Auftragsverarbeitungsvertrag (AVV)

nach Artikel 28 DSGVO für die SaaS-Plattform Kiosa

Version 2.1 — Stand: 20. Oktober 2026 · für bestehende Verträge wirksam ab 1. Dezember 2026

Parteien

Verantwortlicher (Auftraggeber): Der Kunde (Gastronomiebetrieb)

Auftragsverarbeiter (Auftragnehmer): Alchemista Rituals OÜ, Ahtri tn 12, 10151 Tallinn, Estland.

Geschäftsführer: Sven Schneider. USt-IdNr.: EE102913396.

Kontakt für Datenschutzanfragen: datenschutz@kiosa.ai

§ 1 Gegenstand und Dauer

1.1 Der Auftragsverarbeiter stellt dem Auftraggeber mit der SaaS-Plattform Kiosa ein webbasiertes Dashboard zur Verfügung. Im Rahmen dieser Plattformnutzung verarbeitet der Auftragsverarbeiter personenbezogene Daten des Auftraggeber gemäß den Bestimmungen dieses Vertrags und den Anweisungen des Auftraggebers.

1.2 Die Verarbeitung personenbezogener Daten erfolgt für die in § 2 definierten Zwecke. Sie beginnt mit der Leistungserbringung nach dem Hauptvertrag (AGB von Alchemista Rituals OÜ und anwendbarer Servicevertrag) und dauert nach dessen Beendigung ausschließlich für die in § 12 geregelte Rückgabe, Aufbewahrung und Löschung fort. Eine Anonymisierung nach § 2.11 erfolgt nur während der Vertragslaufzeit.

1.3 Mit Beendigung des Nutzungsverhältnisses werden die personenbezogenen Daten gemäß § 12 dieses Vertrags gelöscht oder zurückgegeben.

§ 2 Art und Zweck der Verarbeitung

Der Auftragsverarbeiter führt folgende Verarbeitungstätigkeiten durch:

2.1 Aggregation und Aufbereitung von Geschäftsdaten des Auftraggeber aus verschiedenen Drittsystemen (z. B. Kassensysteme, Zeiterfassung, Lohnverwaltung).

2.2 Berechnung von Key Performance Indicators (KPIs), Forecasts und Business Analytics basierend auf den aggregierten Daten, einschließlich Training, Kalibrierung und Bewertung kundenbezogener Modelle (§ 4a Abs. 1 AGB).

2.3 Generierung von KI-gestützten Briefings und Reports mit textuellen Interpretationen und Handlungsempfehlungen.

2.4 Versand von automatisierten Benachrichtigungs-E-Mails an konfigurierte Empfänger (Admin-User des Auftraggeber).

2.5 Bereitstellung eines rollenbasierten Dashboards mit Echtzeit- und historischen Auswertungen.

2.6 Empfang und strukturierte Erfassung von Eingangsrechnungen des Auftraggeber (PDF-Upload, E-Mail-Inbox, strukturierte E-Rechnungen im ZUGFeRD- und XRechnung-Format).

2.7 Workflow-gestützte Rechnungsfreigabe mit konfigurierbarer Approval-Kette (Inhaltliche Prüfung durch Restaurant-/Küchenleitung, Freigabe durch Geschäftsführung, Ausführung durch Buchhaltung) inklusive Audit-Trail mit Hash-Chain zur Erkennung nachträglicher Änderungen.

2.8 Vermittlung von SEPA-Überweisungs- und SEPA-Lastschrift-Initiierungen über den zugelassenen Zahlungsdienstleister BANKSapi Technology GmbH (München). BANKSapi erbringt die regulierten Zahlungsdienste eigenverantwortlich gegenüber dem Auftraggeber und ist NICHT Unterauftragsverarbeiter

des Auftragsverarbeiters. Die Datenschutzhinweise und Nutzungsbedingungen von BANKSapi werden dem Auftraggeber im Onboarding-Prozess vorgelegt (siehe § 8.4).

2.9 Abruf und Auswertung von Bankkontobewegungen des Auftraggeber über BANKSapi für die automatisierte Zuordnung von Bank-Buchungen zu offenen Rechnungen (Reconciliation), Erstellung von Liquiditäts- und Cashflow-Prognosen sowie Anomalie-Erkennung (z. B. fehlende oder unerwartete Lastschriften).

2.10 KI-gestützte Auto-Kontierungs-Vorschläge basierend auf historischen Buchungsmustern und vom Auftraggeber importierten DATEV- oder Agenda-Buchungsstapeln, Bereitstellung interaktiver KI-Beratung zu einzelnen Belegen (Frage-Antwort) sowie proaktive Hinweise zu Auffälligkeiten (Anomalien, IBAN-Wechsel, Liquiditätsengpässen).

2.11 Anonymisierung personenbezogener Daten des Auftraggebers zur Verwendung für übergreifende Modelle und Netzwerk-Funktionen nach § 4a AGB. Vor jeder übergreifenden Verwendung werden direkte und indirekte Identifikatoren entfernt oder verallgemeinert (insbesondere Namen, Nutzer- und Mitarbeiterkennungen, Freitexte). Übergreifende Modelle werden ausschließlich mit Daten ohne Personenbezug oder mit nach dieser Ziffer anonymisierten Daten trainiert; pseudonymisierte personenbezogene Daten werden hierfür nicht verwendet. Mit der Anonymisierung endet die Verarbeitung personenbezogener Daten im Sinne dieses Vertrags. Lässt sich die Anonymität für eine Datenklasse nicht hinreichend sicher feststellen, unterbleibt deren übergreifende Verwendung. Der Auftraggeber stellt sicher, dass ihm für diese Weisung eine Rechtsgrundlage zur Verfügung steht (§ 9 Abs. 4 AGB); die Pflichten des Auftragsverarbeiters bleiben unberührt.

2.12 Speicherung von Entscheidungen und Rückmeldungen der berechtigten Nutzer zu Vorschlägen, Hinweisen und Empfehlungen (Aktion, Zeitpunkt, Nutzerkennung, angezeigter Datenkontext) zur Nachvollziehbarkeit, zur Wirkungsmessung und zur Verbesserung der Plattform nach § 4a AGB, beschränkt auf die hierfür erforderlichen Inhalte. Die Daten werden für die Dauer des Vertrags gespeichert und nach § 12 gelöscht; Zugriff haben der Auftraggeber und, soweit für Betrieb und Verbesserung erforderlich, Mitarbeiter des Auftragsverarbeiters.

2.13 Zeitversetzte oder filialweise gestaffelte Bereitstellung von Hinweisen und Empfehlungen zur Wirkungsmessung nach § 4a Abs. 5 AGB. Die Leistung einzelner Mitarbeiter ist nicht Gegenstand der Messung.

2.14 Aufbau einer Kundenbasis des Auftraggeber aus Loyalty-Programm, Reservierungs- und Kassensystem für Gäste, deren Daten der Auftraggeber auf einer Rechtsgrundlage (insbesondere Einwilligung) einbringt, Abgleich von Einwilligungen und Auswertungen zu Besuchen und Kundenbindung.

2.15 Abruf von Bewertungen (Google Business Profile, Lieferplattformen), Auswertung sowie Erstellung AI-gestützter Antworten, die je nach Einstellung des Auftraggebers als Entwurf zur Freigabe vorgelegt oder automatisch veröffentlicht werden. Die Aktivierung der automatischen Veröffentlichung durch einen berechtigten Nutzer ist eine dokumentierte Weisung des Auftraggebers; sie kann jederzeit deaktiviert werden. Antworten werden ausschließlich aus Bewertung, Note, Name des Bewertenden und Angaben zum Betrieb erzeugt.

2.16 Erstellung von Dienstplanvorschlägen anhand des Personalbedarfs, der vom Auftraggeber vorgegebenen Regeln und Mitarbeitermerkmale sowie Zeiterfassung und Verwaltung von Verfügbarkeiten und Abwesenheiten im Rahmen der gebuchten Module. Der Dienstplanvorschlag beruht auf mathematischer Optimierung mit festgelegter Zielfunktion und Nebenbedingungen. Individuelle Leistungsbewertungen, Rankings einzelner Mitarbeiter und darauf beruhende Empfehlungen zu Einstellung, Entlassung, Vergütung oder Schichtzuteilung durch den AI-Partner sind kein Verarbeitungszweck; Krankheitstage fließen nicht in solche Auswertungen oder übergreifende Modelle ein.

§ 3 Kategorien personenbezogener Daten

Der Auftragsverarbeiter verarbeitet folgende Kategorien personenbezogener Daten:

3.1 Nutzerkontodaten der nach § 9 Abs. 5 AGB berechtigten Nutzer (Admin-User und weitere Nutzer): E-Mail-Adresse, Vor- und Nachname, Rolle im System, Benachrichtigungseinstellungen, Login-Status und Zeitstempel, Passwort-Hash (bcrypt mit 12 Salt-Rounds), WebAuthn-Credentials.

3.2 Mitarbeiterdaten des Auftraggeber: Vorname und Nachname, Rolle/Funktion, Arbeitsbereich (Service, Küche, Spüler), Qualifikationen je Arbeitsbereich und vom Auftraggeber festgelegte Erfahrungsstufe, Vertragsstunden, Verfügbarkeiten und Planungswünsche, externe Mitarbeiter-Identifikationsnummern (z. B. gastromatic ID), Kassierer-Identifikation und Name aus dem verbundenen Kassensystem.

3.3 Mitarbeiter-Arbeitszeitdaten: Schichtbeginn und Schichtende, Pausendauer in Minuten, Netto-Arbeitsminuten, zugeordneter Arbeitsbereich, Datenquelle (Zeiterfassungssystem), Abwesenheiten einschließlich Krankheitstagen (ohne Diagnose; besondere Kategorie nach Art. 9 DSGVO, Rechtsgrundlage beim Auftraggeber als Arbeitgeber).

3.4 Lohndaten: Stundenlohn pro Mitarbeiter, Gültigkeitszeitraum der Lohndaten, Import-Batch-Referenz.

3.5 Gästedaten werden nur im Umfang von § 3.12 und § 3.13 verarbeitet. Reservierungs- und Bestelldaten aus Reservierungs- und Kassensystemen werden ohne Namen und Kontaktdaten der Gäste gespeichert; ausgenommen sind Namen und Kontaktdaten, die der Auftraggeber nach § 3.12 rechtmäßig in die Kundenbasis übernimmt.

3.6 Lieferanten- und Geschäftspartnerdaten des Auftraggeber: Firmenname, Anschrift, Bankverbindung (IBAN/BIC, App-seitig verschlüsselt at-rest), Kontaktdaten, Steuer-Identifikationsmerkmale (falls in Rechnungen enthalten), zugeordnete Kreditor-Kontonummer im Buchhaltungssystem.

3.7 Beleginhaltliche Daten: Rechnungsnummer, Belegdatum, Beträge (Netto/Brutto/Steuer-Aufschlüsselung), Verwendungszweck, Leistungsbeschreibung, Zahlungsbedingungen, Mandatsreferenzen (bei SEPA-Lastschriften), End-to-End-Referenzen, Beleg-PDF/-XML als Original im verschlüsselten Speicher.

3.8 Bankkonto-Bewegungsdaten des Auftraggeber: IBAN/BIC des Tenant-Bankkontos (App-seitig verschlüsselt at-rest mit HMAC-Fingerprint für Equality-Lookup), Kontostand, Buchungszeitpunkt, Betrag, Verwendungszweck, Empfänger/Sender (Name, IBAN), Buchungs-ID des Providers.

3.9 Approval- und Audit-Daten: Aktor-User-ID, ausgeführte Aktion, Zeitstempel, optional Vertretungs-Referenz (representedUserId bei Substitution), Begründung bei Ablehnung/Rückgabe, Hash-Chain-Eintrag zur Manipulationsdetektion.

3.10 AI-Outputs: Anomalie-Erklärungen, Triage-Zusammenfassungen, Onboarding-Vorschläge, Cashflow-Warnungen, Antworten des AI-Partners, Bewertungsantworten — können Bezug auf Lieferanten-, Buchungs- oder Mitarbeiterdaten enthalten. Werden aus den verarbeiteten Geschäftsdaten generiert; eine Anreicherung erfolgt nur mit öffentlich verfügbaren Daten (z. B. Wetter, Feiertage, Veranstaltungen) und mit Ergebnissen aus Netzwerk-Funktionen nach § 4a Abs. 3 AGB, die keine personenbezogenen Daten anderer Auftraggeber enthalten.

3.11 Entscheidungs- und Rückmeldungsdaten der berechtigten Nutzer: ausgeführte Aktion (Freigabe, Ablehnung, Korrektur, Bewertung), Zeitstempel, Nutzerkennung, optionale Begründung, Momentaufnahme des angezeigten Datenkontexts.

3.12 Gästedaten der Kundenbasis aus Loyalty-Programm, Reservierungs- und Kassensystem des Auftraggebers, soweit der Auftraggeber sie auf einer Rechtsgrundlage (insbesondere Einwilligung) einbringt: E-Mail-Adresse, Vor- und Nachname (feldverschlüsselt, Identität nur als HMAC der E-Mail-Adresse), Quelle, Einwilligungsstatus und -zeitpunkt, Zeitpunkt des letzten Besuchs, Filialzuordnung. Widerruf und Löschung werden auf Anweisung des Auftraggebers umgesetzt.

3.13 Bewertungsdaten: Name des Bewertenden (wie von der Plattform angezeigt), Bewertungstext, Note, Datum sowie Antwortentwürfe und veröffentlichte Antworten. Bewertungstexte können Angaben enthalten, die der Bewertende selbst veröffentlicht hat.

§ 4 Kategorien betroffener Personen

Die Verarbeitung betrifft personenbezogene Daten folgender Kategorien betroffener Personen:

4.1 Berechtigte Nutzer mit Zugang zur Kiosa-Plattform, einschließlich eingeladener Mitarbeiter verbundener Betriebe und Berater nach § 9 Abs. 5 AGB.

4.2 Mitarbeiter des Auftraggeber (Beschäftigte im Gastronomiebetrieb), deren Arbeitszeiten, Rollen und Lohndaten in die Plattform importiert werden.

4.3 Vertretene Personen im Sinne der Substitution-Funktion (Vertretung bei Abwesenheit eines Approver), sofern eine aktive Vertretung läuft.

4.4 Kontaktpersonen bei Lieferanten des Auftraggeber, sofern Name oder Kontaktdaten in den Beleg-Inhalten oder Stammdaten enthalten sind.

4.5 Gäste des Auftraggeber, deren Daten nach § 3.12 verarbeitet werden, sowie Personen, die den Auftraggeber auf Bewertungsplattformen bewertet haben (§ 3.13).

§ 5 Weisungsgebundenheit

5.1 Der Auftragsverarbeiter verarbeitet die in diesem Vertrag genannten personenbezogenen Daten ausschließlich auf dokumentierte Weisungen des Auftraggeber.

5.2 Die Weisungen ergeben sich insbesondere aus: - Dem Hauptvertrag und den AGB von Alchemista Rituals OÜ - Der Konfiguration der Plattform durch den Auftraggeber (Konfigurationseinstellungen, Datenquellen, Benachrichtigungsregeln, Approval-Chain-Auswahl, Bank-Anbindungen) - § 4a der AGB (eigene Modelle, Netzwerk-Funktionen, Wirkungsmessung) als dokumentierte Weisung für die Verarbeitungen nach §§ 2.11 bis 2.13

5.3 Sollte der Auftraggeber den Auftragsverarbeiter anweisen, personenbezogene Daten auf rechtswidrige Weise zu verarbeiten, wird der Auftragsverarbeiter den Auftraggeber unverzüglich darauf hinweisen und die Verarbeitung verweigern.

§ 6 Vertraulichkeit

6.1 Der Auftragsverarbeiter gewährleistet, dass alle Personen, die Zugang zu personenbezogenen Daten des Auftraggeber haben, auf Vertraulichkeit verpflichtet sind oder einer rechtlichen Geheimhaltungspflicht unterliegen.

6.2 Der Zugang zu personenbezogenen Daten ist auf das erforderliche Personal beschränkt, das für die Verarbeitung gemäß § 2 notwendig ist.

§ 7 Technische und organisatorische Maßnahmen (TOMs)

7.1 Der Auftragsverarbeiter implementiert angemessene technische und organisatorische Maßnahmen zur Sicherung der Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten:

Zugangs- und Zugriffskontrolle - E-Mail/Passwort-Authentifizierung mit bcrypt Hashing (12 Salt-Rounds) - WebAuthn/Passkey-Authentifizierung - JWT-basierte Sessions mit 8-Stunden-Gültigkeitsdauer - Begrenzung von Anmelde- und Passwort-Rücksetzversuchen je IP-Adresse (Rate Limiting) - Rollenbasierte Zugriffskontrolle (RBAC) mit definierten Rollen (Banking-spezifisch: ADMIN, GESCHAEFTSFUEHRER, RESTAURANT_KUECHENLEITUNG, BUCHHALTUNG) - Restaurant-Scope-Enforcement: Mitglieder der Rolle RESTAURANT_KUECHENLEITUNG sehen ausschließlich Daten der ihnen zugeordneten Filiale - Substitution

(Vertretung) nur durch ADMIN konfigurierbar; ADMIN-Rolle ist selbst nicht vertretbar - Multi-Tenant-Isolation auf Anwendungsebene (Datenseparation nach Kundeninstanzen) - Zugriffe von Mitarbeitern des Auftragsverarbeiters auf Daten des Auftraggebers nur, soweit für Betrieb, Support, Sicherheit oder die nach diesem Vertrag zulässige Verbesserung und Weiterentwicklung der Plattform erforderlich; Anmeldungen im Namen eines Auftraggebers werden protokolliert - Bearer-Token-Authentifizierung für automatisierte Hintergrundjobs

Verschlüsselung - TLS/HTTPS mit HSTS (HTTP Strict Transport Security) für Transit-Verschlüsselung - Feldverschlüsselung sicherheitskritischer Daten mit AES-256-GCM: Bankverbindungen (IBAN), E-Rechnungs-XML, Zugangsdaten und Tokens zu angebundenen Systemen, Kontaktdaten der Gäste-Kundenbasis, Zahlungsexport-Dateien - HMAC-SHA256-Fingerprints für Gleichwert-Abfragen ohne Klartext-Zugriff (IBAN, Gäste-Identität je Mandant) - Schlüssel getrennt von der Datenbank in der geschützten Konfiguration der Hosting-Umgebung; Rotation anlassbezogen nach dokumentiertem Verfahren - Keine Übermittlung von Kontaktdaten der Gäste-Kundenbasis an AI-Dienstleister oder über die MCP-Schnittstelle

Integrität und Audit - Append-Only-Postgres-Trigger auf ApprovalEvent und PaymentOrder: im regulären Anwendungsbetrieb UPDATE/DELETE serverseitig blockiert; Korrekturen über neue Audit-Events mit Referenz auf den vorherigen Eintrag. Löschungen und rechtlich gebotene Berichtigungen nach §§ 10 und 12 erfolgen über ein gesondertes, kontrolliertes und protokolliertes Verfahren. - Hash-Chain-Verifikation (SHA-256 mit canonical Serialization) auf allen Approval- und Zahlungs-Aktionen als nächtlicher Hintergrund-Job. Bei Mismatch Alarmierung der Tenant-Administratoren. - Signierte Callback-States (JWT mit 30-min-Gültigkeit + Nonce-Replay-Schutz) für BANKSapi-Webform-Rückkehr. Callback-Host-Allowlist im Code festgelegt.

Sicherheits-Header - Content Security Policy (CSP) - X-Frame-Options: DENY (Schutz vor Clickjacking) - X-Content-Type-Options: nosniff (Schutz vor MIME-Type-Sniffing) - HSTS (HTTP Strict Transport Security) - Referrer-Policy zur Kontrolle von Referrer-Informationen

Datenbankzugriff - Verwendung von Prisma ORM mit parametrisierten Queries zur Vermeidung von SQL-Injection - Keine direkte Exposition der Datenbankverbindungen nach außen

Verfügbarkeit und Wiederherstellung - Tägliche Sicherung des Servers über die Backup-Funktion des Hosting-Anbieters (rollierend, 7 Tage) - Zusätzliche Sicherung der Datenbank vor jeder Änderung der Datenbankstruktur bei Updates (Löschung spätestens nach 30 Tagen) - Automatischer Gesundheitscheck nach Updates mit Rückkehr zur vorherigen Version bei Fehlschlag

Infrastruktur und Bereitstellung - Containerisierung mit Docker Compose für isolierte Umgebungen - Automatisierte CI/CD-Pipelines - Nginx Reverse Proxy als Zugangsgateway

7.2 Der Auftragsverarbeiter darf die Maßnahmen an den technischen Fortschritt anpassen, sofern das Schutzniveau nach § 7.1 nicht unterschritten wird.

§ 8 Unterauftragsverarbeiter (Sub-Processors)

8.1 Der Auftragsverarbeiter nutzt die folgenden Unterauftragsverarbeiter zur Durchführung spezifischer Verarbeitungsfunktionen:

Dienstleister	Land	Funktion	Verarbeitete Daten
Anthropic PBC	USA (San Francisco)	AI-Textgenerierung, Analyse und Extraktion (Claude API) für Funktionen der Plattform (u. a. AI-Partner, Briefings, Reports, Bewertungsantworten, Beleg- und Rezepterfassung; Zuordnung je Funktion),	Geschäftsdaten, Beleg-Inhalte, ggf. Mitarbeiternamen, Namen und Texte von Bewertungen; keine Kontaktdaten der Gäste-Kundenbasis

Dienstleister	Land	Funktion	Verarbeitete Daten
		NICHT für den Cashflow-/Banking-AI-Layer	
OpenServ Labs Ltd, 71–75 Shelton Street, Covent Garden, London WC2H 9JQ, Vereinigtes Königreich	Vereinigtes Königreich (Angemessenheitsbeschluss Art. 45 DSGVO)	AI-Inferenz für Funktionen der Plattform (Zuordnung je Funktion); für den Cashflow-/Banking-AI-Layer wird ausschließlich OpenServ eingesetzt	Geschäftsdaten, Beleg-Inhalte, ggf. Mitarbeiternamen; im Banking-Layer IBANs maskiert und Gegenpartei-/Lieferantennamen pseudonymisiert; keine Kontaktdaten der Gäste-Kundenbasis; keine Daten anderer Auftraggeber
Voyage AI Innovations, Inc. (MongoDB-Gruppe)	USA	Embeddings (Vektor-Repräsentationen) für Artikel-, Zutaten- und Rezeptabgleich sowie das Gedächtnis des AI-Partners; Nutzung der Daten zum Modelltraining durch den Anbieter abgewählt	Artikel-, Zutaten- und Rezeptbezeichnungen; Gedächtnisnotizen des AI-Partners (können Mitarbeiternamen enthalten); keine Kontaktdaten der Gäste-Kundenbasis
Resend Inc.	USA	E-Mail-Versand (Benachrichtigungen, Eskalationen, Reports)	Empfänger-E-Mail-Adressen, HTML-E-Mail-Body
GitHub Inc. (Microsoft)	USA	Code-Hosting, CI/CD, Bearbeitung von Support-Anfragen	Betreff und Text von Support-Anfragen der Admin-User (vorab redigiert), Verweise auf Anhänge
Hetzner Online GmbH	Deutschland (Falkenstein/Nürnberg)	Server-Hosting, Datenbank-Hosting, Datensicherung	Alle verarbeiteten Daten

8.2 Allgemeine Genehmigung und Änderungen: Der Auftraggeber genehmigt die in Anlage 2 genannten Unterauftragsverarbeiter. Über die beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters informiert der Auftragsverarbeiter mindestens 30 Tage vorab per E-Mail. Der Auftraggeber kann innerhalb dieser Frist aus berechtigten datenschutzrechtlichen Gründen in Textform widersprechen. Der Auftragsverarbeiter prüft den Einwand und kann eine wirtschaftlich zumutbare Abhilfe anbieten; zu einer unwirtschaftlichen Sonderlösung ist er nicht verpflichtet. Bleibt ein berechtigter Einwand bestehen, kann der Auftragsverarbeiter die betroffene, trennbare Leistung (z. B. ein Modul) vor dem Wechsel aussetzen oder zum Wechseltermin beenden; der Auftraggeber kann diese Leistung ebenfalls zum Wechseltermin kündigen. Solange der Einwand nicht gelöst oder die erforderliche Genehmigung nicht anderweitig wirksam erteilt ist, erhält der neue Unterauftragsverarbeiter für diese Leistung keine Daten des widersprechenden Auftraggebers. Ohne fristgerechten Widerspruch gilt die Änderung als genehmigt. Muss ein Unterauftragsverarbeiter aus Sicherheits-, Rechts- oder Verfügbarkeitsgründen dringend ersetzt werden, informiert der Auftragsverarbeiter unverzüglich vorab unter Angabe des Grundes und einer verkürzten, angemessenen Widerspruchsfrist; ist eine rechtmäßige Überbrückung nicht möglich, kann er die betroffene Funktion bis zur Klärung aussetzen. Aus der rechtmäßigen Änderung als solcher stehen dem Auftraggeber keine weiteren Ansprüche zu; zwingende Rechte bleiben unberührt.

8.3 Hinweis zu Datenquellen: Kassen-, Personal-, Lohn- und Reservierungssysteme (z. B. OktoPOS, Gastronovi, Hypersoft, gastromatic, ordio, e2n, zeit-lohn, OpenTable), Google (Business Profile, Places, Sheets/Drive), Lieferplattformen und Open-Meteo sind KEINE Unterauftragsverarbeiter, sondern Datenquellen, auf die der Auftragsverarbeiter lesend zugreift; bei Google Business Profile erfolgt zur Veröffentlichung von Bewertungsantworten nach § 2.15 zusätzlich ein schreibender Zugriff entsprechend der Konfiguration des

Auftraggebers. Gleiches gilt für vom Auftraggeber bereitgestellte DATEV- oder Agenda-Buchungsstapel-Exports. Stripe Payments Europe Ltd. rechnet die Kiosa-Lizenz gegenüber dem Auftraggeber ab; diese Verarbeitung erfolgt in eigener Verantwortung des Auftragsverarbeiters und nicht im Auftrag.

8.4 Hinweis zu BANKSapi: Die BANKSapi Technology GmbH (München, Deutschland) ist KEIN Unterauftragsverarbeiter im Sinne dieses Vertrags. BANKSapi erbringt reguläre Zahlungsdienste (Kontoinformationsdienst gemäß § 1 Abs. 34 ZAG, Zahlungsauslösedienst gemäß § 1 Abs. 33 ZAG) eigenverantwortlich gegenüber dem Auftraggeber als Zahlungsdienstenutzer (PSU). BANKSapi hat eigene Datenschutzhinweise und Nutzungsbedingungen mit dem Auftraggeber, die im Onboarding vorgelegt werden. Der Auftragsverarbeiter agiert als Schnittstellen-Vermittler zwischen Kiosa-Plattform und BANKSapi-API. Die Autorisierung von Zahlungsaufträgen erteilt der Auftraggeber gegenüber BANKSapi bzw. seiner Bank; die Rechnungsfreigabe in Kiosa ersetzt sie nicht. Die Datenschutzhinweise und Nutzungsbedingungen von BANKSapi sind verfügbar unter: - https://banksapi.io/customer/v2/webform/docs/2025_09_05_BANKSapi_Datenschutzhinweise.pdf - https://banksapi.io/customer/v2/webform/docs/2025_09_18_BANKSapi_Nutzungsbedingungen.pdf

8.5 Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter vertraglich im Wesentlichen gleichwertige Datenschutzpflichten auf wie in diesem Vertrag. Er bleibt gegenüber dem Auftraggeber für die Einhaltung der Pflichten der Unterauftragsverarbeiter nach Art. 28 Abs. 4 DSGVO verantwortlich; § 13 AGB bleibt unberührt.

8.6 Soweit Unterauftragsverarbeiter Daten außerhalb des EWR verarbeiten, erfolgt die Übermittlung auf Grundlage eines Angemessenheitsbeschlusses (Art. 45 DSGVO, z. B. Vereinigtes Königreich oder EU-US Data Privacy Framework bei zertifizierten Empfängern) oder der Standardvertragsklauseln der EU-Kommission (Beschluss 2021/914, Art. 46 Abs. 2 lit. c DSGVO). Die Grundlage je Empfänger ist in Anlage 2 angegeben.

§ 9 Meldepflichten bei Datenpannen

9.1 Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich nach Kenntnis einer Datenpanne (im Sinne von Artikel 33 DSGVO) mit den zu diesem Zeitpunkt verfügbaren Informationen, spätestens innerhalb von 48 Stunden. Weitere Informationen werden nachgereicht, sobald sie vorliegen.

9.2 Die Benachrichtigung muss folgende Informationen enthalten: - Art und Umfang der Datenpanne - Betroffene Kategorien personenbezogener Daten und ungefähre Anzahl betroffener Personen - Wahrscheinliche Folgen der Datenpanne - Gegenmaßnahmen und empfohlene Maßnahmen zur Schadensminderung

9.3 Der Auftraggeber ist verantwortlich für die Benachrichtigung der betroffenen Personen und der zuständigen Aufsichtsbehörden gemäß den Anforderungen der DSGVO (insbesondere Artikel 33 und 34).

§ 10 Unterstützung bei Betroffenenrechten

10.1 Betroffene Personen (insbesondere Admin-User, Mitarbeiter, Gäste, Bewertende und Kontaktpersonen bei Lieferanten) richten Anfragen zu ihren Rechten (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit) an den Auftraggeber als Verantwortlichen. Erreicht eine solche Anfrage den Auftragsverarbeiter, leitet er sie unverzüglich an den Auftraggeber weiter.

10.2 Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Erfüllung dieser Anfragen, indem er: - Personenbezogene Daten zur Verfügung stellt (für Auskunftsanfragen) - Daten korrigiert oder aktualisiert (auf Anweisung des Auftraggebers) - Daten löscht (auf Anweisung des Auftraggebers); eine Pseudonymisierung erfolgt nur als vorübergehende Schutzmaßnahme oder nach § 12.5 - Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellt (für Datenportabilität, über den Daten-Export)

§ 11 Unterstützung bei Datenschutz-Folgenabschätzungen

11.1 Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Durchführung von Datenschutz-Folgenabschätzungen (DPIA) gemäß Artikel 35 DSGVO, soweit die Verarbeitung im Rahmen der Plattform Kiosa betroffen ist.

11.2 Der Auftragsverarbeiter stellt dem Auftraggeber auf Anfrage die erforderlichen Informationen über die Art der Verarbeitung, die implementierten technischen und organisatorischen Maßnahmen sowie die Risikobewertung zur Verfügung, die der Auftraggeber für die Durchführung einer DPIA benötigt. Eine vom Auftragsverarbeiter eigenständig erstellte DPIA für die SaaS-Plattform Kiosa liegt vor und wird dem Auftraggeber auf Anfrage zur Verfügung gestellt.

11.3 Sofern eine vorherige Konsultation der zuständigen Aufsichtsbehörde gemäß Artikel 36 DSGVO erforderlich ist, unterstützt der Auftragsverarbeiter den Auftraggeber auch bei dieser Konsultation im Rahmen des Zumutbaren.

§ 12 Löschung und Rückgabe nach Vertragsende

12.1 Nach Vertragsende kann der Auftraggeber innerhalb von neunzig (90) Tagen die Rückgabe seiner Daten durch Export nach § 12.2 verlangen; auf seine Weisung löscht der Auftragsverarbeiter früher. Nach Ablauf dieser Frist löscht der Auftragsverarbeiter alle personenbezogenen Daten des Auftraggebers, soweit nicht nach dem Unionsrecht oder dem Recht eines Mitgliedstaats eine Pflicht des Auftragsverarbeiters zur Speicherung besteht.

12.2 Der Auftragsverarbeiter stellt die strukturierten Daten in einem gängigen maschinenlesbaren Format (z. B. CSV oder JSON) sowie die gespeicherten Originalbelege (PDF/XML) und die Freigabe-Audit-Trails zur Verfügung.

12.3 Eine Löschung entfällt insoweit, als die personenbezogenen Daten aufgrund von EU- oder Mitgliedstaatsrecht aufbewahrt werden müssen (z. B. Aufbewahrungspflichten nach Handelsrecht oder Steuerrecht). In diesem Fall wird der Auftragsverarbeiter die Daten entsprechend schützen und nur insoweit verarbeiten, wie es durch die Aufbewahrungspflicht erforderlich ist.

12.4 Aufbewahrungspflichten des Auftraggebers (z. B. § 257 HGB, § 147 AO) begründen keine Pflicht des Auftragsverarbeiters zur Speicherung über die Frist nach § 12.1 hinaus. Der Auftraggeber sichert aufbewahrungspflichtige Unterlagen durch den Export nach § 12.2. Eine Archivierung durch den Auftragsverarbeiter erfolgt nur nach gesonderter Vereinbarung über Umfang, Speicherort, Frist, Zugriff und Vergütung. Während der Vertragslaufzeit sind Beleg-, Freigabe- und Zahlungsdaten gegen nachträgliche Änderung geschützt (§ 7.1, Integrität und Audit); rechtlich gebotene Berichtigungen und Löschungen bleiben möglich und werden nachvollziehbar protokolliert.

12.5 Bei Ausscheiden eines Mitarbeiters oder Admin-Users löscht der Auftragsverarbeiter dessen Daten auf Anweisung des Auftraggebers. Soweit Audit-Trail-Einträge zur Nachvollziehbarkeit oder wegen Aufbewahrungspflichten des Auftraggebers erhalten bleiben müssen, wird die Referenz auf die Person pseudonymisiert (beispielsweise wird die E-Mail-Adresse zu deleted-user-{id}@removed.local ersetzt, Vor- und Nachname zu „Gelöschter Mitarbeiter“).

12.6 Datensicherungen werden nicht produktiv genutzt, gesichert vorgehalten und spätestens nach 30 Tagen überschrieben oder gelöscht. Wird eine Datensicherung wiederhergestellt, wendet der Auftragsverarbeiter zwischenzeitlich erfolgte Löschungen erneut an. Die Pflichten aus diesem Vertrag gelten bis zur vollständigen Löschung fort.

12.7 Von der Löschung nach § 12.1 ausgenommen sind ausschließlich die nach § 4a Abs. 6 AGB dauerhaft nutzbaren, personenbezugsfreien übergreifenden Modelle und verdichteten Wissensbestände (z. B. abstrakte Zuordnungen von Lieferantenartikeln zu Buchungskonten) sowie aggregierte Erkenntnisse. Kundenbezogene Rohbeiträge, Herkunftsmarker und Kontrollinformationen für die Schwellenprüfung werden nach § 12.1

entfernt. Die Ausnahme erlaubt keine personenbezogenen Restbestände; Vertraulichkeit und Ausgabeschwellen nach § 4a Abs. 3 AGB gelten weiter. Pseudonymisierte Daten sind personenbezogene Daten und werden nach § 12.1 gelöscht.

§ 13 Kontrollrechte

13.1 Der Auftraggeber hat das Recht, die Einhaltung der in diesem Vertrag festgelegten technischen und organisatorischen Maßnahmen zu überprüfen.

13.2 Durchführung: Überprüfungen erfolgen vorrangig durch Prüfung von Dokumenten und Nachweisen (z. B. Selbstauskunft zu § 7, Prüfberichte und Zertifikate der Unterauftragsverarbeiter) sowie remote. Eine Prüfung vor Ort ist zulässig, soweit konkrete erhebliche Zweifel an der Einhaltung dieses Vertrags auf diesem Weg nicht ausgeräumt werden können oder eine Aufsichtsbehörde dies verlangt. Sie wird mindestens 14 Werktage im Voraus angekündigt, es sei denn, ein konkreter Verdacht einer Datenschutzverletzung erfordert eine kürzere Frist, und findet während der Geschäftszeiten statt. Sie ist auf die Verarbeitung für den Auftraggeber beschränkt; Daten anderer Auftraggeber und Geschäftsgeheimnisse des Auftragsverarbeiters bleiben geschützt, eine Offenlegung von Quellcode erfolgt nicht. Prüfer müssen zur Verschwiegenheit verpflichtet sein und dürfen nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter stehen.

13.3 Kosten: Jeder Auftraggeber kann eine Überprüfung pro Kalenderjahr ohne Vergütung des Auftragsverarbeiters verlangen. Darüber hinausgehenden Aufwand, insbesondere für Prüfungen vor Ort, vergütet der Auftraggeber angemessen, es sei denn, die Prüfung ergibt einen wesentlichen Verstoß des Auftragsverarbeiters.

§ 14 Schlussbestimmungen

14.1 Salvatorische Klausel: Sollte eine Bestimmung dieses Vertrags ganz oder teilweise nicht gültig oder durchsetzbar sein, bleibt die Gültigkeit der übrigen Bestimmungen unberührt. Die ungültige oder nicht durchsetzbare Bestimmung wird durch eine gültige Regelung ersetzt, die der wirtschaftlichen Wirkung der ungültigen Bestimmung am nächsten kommt.

14.2 Anwendbares Recht und Gerichtsstand: Dieser Vertrag unterliegt estnischem Recht, ungeachtet seiner Kollisionsnormen. Beide Parteien vereinbaren die ausschließliche Gerichtsbarkeit der Gerichte in Tallinn, Estland.

14.3 Änderungen und Ergänzungen: Änderungen dieses Vertrags bedürfen der Textform. § 24 der AGB (Änderungen) gilt für diesen Vertrag entsprechend.

14.4 Dauer: Dieser Vertrag tritt mit dem Beginn der Datenverarbeitung in Kraft und gilt, solange der Auftraggeber die Kiosa-Plattform nutzt. Nach Beendigung des Nutzungsverhältnisses gilt er bis zur vollständigen Löschung der personenbezogenen Daten nach § 12 fort.

14.5 Vorrang: Bei Widersprüchen zwischen diesem Vertrag und den AGB gehen in datenschutzrechtlichen Fragen die Regelungen dieses Vertrags vor.

Anlage 1: Technische und organisatorische Maßnahmen (TOMs)

Die technischen und organisatorischen Maßnahmen ergeben sich aus § 7.1 in der Fassung dieses Vertrags (Version siehe Kopf). Änderungen nach § 7.2 teilt der Auftragsverarbeiter dem Auftraggeber bei wesentlichen Änderungen mit.

Anlage 2: Unterauftragsverarbeiter (Sub-Processors)

Die Anlage 2 enthält die aktuelle Liste der Unterauftragsverarbeiter gemäß § 8.

Unterauftragsverarbeiter	Ort	Verarbeitungstätigkeit	Übermittlungsgrundlage (§ 8.6)
Anthropic PBC	USA	AI-Textgenerierung, Analyse und Extraktion für Funktionen der Plattform (Zuordnung je Funktion)	Standardvertragsklauseln (DPA des Anbieters)
OpenServ Labs Ltd	Vereinigtes Königreich	AI-Inferenz für Funktionen der Plattform; ausschließlicher Dienstleister für den Cashflow-/Banking-AI-Layer	Angemessenheitsbeschluss (Art. 45 DSGVO)
Voyage AI Innovations, Inc. (MongoDB-Gruppe)	USA	Embeddings für Artikel-, Zutaten- und Rezeptabgleich und das Gedächtnis des AI-Partners	Standardvertragsklauseln (DPA des Anbieters)
Resend Inc.	USA	Automatisierter E-Mail-Versand	EU-US Data Privacy Framework und Standardvertragsklauseln (DPA des Anbieters)
GitHub Inc. (Microsoft)	USA	Quellcode-Versionierung, CI/CD, Bearbeitung von Support-Anfragen	EU-US Data Privacy Framework und/oder Standardvertragsklauseln (DPA des Anbieters)
Hetzner Online GmbH	Deutschland (Falkenstein/Nürnberg)	Infrastruktur und Datenhosting (Server, Datenbank, Datensicherung)	keine Drittlandübermittlung

Keine Unterauftragsverarbeiter, sondern Datenquellen oder eigenständige Dienstleister: - Kassen-, Personal-, Lohn- und Reservierungssysteme (z. B. OktoPOS, Gastronovi, Hypersoft, gastromatic, ordio, e2n, zeit-lohn, OpenTable), Google (Business Profile, Places, Sheets/Drive), Lieferplattformen, Open-Meteo (Datenquellen mit Lesezugriff; bei Google Business Profile zusätzlich Veröffentlichung von Bewertungsantworten nach § 2.15) - BANKSapi Technology GmbH (eigenständiger regulierter Zahlungsdienstleister mit eigenem PSU-Vertrag, siehe § 8.4) - DATEV-/Agenda-Buchungsstapel-Exports (vom Auftraggeber bereitgestellte Datenquellen, § 8.3) - Stripe Payments Europe Ltd. (Abrechnung der Kiosa-Lizenz in eigener Verantwortung des Auftragsverarbeiters)

Diese Liste wird regelmäßig überprüft und aktualisiert. Über Änderungen wird der Auftraggeber nach § 8.2 informiert.

Vertragsabschluss

Dieser Vertrag ist Bestandteil des Nutzungsvertrags (§ 11 Abs. 1 AGB) und kommt mit diesem elektronisch zustande.

Eine handschriftliche Unterschrift ist nicht erforderlich.

Version 2.1 — Stand: 20. Oktober 2026, für bestehende Verträge wirksam ab 1. Dezember 2026. Vorgänger: Version 2.0 (Mai/Juli 2026), Version 1.0 (März 2026). Erweiterungen in 2.1: §§ 2.11 bis 2.16, 3.11 bis 3.13, 4.5, 5.2, 7.2, 8.5, 8.6, 12.6, 12.7, 14.5 (neu); §§ 1.2, 2.2, 2.7, 3.1, 3.3, 3.5, 3.10, 7.1, 8.1 bis 8.4, 4.1, 9.1, 10.1, 10.2, 12.1, 12.2, 12.4, 12.5, 13.2, 13.3, 14.3, 14.4, Anlagen 1 und 2 (geändert).