

Invotica

Vereinbarung zur Auftragsbearbeitung / Auftragsverarbeitung (AVV)

Anhang zu den AGB von Invotica - Version 09.07.2026

Anbieter / Auftragsbearbeiter	Florin Buehlmann / Invotica, Schweiz
Kunde / Verantwortlicher	Der jeweilige Firmenkunde bzw. Nutzer, der Invotica fuer eigene Zwecke einsetzt
Geltung	Soweit Invotica personenbezogene Daten im Auftrag des Kunden verarbeitet
Einbindung	Diese AVV ist als Anhang Bestandteil der AGB, soweit der Kunde die AGB akzeptiert
Hinweis	Kurze operative Vorlage. Bei Grosskunden, Sonderdaten oder Sondervertraegen juristisch pruefen.

Zweck dieses Dokuments: Diese Vereinbarung regelt die datenschutzrechtliche Rollenverteilung und die Pflichten von Invotica, wenn Firmenkunden Invotica zur Verarbeitung personenbezogener Daten verwenden, insbesondere fuer Rechnungen, Offerten, Zeiterfassung, Mitarbeiterverwaltung, Lohnabrechnungen und verwandte Funktionen.

1. Gegenstand und Geltung

Diese Vereinbarung zur Auftragsbearbeitung / Auftragsverarbeitung ("AVV") gilt zwischen dem Kunden und Invotica, soweit Invotica personenbezogene Daten im Auftrag des Kunden verarbeitet. Sie bildet einen Anhang zu den Allgemeinen Geschäftsbedingungen (AGB) von Invotica.

Der Kunde bleibt Verantwortlicher fuer die von ihm in Invotica eingegebenen, importierten oder hochgeladenen Daten. Invotica verarbeitet diese Daten grundsatzlich nur zur Bereitstellung, Sicherung und Wartung der Invotica-Plattform sowie nach Massgabe dieser AVV, der AGB und der Datenschutzerklaerung.

2. Rollen der Parteien und Weisungen

Der Kunde ist Verantwortlicher im Sinne des anwendbaren Datenschutzrechts. Invotica ist, soweit Invotica personenbezogene Daten fuer den Kunden verarbeitet, Auftragsbearbeiter nach Schweizer DSG bzw. Auftragsverarbeiter nach DSGVO.

Die Weisungen des Kunden ergeben sich aus der Nutzung der Invotica-Plattform, den gewaehlten Funktionen, den Einstellungen des Kunden, den AGB, dieser AVV und allfaelligen schriftlichen Zusatzvereinbarungen.

Invotica informiert den Kunden, wenn Invotica der Ansicht ist, dass eine Weisung gegen anwendbares Datenschutzrecht verstoesst, soweit Invotica dazu rechtlich befugt ist.

3. Zweck, Umfang und Dauer der Verarbeitung

Zweck der Verarbeitung ist die Bereitstellung der Invotica-Plattform fuer betriebliche Verwaltungsprozesse des Kunden, insbesondere Rechnungen, Offerten, Kundenverwaltung, Mitarbeiterverwaltung, Zeiterfassung, Erinnerungen, Mahnungen, Lohnabrechnungen, Dokumentenerstellung, E-Mail-Versand und optionale KI-Funktionen.

Der Umfang der Verarbeitung richtet sich nach den Funktionen, die der Kunde tatsaechlich nutzt, und nach den Daten, die der Kunde selbst eingibt, importiert, hochlaedt oder ueber eigene Systeme uebermittelt.

Die Verarbeitung dauert grundsatzlich fuer die Dauer des Vertragsverhaeltnisses. Gesetzliche Aufbewahrungspflichten, technische Backup-Zyklen und berechnigte Nachweis- oder Abrechnungszwecke bleiben vorbehalten.

4. Kategorien betroffener Personen und Datenarten

Je nach Nutzung koennen insbesondere folgende Personengruppen betroffen sein: Nutzer und Administratoren des Kunden, Mitarbeiter des Kunden, Ansprechpartner bei Kunden oder Lieferanten des Kunden, Rechnungsempfaenger, Kontaktpersonen, Bewerber oder sonstige Personen, deren Daten der Kunde in Invotica verarbeitet.

- Stammdaten: Name, Firma, Adresse, E-Mail, Telefonnummer, Rolle, Sprache, Benutzerkonto.
- Geschaeftsdaten: Rechnungen, Offerten, Leistungsbeschreibungen, Zahlungs- und Abo-Informationen, Kundennotizen.
- Mitarbeiter- und Zeitdaten: Arbeitszeiten, Abwesenheiten, Zeiteintraege, interne Zuordnungen, Dokumente.
- Lohn- und Abrechnungsdaten: Lohnabrechnungen, Lohnausweise und damit verbundene Angaben, soweit der Kunde diese Funktionen nutzt.
- Technische Daten: Login- und Sessiondaten, IP-Adressen, Sicherheitsereignisse, technische Protokolle, geraete- und browserbezogene Daten.
- Kommunikationsdaten: vom Kunden ausgeloeoste E-Mails, Kontaktformular- und Feedback-Inhalte.

Besondere Kategorien personenbezogener Daten werden von Invotica nicht gezielt verlangt. Sie koennen aber je nach Nutzung entstehen, z.B. wenn der Kunde Krankheits-, Abwesenheits- oder sonstige besonders schuetzenswerte Angaben erfasst oder hochlaedt. Fuer die Rechtmassigkeit solcher Eingaben ist der Kunde verantwortlich.

5. Pflichten von Invotica

Invotica verarbeitet personenbezogene Daten nur im Rahmen dieser AVV, der AGB, der Datenschutzerklaerung, der technischen Plattformfunktionen und dokumentierter Weisungen des Kunden.

Invotica trifft angemessene technische und organisatorische Massnahmen zum Schutz der Daten, insbesondere Zugriffskontrolle, Authentifizierung, Verschluesselung, Datenminimierung in Logs, regionale Infrastrukturwahl und Rollen-/Rechtekonzepte.

Personen, die fuer Invotica auf personenbezogene Daten zugreifen koennen, werden zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen oder vertraglichen Verschwiegenheitspflicht.

Invotica unterstuetzt den Kunden im zumutbaren Umfang bei der Erfuellung von Betroffenenrechten, bei Sicherheitsvorfaellen, bei Nachweisen gegenueber Behoerden und bei datenschutzrechtlichen Informationspflichten, soweit die Informationen Invotica vorliegen.

6. Pflichten des Kunden

Der Kunde ist verantwortlich fuer die Rechtmassigkeit der Verarbeitung, fuer die Auswahl der in Invotica gespeicherten Daten, fuer die Information betroffener Personen und fuer die erforderlichen Rechtsgrundlagen, Einwilligungen oder arbeitsrechtlichen Grundlagen.

Der Kunde darf keine Daten in Invotica verarbeiten, fuer die er keine ausreichende Rechtsgrundlage besitzt. Der Kunde ist insbesondere verantwortlich fuer die Nutzung von Mitarbeiterdaten, Lohnabrechnungen, Krankheits- oder Abwesenheitsangaben und sonstigen besonders schuetzenswerten Daten.

Der Kunde sorgt fuer sichere Benutzerverwaltung innerhalb seines Accounts, insbesondere fuer angemessene Passwoerter, Zugriffsbeschaenkungen, rechtzeitige Deaktivierung ausgeschiedener Nutzer und sorgfaeltige Verwendung eigener SMTP-Zugangsdaten.

7. Unterauftragsbearbeiter und Dienstleister

Der Kunde erteilt Invotica eine allgemeine Genehmigung, Unterauftragsbearbeiter und technische Dienstleister einzusetzen, soweit dies fuer Betrieb, Sicherheit, Support, Zahlungsabwicklung, Hosting, E-Mail-Versand oder optionale KI-Funktionen erforderlich ist.

Invotica setzt nur Dienstleister ein, die nach Invoticas Einschaeztung angemessene Datenschutz- und Sicherheitsmassnahmen bieten. Mit zentralen Dienstleistern bestehen entsprechende Datenschutzvereinbarungen bzw. deren Datenschutzbedingungen gelten als Vertragsbestandteil.

Die derzeit wesentlichen Dienstleister sind in Anlage 3 aufgefuehrt. Einzelne Anbieter, insbesondere Zahlungsdienstleister, koennen fuer bestimmte Verarbeitungsvorgaenge auch selbst Verantwortliche sein.

8. Internationale Datenuebermittlungen

Die primaere Speicherung der Anwendungsdaten erfolgt nach aktueller Konfiguration in der Schweiz bei Supabase, Region Central Europe (Zurich), und die Vercel Functions sind auf Frankfurt/EU konfiguriert. Dennoch koennen je nach Dienstleister, Funktion, Support, Zahlungsabwicklung, optionaler KI-Nutzung oder Subprozessor internationale Datenuebermittlungen, insbesondere in die USA, nicht vollstaendig ausgeschlossen werden.

Soweit erforderlich, stuetzt Invotica solche Uebermittlungen auf geeignete Garantien, etwa Angemessenheitsbeschuesse, Standardvertragsklauseln, Data Privacy Frameworks oder vergleichbare vertragliche und technische Schutzmechanismen.

9. Loeschung, Rueckgabe und Export

Nach Ende des Vertragsverhaeltnisses loescht oder anonymisiert Invotica personenbezogene Daten des Kunden nach Massgabe der AGB, der Datenschutzerklaerung, gesetzlicher Aufbewahrungspflichten und technischer Backup-Zyklen. Soweit technisch vorgesehen, kann der Kunde Daten vor Vertragsende exportieren.

Backups und technische Protokolle koennen fuer eine begrenzte Zeit weiterbestehen und werden im Rahmen der regulaeren Backup- und Log-Aufbewahrung ueberschrieben oder geloescht. Eine sofortige Einzelloeschung aus allen Backups ist regelmaessig nicht geschuldet, sofern die Daten dort nur eingeschaenkt und sicher verarbeitet werden.

10. Datensicherheit und Sicherheitsvorfaelle

Invotica trifft angemessene Massnahmen gegen unbefugten Zugriff, Verlust, Veraenderung oder Offenlegung personenbezogener Daten. Eine Zusammenfassung der technischen und organisatorischen Massnahmen findet sich in Anlage 2.

Invotica informiert den Kunden unverzueglich, wenn Invotica eine Verletzung der Datensicherheit feststellt, die personenbezogene Daten des Kunden betrifft und voraussichtlich ein Risiko fuer betroffene Personen begruendet. Invotica stellt dem Kunden die bekannten Informationen zur Verfuegung, soweit dies rechtlich und tatsaechlich moeglich ist.

11. Kontrolle, Nachweise und Audits

Invotica stellt dem Kunden auf angemessene Anfrage Informationen zur Verfuegung, die zur Beurteilung der Einhaltung dieser AVV erforderlich sind, etwa Angaben zu Dienstleistern, Regionen, Sicherheitsmassnahmen oder Datenschutzdokumenten.

Vor-Ort-Audits sind nur nach vorheriger Abstimmung, bei berechtigtem Anlass und unter Wahrung von Sicherheits-, Geheimhaltungs- und Betriebsinteressen von Invotica und anderen Kunden zulaessig. Invotica kann angemessene alternative Nachweise anbieten.

12. Rangfolge und Aenderungen

Bei Widerspruechen zwischen dieser AVV und den AGB gehen fuer Fragen der Auftragsbearbeitung die Regelungen dieser AVV vor. Im Uebrigen bleiben AGB und Datenschutzerklaerung anwendbar.

Invotica kann diese AVV anpassen, wenn dies wegen technischer, rechtlicher oder organisatorischer Aenderungen erforderlich ist. Wesentliche Aenderungen werden in geeigneter Weise kommuniziert oder in den AGB bzw. der Datenschutzerklärung aktualisiert.

Anlage 1 - Beschreibung der Verarbeitung

Gegenstand	Beschreibung
Dienst	Invotica SaaS-Plattform fuer Verwaltung, Rechnungen, Offerten, Mitarbeiter-/Zeitdaten, Dokumente, E-Mail-Versand und optionale KI-Funktionen.
Zwecke	Bereitstellung, Betrieb, Wartung, Support, Sicherheit, Abrechnung, Kommunikation, Dokumentenerstellung und vom Kunden ausgeloste Prozesse.
Betroffene Personen	Nutzer/Admins des Kunden, Mitarbeiter, Ansprechpartner, Kunden/Lieferanten des Kunden, Rechnungsempfaenger und sonstige vom Kunden erfasste Personen.
Datenarten	Stammdaten, Kontakt- und Kommunikationsdaten, Rechnungs-/Offertdaten, Mitarbeiter-/Zeitdaten, Lohn-/Abrechnungsdaten, technische Login-/Sicherheitsdaten, freiwillige Eingaben.
Besondere Daten	Nicht gezielt erforderlich, koennen aber durch Kundennutzung entstehen, z.B. Krankheits-/Abwesenheitsangaben oder sensible Mitarbeiterdokumente.
Dauer	Vertragsdauer plus technische, gesetzliche und berechnigte Aufbewahrungsfristen.

Anlage 2 - Technische und organisatorische Massnahmen (TOMs)

Bereich	Massnahmen
Zugriffskontrolle	Authentifizierung, Session-/JWT-Mechanismen, Rollen- und Rechtekonzepte, Trennung von Mandanten-/Kundendaten.
Transport- und Speicherschutz	TLS/HTTPS fuer Uebertragung; Verschluesselung und Sicherheitsmechanismen der eingesetzten Infrastruktur; verschluesselte Speicherung sensibler SMTP-Zugangsdaten.
Datenminimierung	Keine unnoetigen personenbezogenen Daten in Serverlogs; JWTs nicht in PDF-URLs; private PDF-Responses mit no-store.
Infrastrukturregionen	Supabase Projektregion Central Europe (Zurich), Region-Code eu-central-2; Vercel Functions auf fra1 / Frankfurt konfiguriert.
Verfuegbarkeit	Cloud-Infrastruktur mit Backup-/Wiederherstellungsmechanismen der Dienstleister; technische Betriebsueberwachung im Rahmen der Plattform.
Trennung und Mandantenfaehigkeit	Logische Trennung von Kundendaten ueber Datenbank-, Authentifizierungs- und Berechtigungsmechanismen.
Dokumentenschutz	Private PDF-Routes mit no-store, Pragma no-cache, Expires 0 und X-Robots-Tag noindex/nofollow konfiguriert.
KI-Minimierung	Optionale Invotica-AI-Funktionen senden keinen automatischen Vollzugriff auf die Datenbank; uebermittelt werden nur Nutzereingaben und minimaler Kontext der genutzten Funktion.

Anlage 3 - Wesentliche Dienstleister / Unterauftragsbearbeiter

Dienstleister	Zweck	Region / Hinweis
Supabase	Datenbank, Authentifizierung, Storage, Backend-Infrastruktur	Projektregion Central Europe (Zurich), eu-central-2; DPA intern gespeichert.
Vercel	Hosting, Deployment, Serverless Functions, CDN/Edge-Infrastruktur	Functions auf fra1 / Frankfurt; Pro-Plan; DPA fuer Pro/Enterprise abgedeckt.
Hostpoint AG	SMTP/E-Mail-Versand fuer Invotica-Systemmails	Schweiz; ADV/DPA nach Hostpoint-Bedingungen/AGB.
Stripe	Zahlungsabwicklung, Abo- und Rechnungsbezogene Zahlungsdaten	Kann je nach Vorgang als Processor und/oder Controller handeln; DPA/Data Transfers intern gespeichert.
Anthropic	Optionale Invotica-AI-Funktionen, Verarbeitung von Nutzereingaben und minimalem Kontext	Drittlandverarbeitung moeglich; Nutzung nur fuer optionale KI-Funktionen.
Google Analytics	Webanalyse nur soweit eingesetzt und rechtlich zulaessig, insbesondere bei Einwilligung	Kann Drittlandbezug haben; Details in Datenschutzerklärung.
Kundeneigene SMTP-Server	Vom Kunden konfigurierte Mailserver fuer E-Mail-Versand aus Invotica	Der Kunde ist fuer Auswahl, Rechtmassigkeit und Sicherheit der eigenen SMTP-Konfiguration verantwortlich.