellt der Auftragsverarbeiter sicher, dass hierfür geeignete Garantien im Sinne der Art. 44 ff. DSGVO vorliegen (z. B. Angemessenheitsbeschluss der EU-Kommission oder EU-Standardvertragsklauseln).

§ 8 Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden, und trägt hierzu bei.

(2) Nachweise können, soweit ausreichend, auch durch die Vorlage aktueller Zertifizierungen, Testate oder Auditberichte unabhängiger Prüfer (z. B. zu vom Auftragsverarbeiter genutzten Hosting-Anbietern) erbracht werden, sofern diese eine Beurteilung der Einhaltung der in diesem Vertrag vereinbarten Pflichten ermöglichen.

(3) Vor-Ort-Kontrollen sind mit angemessenem Vorlauf (mindestens 2 Wochen) schriftlich anzukündigen und finden während der üblichen Geschäftszeiten statt, ohne den Betrieb des Auftragsverarbeiters unangemessen zu beeinträchtigen. Der Verantwortliche trägt die Kosten einer solchen Kontrolle, sofern diese nicht Anlass für die Feststellung eines erheblichen Verstoßes des Auftragsverarbeiters gegen diesen Vertrag war.

§ 9 Weisungsbefugte Person

Weisungsbefugt beim Verantwortlichen ist die bei der Registrierung angegebene bzw. im Kundenkonto hinterlegte Kontaktperson. Ansprechpartner beim Auftragsverarbeiter ist:

Northwood UG (haftungsbeschränkt)
z. Hd. Thorsten Szutkus

§ 10 Löschung und Rückgabe personenbezogener Daten

(1) Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter alle personenbezogenen Daten, die im Auftrag des Verantwortlichen verarbeitet wurden, oder gibt sie nach Wahl des Verantwortlichen zurück, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Dem Verantwortlichen wird hierzu die in den AGB (§ 8) beschriebene Exportmöglichkeit für einen Zeitraum von 30 Tagen nach Vertragsende zur Verfügung gestellt. Nach Ablauf dieser Frist löscht der Auftragsverarbeiter die verbleibenden Daten, soweit keine gesetzlichen Aufbewahrungspflichten (z. B. für Rechnungsdaten gemäß § 147 AO, § 257 HGB) entgegenstehen.

§ 11 Haftung

(1) Es gelten die gesetzlichen Haftungsregelungen der Art. 82, 28 Abs. 10 sowie Art. 83 DSGVO.

(2) Im Übrigen gelten die in den AGB vereinbarten Haftungsbeschränkungen entsprechend, soweit dem nicht zwingende gesetzliche Vorgaben der DSGVO entgegenstehen.

§ 12 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags sowie aller seiner Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen oder elektronisch dokumentierten Vereinbarung.

(2) Bei Widersprüchen zwischen diesem AVV und Regelungen aus sonstigen Vereinbarungen zwischen den Parteien, insbesondere den AGB, gehen die Regelungen dieses AVV im Hinblick auf datenschutzrechtliche Fragestellungen vor.

(3) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

(4) Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1: Gegenstand, Art, Zweck der Verarbeitung und Kategorien

Gegenstand und Dauer der Verarbeitung

Bereitstellung der SmooOps-Anwendung als Software-as-a-Service über die Vertragslaufzeit des Hauptvertrags.

Art und Zweck der Verarbeitung

Erfassung, Speicherung, Organisation, Anzeige, Änderung, Export und Löschung personenbezogener Daten, die der Verantwortliche im Rahmen der Nutzung der folgenden SmooOps-Module einträgt bzw. hochlädt:

- **Partner (CRM):** Verwaltung von Kontakt- und Geschäftsbeziehungsdaten
- **Produktkatalog:** Verwaltung von Produkt-/Leistungsangaben (i. d. R. keine personenbezogenen Daten, sofern nicht Ansprechpersonen o. Ä. hinterlegt werden)
- **Verträge:** Erstellung, Speicherung und Verwaltung von Vertragsdokumenten
- **Dokumente:** Erstellung, Speicherung, Hochladen und Verwaltung von Dokumenten der Typen Vertrag, Rechnung, Angebot, Lieferschein, Brief und Beleg, einschließlich Unterstützung der Rechnungsformate XRechnung/ZUGFeRD sowie automatisiert aus hochgeladenen Dokumenten extrahierter Daten (Texterkennung/IDP)
- **Notizen:** Erfassung von Notizen und Kommentaren zu Partnern, Verträgen, Zahlungen und Produkten
- **Zahlungen:** Erfassung und Nachverfolgung von Zahlungsvorgängen zu Rechnungen
- **Dashboard:** Aggregierte Auswertungen der vorgenannten Daten

Art der personenbezogenen Daten

- Vor- und Nachname
- Firmenname, Anschrift
- Kontaktdaten (E-Mail-Adresse, Telefonnummer)

- Rechnungs- und Zahlungsdaten (Rechnungsbeträge, Zahlungsstatus, Bankverbindung, sofern vom Verantwortlichen hinterlegt)
- Vertragsdaten und -inhalte, sofern personenbezogen
- Notiz- und Kommentarinhalte zu Partnern, Verträgen, Zahlungen und Produkten (Notizen-Modul)
- Inhalte hochgeladener oder generierter Dokumente sowie automatisiert daraus extrahierte Daten (Dokumente-Modul, z. B. Texterkennung/IDP von Rechnungen und Belegen)
- Fotos, sofern vom Verantwortlichen zu Partnern oder Produkten hinterlegt

Kategorien betroffener Personen

- Geschäftspartner:innen, Kund:innen und Ansprechpersonen des Verantwortlichen
 - Mitarbeitende des Verantwortlichen, soweit im Zusammenhang mit Verträgen/Rechnungen erfasst
-

Anlage 2: Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

1. Vertraulichkeit

- **Zutrittskontrolle:** Zutrittskontrolle erfolgt durch den Hosting-Anbieter AWS an dessen Rechenzentren gemäß dessen Zertifizierungen
- **Zugangskontrolle:** Zugang zu Systemen ausschließlich über individuelle Zugangsdaten
- **Zugriffskontrolle:** Rollen- und Rechtekonzept, das den Zugriff auf personenbezogene Daten auf das für die jeweilige Aufgabe erforderliche Maß beschränkt (Need-to-know-Prinzip)
- **Trennungskontrolle:** Logische Trennung der Daten verschiedener Kund:innen auf Anwendungsebene (Mandantentrennung)

2. Integrität

- **Weitergabekontrolle:** Verschlüsselte Datenübertragung (TLS) bei der Kommunikation zwischen Client und Server
- **Eingabekontrolle:** Protokollierung sicherheitsrelevanter Ereignisse und Änderungen in Form von Audit Logs

3. Verfügbarkeit und Belastbarkeit

- Regelmäßige Datensicherung (Backups) alle 7 Tage
- Redundante Auslegung der Infrastruktur über die vom Hosting-Anbieter bereitgestellten Verfügbarkeitszonen
- Notfallkonzept zur Wiederherstellung der Verfügbarkeit nach einem physischen oder technischen Zwischenfall

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Regelmäßige Überprüfung der eingesetzten Sicherheitsmaßnahmen (halbjährlich)
 - Auftragsverarbeitungsverträge mit sämtlichen eingesetzten Unterauftragsverarbeitern (siehe Anlage 3)
 - Software-Updates und Sicherheitspatches nach Prüfung in Staging Umgebung
-

Anlage 3: Genehmigte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Verarbeitungsort	Garantie bei Drittlandtransfer
Amazon Web Services (AWS)	Hosting, Infrastruktur (u. a. AWS Lambda, DynamoDB, S3) sowie Content Delivery/Angriffsschutz (CloudFront, WAF)	eu-central-1 (Frankfurt am Main); WAF-WebACL aus technischen Gründen in us-east-1 (Nord-Virginia) verwaltet, verarbeitet dort nur Anfragemetadaten	EU-US Data Privacy Framework (Zertifizierung), ergänzend EU-Standardvertragsklauseln als Rückfallmechanismus
Stripe Payments Europe, Ltd. (ggf. verbundenes Unternehmen Stripe, Inc., USA)	Zahlungsabwicklung	Dublin, Irland (Stripe, Inc.: USA)	EU-Standardvertragsklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO
Amazon Web Services (AWS SES)	Versand von Transaktions-E-Mails	eu-central-1 (Frankfurt am Main)	entfällt (EU-Region)

Stand: 29.07.2026