

Vertrag über die Auftragsverarbeitung

nach Art. 28 Datenschutz-Grundverordnung (DSGVO), Stand: Oktober 2026

Vertragsparteien

Verantwortlicher (nachfolgend „Kunde“): das Unternehmen, das mit uns einen Vertrag über die Nutzung der Software Komplea geschlossen hat.

Auftragsverarbeiter (nachfolgend „Anbieter“):

Komplea, Inhaber A. Sakali

Saarbrücker Weg 10

59439 Holzwickede

E-Mail: info@komplea.de, Telefon: 02301 1870478

§ 1 Gegenstand und Dauer

(1) Der Anbieter stellt dem Kunden die Software Komplea als Online-Dienst bereit (Hauptvertrag nach unseren Allgemeinen Geschäftsbedingungen). Dabei verarbeitet der Anbieter personenbezogene Daten, die der Kunde in Komplea erfasst, ausschließlich im Auftrag und nach Weisung des Kunden.

(2) Dieser Vertrag gilt für die Dauer des Hauptvertrags und darüber hinaus, solange der Anbieter Daten des Kunden verarbeitet (§ 10). Er wird mit Abschluss des Hauptvertrags vereinbart; einer gesonderten Unterschrift bedarf es nicht. Auf Wunsch stellen wir ihn unterschrieben zur Verfügung.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Zweck der Verarbeitung ist der Betrieb der Software Komplea für den Kunden: Speichern, Anzeigen, Verarbeiten, Sichern und Löschen der Daten, die der Kunde für seine Warenwirtschaft, Buchhaltung, Kundenbeziehungen und Kommunikation erfasst oder über Schnittstellen einliest.

(2) Arten der Daten:

- Stammdaten von Kunden, Interessenten, Lieferanten und Ansprechpartnern (Name, Firma, Anschrift, Telefon, E-Mail)
- Vertrags-, Beleg- und Abrechnungsdaten (Angebote, Aufträge, Rechnungen, offene Posten, Zahlungen)
- Bankverbindungen und SEPA-Mandate
- Kommunikationsdaten (E-Mails, Anrufe mit Rufnummer und Zeitpunkt, Termine, Notizen, Anhänge)
- Daten von Mitarbeitern des Kunden (Benutzerkonten, Rechte, bei Nutzung des Personalmoduls Arbeitszeiten, Abwesenheiten und Qualifikationen)
- Protokolldaten (wer hat wann welchen Datensatz angelegt oder geändert)

(3) Kreise der betroffenen Personen: Kunden, Interessenten, Lieferanten und deren Ansprechpartner, Mitarbeiter des Kunden sowie sonstige Personen, deren Daten der Kunde in Komplea erfasst.

(4) Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind für die Verarbeitung nicht vorgesehen. Erfasst der Kunde sie dennoch, etwa als Abwesenheitsgrund, trägt er dafür die Verantwortung.

(5) Die Verarbeitung erfolgt ausschließlich in Deutschland. Eine Übermittlung in Länder außerhalb der EU oder des EWR findet durch den Anbieter nicht statt.

§ 3 Weisungen des Kunden

(1) Der Anbieter verarbeitet die Daten nur auf dokumentierte Weisung des Kunden. Weisungen sind der Hauptvertrag, dieser Vertrag sowie die Nutzung der Software durch den Kunden selbst. Weitere Weisungen erteilt der Kunde in Textform.

(2) Ist der Anbieter der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, weist er den Kunden unverzüglich darauf hin und darf die Ausführung bis zur Klärung aussetzen.

(3) Schnittstellen zu Diensten Dritter (zum Beispiel E-Mail-Postfach, Telefonanlage, Bank, DATEV, Finanzamt, Online-Shops, Paketdienste) nutzt Komplea nur, wenn der Kunde sie selbst mit seinen eigenen Zugangsdaten einrichtet. Die Übermittlung an diese Dienste erfolgt auf Weisung des Kunden; die Anbieter dieser Dienste sind Vertragspartner des Kunden und keine Unterauftragsverarbeiter des Anbieters.

§ 4 Pflichten des Anbieters

(1) Der Anbieter verpflichtet alle Personen, die Zugang zu den Daten haben, zur Vertraulichkeit, soweit sie nicht einer gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Der Anbieter trifft die technischen und organisatorischen Maßnahmen nach Anlage 1 und passt sie dem Stand der Technik an. Das Schutzniveau darf dabei nicht sinken.

(3) Der Anbieter unterstützt den Kunden mit geeigneten Maßnahmen bei der Erfüllung der Rechte der betroffenen Personen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch). Komplea enthält dafür eigene Funktionen, insbesondere Auskunft als Druck und Datei, Export und Anonymisierung. Wendet sich eine betroffene Person direkt an den Anbieter, leitet er die Anfrage unverzüglich an den Kunden weiter.

(4) Der Anbieter unterstützt den Kunden bei Datenschutz-Folgenabschätzungen und bei Meldungen an Aufsichtsbehörden, soweit es um die Verarbeitung im Auftrag geht.

(5) Der Anbieter informiert den Kunden unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis, über Verletzungen des Schutzes personenbezogener Daten. Die Mitteilung enthält, soweit bekannt, Art der Verletzung, betroffene Daten und Personen, wahrscheinliche Folgen und ergriffene Maßnahmen.

(6) Der Anbieter verwendet die Daten nicht für eigene Zwecke und gibt sie nicht an Dritte weiter, soweit nicht eine gesetzliche Pflicht besteht. Über eine solche Pflicht informiert er den Kunden vorab, soweit das Gesetz dies nicht verbietet.

§ 5 Pflichten des Kunden

(1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen verantwortlich.

(2) Der Kunde vergibt Zugänge und Rechte für seine Mitarbeiter in Komplea selbst und hält die Zugangsdaten geheim.

(3) Der Kunde informiert den Anbieter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 6 Unterauftragsverarbeiter

(1) Der Kunde stimmt dem Einsatz der in Anlage 2 genannten Unterauftragsverarbeiter zu.

(2) Der Anbieter informiert den Kunden mindestens vier Wochen vorher in Textform über die beabsichtigte Hinzuziehung oder den Austausch eines Unterauftragsverarbeiters. Der Kunde kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Können sich die Parteien nicht einigen, kann der Kunde den Hauptvertrag zum Zeitpunkt der Änderung kündigen.

(3) Der Anbieter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf die Pflichten dieses Vertrags. Er setzt nur Unterauftragsverarbeiter ein, die ihre Leistungen in der EU oder im EWR erbringen.

§ 7 Kontrollrechte

(1) Der Kunde kann sich von der Einhaltung dieses Vertrags überzeugen. Der Anbieter stellt ihm dazu auf Anfrage die erforderlichen Informationen zur Verfügung, insbesondere eine aktuelle Beschreibung der Maßnahmen nach Anlage 1 und, soweit vorhanden, Nachweise seiner Unterauftragsverarbeiter (zum Beispiel Zertifikate des Rechenzentrums).

(2) Prüfungen vor Ort sind nach Anmeldung mit angemessener Frist während der Geschäftszeiten möglich, ohne den Betrieb zu stören und unter Wahrung der Vertraulichkeit gegenüber anderen Kunden. Prüfungen in Rechenzentren von Unterauftragsverarbeitern richten sich nach deren Bedingungen. Den Aufwand für Prüfungen vor Ort trägt der Kunde, soweit die Prüfung keinen Verstoß ergibt.

§ 8 Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags.

§ 9 Datensicherung

Der Anbieter sichert die Daten täglich (Anlage 1, Nr. 4). Sicherungen werden nach 14 Tagen überschrieben. Daten, die der Kunde löscht, sind damit spätestens nach 14 Tagen auch aus den Sicherungen entfernt.

§ 10 Rückgabe und Löschung nach Vertragsende

(1) Nach Ende des Hauptvertrags kann der Kunde seine Daten noch 30 Tage lang exportieren (zum Beispiel CSV, Excel, DATEV-Format, GoBD-Export, archivierte Belege als PDF).

(2) Danach löscht der Anbieter alle Daten des Kunden, soweit keine gesetzliche Pflicht zur Aufbewahrung beim Anbieter besteht. Sicherungskopien werden im Rahmen des regulären Sicherungszyklus (§ 9) überschrieben. Auf Verlangen bestätigt der Anbieter die Löschung in Textform.

(3) Die gesetzlichen Aufbewahrungspflichten des Kunden selbst (zum Beispiel acht Jahre für Buchungsbelege und zehn Jahre für Bücher und Jahresabschlüsse) bleiben Sache des Kunden.

§ 11 Schlussbestimmungen

(1) Bei Widersprüchen geht dieser Vertrag den Regelungen des Hauptvertrags vor, soweit es um den Schutz personenbezogener Daten geht.

(2) Änderungen dieses Vertrags bedürfen der Textform. Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) Es gilt deutsches Recht. Gerichtsstand ist, soweit zulässig, Holzwickede.

Anlage 1: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

1. Vertraulichkeit

- Betrieb in einem Rechenzentrum in Nürnberg (Deutschland); Zutrittskontrolle und Brandschutz durch den Rechenzentrumsbetreiber (Anlage 2)
- Zugriff auf den Server nur durch den Inhaber des Anbieters; Verwaltung ausschließlich über verschlüsselte Verbindungen
- Die Datenbank ist nicht aus dem Internet erreichbar; die Anwendung ist nur über einen vorgeschalteten Webserver mit HTTPS erreichbar
- Benutzerkonten mit Kennwort; Kennwörter werden nur als sichere Prüfsumme (PBKDF2) gespeichert
- Rechte je Benutzer und Bereich (zum Beispiel Belege, Buchhaltung, Personal), Rollen, Nur-Lesen-Zugänge, Sonderrechte für sensible Bereiche
- Strikte Trennung der Daten verschiedener Kunden (Mandantentrennung in der Anwendung)
- Zugangsdaten zu Diensten Dritter (Mail-Kennwörter, Schlüssel für Schnittstellen) werden verschlüsselt gespeichert

2. Integrität

- Verschlüsselte Übertragung aller Daten zwischen Browser und Server (TLS, HSTS)

- Änderungsprotokoll: Anlage, Änderung und Löschung von Datensätzen werden mit Benutzer und Zeitpunkt protokolliert
- Festgeschriebene Rechnungen und Buchungen sind gegen nachträgliche Änderung gesperrt (GoBD)

3. Verfügbarkeit und Belastbarkeit

- Tägliche Sicherung der Datenbank und der abgelegten Dateien mit Prüfung der Sicherungsdatei, Aufbewahrung 14 Tage
- Fehlerprotokoll bei fehlgeschlagener Sicherung
- Einspielen von Sicherheitsaktualisierungen für Betriebssystem und Anwendung
- Getrennte Testsysteme; Änderungen an der Software werden vor dem Einspielen automatisiert getestet

4. Verfahren zur regelmäßigen Überprüfung

- Überprüfung dieser Maßnahmen mindestens einmal jährlich und bei wesentlichen Änderungen
- Datenschutzfreundliche Voreinstellungen: Funktionen, die Daten automatisch an Dritte senden, sind ab Werk ausgeschaltet und werden vom Kunden selbst eingeschaltet

Anlage 2: Unterauftragsverarbeiter

- netcup GmbH, Daimlerstraße 25, 76185 Karlsruhe, Deutschland. Leistung: Bereitstellung des Servers (Rechenzentrum Nürnberg), auf dem Komplea mit allen Kundendaten und Sicherungen betrieben wird.

Unterschriften (nur falls eine unterschriebene Fassung gewünscht ist)

Ort, Datum

Ort, Datum

Kunde (Firma, Name, Unterschrift)

Komplea, Inhaber A. Sakali