Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO · Stand: Mai 2026

Hinweis: Dieser AVV gilt automatisch für alle Nutzer der Plattform klarofix und wird durch Akzeptanz der AGB bei der Registrierung verbindlich abgeschlossen.

§ 1 Vertragsparteien und Rangfolge

(1) Auftraggeber (Verantwortlicher): Der Nutzer der Plattform „klarofix" (Unternehmer gemäß § 14 BGB), dessen individuelle Angaben bei Vertragsschluss im Nutzerprofil erfasst werden.

(2) Auftragnehmer (Auftragsverarbeiter):

Maximilian Hertwig (Einzelunternehmen)

handelnd unter „klarofix"

Rosengarten 14 · 23730 Neustadt in Holstein

E-Mail: moin@klugesdenken.de

(3) Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus der Nutzung der SaaS-Plattform ergeben. Im Falle von Widersprüchen zwischen diesem AVV und anderen Vereinbarungen (z. B. AGB) gehen die Bestimmungen dieses AVV vor.

§ 2 Gegenstand, Art und Zweck der Verarbeitung

(1) Der Auftragnehmer stellt dem Auftraggeber die SaaS-Plattform „klarofix" zur Verfügung. Die Verarbeitung umfasst die Speicherung und Verwaltung von Kundenstammdaten, Angeboten, Rechnungen, Mahnungen, DATEV-Exporten, Ausgaben, Verträgen und Projektbeschreibungen.

(2) Zweck der Verarbeitung ist die Bereitstellung der Software-Funktionen zur digitalen Büroorganisation und Kundenverwaltung des Auftraggebers.

§ 3 Dauer

Die Dauer dieses Vertrages entspricht der Laufzeit des Hauptvertrages (Nutzungsvertrag klarofix).

§ 4 Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers.

(2) Weisungen erfolgen in der Regel durch die Nutzung der Softwareoberfläche; darüber hinausgehende Weisungen sind in Textform zu erteilen.

(3) Hält der Auftragnehmer eine Weisung für datenschutzrechtswidrig, hat er den Auftraggeber unverzüglich zu informieren.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer gewährleistet, dass alle zur Verarbeitung berechtigten Personen zur Vertraulichkeit verpflichtet wurden.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung).

§ 6 Technische und organisatorische Maßnahmen (TOM)

Der Auftragnehmer setzt gemäß Art. 32 DSGVO folgende Maßnahmen um:

- Zutrittskontrolle: Hosting in zertifizierten Rechenzentren der IONOS SE in Deutschland.
- Zugangskontrolle: Kennwortschutz, Passwort-Hashing mittels bcrypt (mind. 12 Runden).
- Zugriffskontrolle: Authentifizierung über JWT-System, Rollenkonzept; Zugriff nur durch autorisierte Personen.
- Weitergabekontrolle: Durchgehende TLS 1.2/1.3 Transportverschlüsselung.
- Eingabekontrolle: Protokollierung von Systemzugriffen zur Fehleranalyse.
- Verfügbarkeit: 99 % Verfügbarkeit im Jahresmittel; Backups erfolgen alle 7 Tage.
- Trennungsgebot: Strikte Datenisolation auf Basis der user_id; Pseudonymisierung mittels UUID-System.
- Verschlüsselung: AES-256-GCM für SMTP-Credentials.

§ 7 Unterauftragsverarbeiter

(1) Als Unterauftragsverarbeiter ist derzeit die IONOS SE, Elgendorfer Str. 57, 56410 Montabaur (Hosting/Infrastruktur) genehmigt.

(2) Beabsichtigt der Auftragnehmer, weitere Unterauftragnehmer hinzuzuziehen oder zu ersetzen, informiert er den Auftraggeber 30 Tage vorab in Textform. Dem Auftraggeber steht ein Widerspruchsrecht aus wichtigem Grund zu.

§ 8 Betroffenenrechte

Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit bei der Beantwortung von Anfragen zur Ausübung von Betroffenenrechten (Auskunft, Löschung etc.). Erhält der Auftragnehmer eine solche Anfrage direkt, leitet er diese unverzüglich an den Auftraggeber weiter.

§ 9 Datenschutzverletzungen

Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch binnen 48 Stunden nach Bekanntwerden. Die Meldung muss mindestens die Art der Verletzung, die betroffenen Datenkategorien und die ergriffenen Abhilfemaßnahmen enthalten.

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Nach Beendigung des Hauptvertrages wird der Auftragnehmer sämtliche vom Auftraggeber verarbeiteten Daten nach 30 Tagen unwiderruflich löschen.

(2) Der Auftraggeber ist verpflichtet, seine Daten vor Vertragsende eigenständig über die Exportfunktionen der Software zu sichern.

(3) Eine Speicherung über das Vertragsende hinaus erfolgt nur, soweit gesetzliche Aufbewahrungspflichten des Auftragnehmers (z. B. für eigene Rechnungsstellung gegenüber dem Auftraggeber) dies erfordern.

§ 11 Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die Einhaltung dieser Vereinbarung durch Audits zu kontrollieren. Diese sind mit einer Frist von zwei Wochen anzukündigen. Der Auftragnehmer kann dieses Recht auch durch die Vorlage aktueller Testate oder Zertifikate (z. B. von IONOS) erfüllen.

§ 12 Haftung

Die Haftung richtet sich nach den Regelungen der DSGVO. Ergänzend gelten die Haftungsbeschränkungen des Hauptvertrages (AGB).

§ 13 Besondere Regelung: DATEV-Export

Der Auftragnehmer stellt lediglich die technische Export-Schnittstelle im DATEV-Format bereit. Für die inhaltliche Richtigkeit der Buchungsdaten und die steuerrechtliche Konformität der Exporte trägt allein der Auftraggeber die Verantwortung.

§ 14 Besondere Regelung: SMTP-Zugangsdaten

Sofern der Auftraggeber eigene SMTP-Server nutzt, werden die Zugangsdaten mittels AES-256-GCM verschlüsselt gespeichert. Der Auftragnehmer verwendet diese Daten ausschließlich im Auftrag des Nutzers für den technischen Mailversand aus der Applikation heraus.

§ 15 Besondere Regelung: Öffentliche Angebotslinks

Bei Nutzung öffentlicher Angebotslinks entscheidet der Auftraggeber eigenverantwortlich über die Freigabe der Inhalte. Der Auftragnehmer stellt hierfür lediglich die Infrastruktur und das View-Tracking bereit.

§ 16 Schlussbestimmungen

(1) Es gilt deutsches Recht.

(2) Änderungen dieses AVV bedürfen der Textform.

(3) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Gültigkeit der übrigen Regelungen unberührt.