# Auftragsverarbeitungsvertrag (AVV) — Kiosa

nach Artikel 28 DSGVO — Version 2.0

Stand: Juli 2026

# Auftragsverarbeitungsvertrag (AVV) nach Artikel 28 DSGVO für die SaaS-Plattform Kiosa

**Version 2.0 — Stand: Juli 2026 (Banking-Erweiterung)**

## Parteien

**Verantwortlicher (Auftraggeber):** Der Kunde (Gastronomiebetrieb)

**Auftragsverarbeiter (Auftragnehmer):** Alchemista Rituals OÜ Adresse: 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 der Anweisungen des Auftraggeber.

1.2 Die Verarbeitung personenbezogener Daten erfolgt für die in § 2 definierten Zwecke und dauert so lange an, wie das Nutzungsverhältnis zu Kiosa besteht. Der Beginn und das Ende der Verarbeitung bestimmen sich nach der Dauer des Hauptvertrags (AGB von Alchemista Rituals OÜ und anwendbarer Servicevertrag).

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.

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 GoBD-konformem Audit-Trail mit Hash-Chain-Integrität.

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).

---

## § 3 Kategorien personenbezogener Daten

Der Auftragsverarbeiter verarbeitet folgende Kategorien personenbezogener Daten:

3.1 **Admin-User-Daten des Auftraggeber:** 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), externe Mitarbeiter-Identifikationsnummern (z. B. gastromatic ID), Kassierer-Identifikation und Name aus dem verbundenen Kassensystem (OktoPOS).

3.3 **Mitarbeiter-Arbeitszeitdaten:** Schichtbeginn und Schichtende, Pausendauer in Minuten, Netto-Arbeitsminuten, zugeordneter Arbeitsbereich, Datenquelle (Zeiterfassungssystem).

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

3.5 **Hinweis:** Der Auftragsverarbeiter verarbeitet ausdrücklich KEINE Endkunden- oder Gästedaten. Bewertungsdaten werden nur in aggregierter Form (durchschnittliche Noten) verarbeitet, nicht individualisiert.

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 **KI-Outputs:** Anomalie-Erklärungen, Triage-Zusammenfassungen, Onboarding-Vorschläge, Cashflow-Warnungen — können Bezug auf Lieferanten- oder Buchungsdaten enthalten. Werden ausschließlich aus den verarbeiteten Geschäftsdaten generiert, keine Anreicherung aus externen Datenquellen.

---

## § 4 Kategorien betroffener Personen

Die Verarbeitung betrifft personenbezogene Daten folgender Kategorien betroffener Personen:

4.1 Admin-User des Auftraggeber mit Zugang zum Kiosa Dashboard.

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.

---

## § 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)

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 als hochsicherer Zugang
- JWT-basierte Sessions mit 8-Stunden-Gültigkeitsdauer
- 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)
- NextAuth Middleware für Sitzungsmanagement
- Bearer-Token-Authentifizierung für automatisierte Cron-Jobs

### Verschlüsselung

- TLS/HTTPS mit HSTS (HTTP Strict Transport Security) für Transit-Verschlüsselung
- bcrypt für Passwort-Hashing
- App-seitige Envelope-Verschlüsselung für Bank-Kontodaten (IBAN) und E-Rechnungs-XML-Payloads über AES-256-GCM. Master-Verschlüsselungsschlüssel im verwalteten Secret-Storage (Hetzner-Infrastruktur). HMAC-SHA256-Fingerprint pro IBAN für Gleichwert-Abfragen ohne Klartext-Zugriff. Schlüsselrotation: monatlich Master-KEK, Re-Encryption-Job für alle betroffenen Records.
- Postgres Transparent Disk Encryption (TDE) at-rest
- Verschlüsselte Datenbank-Backups, off-site Replikation

### Integrität und Audit

- Append-Only-Postgres-Trigger auf ApprovalEvent und PaymentOrder: UPDATE/DELETE serverseitig blockiert. Korrekturen ausschließlich über neue Audit-Events mit Referenz auf den vorherigen Eintrag.
- Hash-Chain-Verifikation (SHA-256 mit canonical Serialization) auf allen Approval- und Zahlungs-Aktionen als nächtlicher Hintergrund-Job. Bei Mismatch sofortige Alarmierung der Tenant-Administratoren über AI-Findings-Stream und E-Mail.
- Signierte Callback-States (JWT mit 30-min-Gültigkeit + Nonce-Replay-Schutz) für BANKSapi-Webform-Rückverkehr. Callback-Host-Allowlist im Code festgelegt.

### Sicherheits-Header

- 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

### Infrastruktur und Bereitstellung

- Containerisierung mit Docker Compose für isolierte Umgebungen
- Automatisierte CI/CD-Pipelines über GitHub Actions
- Nginx Reverse Proxy als Zugangsgateway

### Geplante Maßnahmen

- Rate Limiting zur DDoS- und Brute-Force-Prävention (Status: Umsetzung geplant)
- Content Security Policy (CSP) (Status: Umsetzung geplant)
- Datenbankebene Row Level Security (RLS) (Status: Evaluierung geplant)
- Automatische Schlüssel-Rotation (Status: Umsetzung geplant)

---

## § 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 (Claude API) für Reports, Briefings, Onboarding-Vorschläge und den allgemeinen AI-Partner-Chat (NICHT für den Cashflow-/Banking-AI-Layer — siehe OpenServ) | Aggregierte Geschäftsdaten, Beleg-Inhalte, ggf. Mitarbeiternamen bei Outliers |
| OpenServ Labs Ltd, 71–75 Shelton Street, Covent Garden, London WC2H 9JQ, Vereinigtes Königreich | Anbietersitz UK — Drittland mit Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO); Datenverarbeitung/Inferenz auf Servern in der EU/im EWR (`inference-api.openserv.ai`) | AI-Inferenz für den Cashflow-/Banking-AI-Layer (Phase A.2 W3): Anomalie-Erklärungen + AI-Cashflow-Tools. **Inferenz-Server hart auf EU/EWR gepinnt** (kein Failover in ein Drittland ohne Angemessenheitsbeschluss); Prompt-Logging beim Anbieter AUS | Aggregierte Cashflow-Kennzahlen + Beträge; **IBANs nie im Klartext (maskiert)**; **Gegenpartei-/Lieferantennamen pseudonymisiert** (LLM sieht „Lieferant A"); keine Cross-Tenant-Daten |
| Resend Inc. | USA | E-Mail-Versand (Benachrichtigungen, Eskalationen, Reports) | Empfänger-E-Mail-Adressen, HTML-E-Mail-Body |
| Google LLC | USA/EU | Cloud-Speicher (Google Sheets, Drive) | Lesezugriff, keine Banking- oder personenbezogenen Daten |
| GitHub Inc. (Microsoft) | USA | Code-Hosting, CI/CD | Keine Kundendaten |
| Hetzner Online GmbH | Deutschland (Falkenstein/Nürnberg) | Server-Hosting, Datenbank-Hosting, Backup-Storage | Alle verarbeiteten Daten |
| Stripe Payments Europe Ltd. | Republik Irland | Abonnement-Verwaltung der Kiosa-Lizenz, Trial-Status, Zahlungs-Methoden des Auftraggeber | KEINE Verarbeitung von Tenant-Banking- oder Tenant-Rechnungs-Daten |

8.2 **Änderungen der Unterauftragsverarbeiter:** Der Auftragsverarbeiter kann neue Unterauftragsverarbeiter nur hinzufügen, nachdem er den Auftraggeber mindestens 30 Tage im Voraus schriftlich benachrichtigt hat. Der Auftraggeber hat das Recht, der Hinzufügung eines neuen Unterauftragsverarbeiters innerhalb dieser Frist schriftlich zu widersprechen. Im Falle eines Widerspruchs wird der Auftragsverarbeiter mit dem Auftraggeber eine Lösungsmöglichkeit erörtern.

8.3 **Hinweis zu Datenquellen:** OktoPOS, gastromatic und Open-Meteo sind KEINE Unterauftragsverarbeiter, sondern Datenquellen des Auftraggeber, auf die der Auftragsverarbeiter lesend zugreift. Gleiches gilt für vom Auftraggeber bereitgestellte DATEV- oder Agenda-Buchungsstapel-Exports für die Auto-Kontierungs-Stammdaten.

8.4 **Hinweis zu BANKSapi:** Die BANKSapi Technology GmbH (München, Deutschland) ist KEIN Unterauftragsverarbeiter im Sinne dieses Vertrags. BANKSapi erbringt regulierte 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. Der Auftragsverarbeiter agiert als Schnittstellen-Vermittler zwischen Kiosa-Plattform und BANKSapi-API.

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

---

## § 9 Meldepflichten bei Datenpannen

9.1 Der Auftragsverarbeiter stellt dem Auftraggeber ohne unzumutbare Verzögerung, spätestens jedoch 48 Stunden nach Kenntnis, alle erforderlichen Informationen über eine Datenpanne (im Sinne von Artikel 33 DSGVO) zur Verfügung.

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 empfohlen 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 (Admin-User und Mitarbeiter) richten Anfragen zu ihren Rechten (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit) an den Auftraggeber als Verantwortlichen.

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 Auftraggeber)
- Daten löscht oder pseudonymisiert (auf Anweisung des Auftraggeber), wobei gesetzliche Aufbewahrungspflichten gemäß § 12 zu beachten sind
- Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellt (für Datenportabilität, über den Daten-Export-Endpoint)

---

## § 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 Der Auftragsverarbeiter löscht oder gibt alle personenbezogenen Daten des Auftraggeber neunzig (90) Tage nach Vertragsende an den Auftraggeber zurück, sofern kein sonstiger Grund für die weitere Aufbewahrung besteht.

12.2 Der Auftraggeber kann vor der Löschung eine Datenexportierung anfordern. Der Auftragsverarbeiter stellt die Daten dann in einem gängigen elektronischen Format (z. B. CSV oder JSON) 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 **Spezifische Aufbewahrungsfristen für Banking-Daten:** Beleg-Daten (PurchaseInvoice einschließlich der dazugehörigen Positionen und E-Invoice-Documents), Approval-Audit-Trails (ApprovalEvent mit Hash-Chain), Zahlungs-Aufträge (PaymentOrder, PayRun) und Bank-Buchungen werden gemäß § 257 HGB sowie § 147 AO für 10 Jahre nach Belegdatum aufbewahrt. Dies geht über die in § 12.1 genannte 90-Tage-Frist hinaus und ist gesetzlich zwingend (steuerrechtliche und handelsrechtliche Aufbewahrungspflicht in Deutschland, Österreich und der Schweiz). Nach Ablauf der 10-Jahres-Frist erfolgt automatische Löschung.

12.5 **Pseudonymisierungs-Strategie bei Mitarbeiter-Wechsel:** Bei Ausscheiden eines Mitarbeiters wird dessen User-Account auf Anweisung des Auftraggeber pseudonymisiert (beispielsweise wird die E-Mail-Adresse zu `deleted-user-{id}@removed.local` ersetzt, Vor- und Nachname zu „Gelöschter Mitarbeiter"). Audit-Trail-Einträge bleiben mit pseudonymisierter Referenz erhalten — GoBD-konform und DSGVO-konform gleichzeitig.

---

## § 13 Kontrollrechte

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

13.2 **Überprüfungen vor Ort:**

- Auf Anfrage des Auftraggeber führt der Auftragsverarbeiter Überprüfungen durch
- Die Überprüfung erfolgt auf Kosten des Auftraggeber (sofern mehrere Überprüfungen pro Jahr angefordert werden)

- Der Auftraggeber muss die Überprüfung mindestens 14 Werktage im Voraus ankündigen

13.3 **Audit-Bericht oder Zertifikat:** Alternativ kann der Auftraggeber einen Audit-Bericht oder ein Konformitätszertifikat (z. B. SOC 2, ISO 27001) anfordern.

---

## § 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 oder Ergänzungen dieses Vertrags müssen schriftlich erfolgen. Das Fehlen einer Schriftform macht diese Vereinbarungen ungültig.

14.4 **Dauer:** Dieser Vertrag tritt mit dem Beginn der Datenverarbeitung in Kraft und bleibt gültig, solange der Auftraggeber die Kiosa Plattform nutzt. Er wird automatisch mit der Beendigung des Nutzungsverhältnisses beendet.

---

## Anlage 1: Technische und organisatorische Maßnahmen (TOMs)

Die Anlage 1 detailliert die in § 7 beschriebenen technischen und organisatorischen Maßnahmen. Sie wird als separates Dokument gepflegt und dem Auftraggeber auf Anfrage zur Verfügung gestellt.

Die aktuelle TOM-Liste ist Bestandteil dieses Vertrags und wird bei wesentlichen Änderungen dem Auftraggeber mitgeteilt.

---

## Anlage 2: Unterauftragsverarbeiter (Sub-Processors)

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

| Unterauftragsverarbeiter | Ort | Verarbeitungstätigkeit |
|---|---|---|
| Anthropic PBC | USA | KI-gestützte Textgenerierung für Reports und Briefings, Anomalie-Erklärungen, Onboarding-Vorschläge |
| OpenServ Labs Ltd | Vereinigtes Königreich (Inferenz-Server EU/EWR; Angemessenheitsbeschluss Art. 45 DSGVO) | AI-Inferenz für den Cashflow-/Banking-AI-Layer: Anomalie-Erklärungen und AI-Cashflow-Tools; IBANs maskiert, Gegenpartei-Namen pseudonymisiert, keine Cross-Tenant-Daten |
| Resend Inc. | USA | Automatisierter E-Mail-Versand |
| Google LLC | USA/EU | Cloud-Datenspeicher (Google Sheets, Drive) |
| GitHub Inc. (Microsoft) | USA | Quellcode-Versionierung und CI/CD |

| Unterauftragsverarbeiter | Ort | Verarbeitungstätigkeit |
|---|---|---|
| Hetzner Online GmbH | Deutschland (Falkenstein/Nürnberg) | Infrastruktur und Datenhosting (Server, Datenbank, Storage mit verschlüsseltem Backup) |
| Stripe Payments Europe Ltd. | Republik Irland | Abonnement-Verwaltung der Kiosa-Lizenz (Trial-Status, Zahlungs-Methoden des Auftraggeber) |

**Keine Unterauftragsverarbeiter**, sondern Datenquellen oder eigenständige Dienstleister:

- OktoPOS, gastromatic, Open-Meteo (Datenquellen mit Lesezugriff)
- BANKSapi Technology GmbH (eigenständiger regulierter Zahlungsdienstleister mit eigenem PSU-Vertrag — siehe § 8.4)
- DATEV/Agenda (Steuerberater des Auftraggeber, eigene Rechtsbeziehung)

Diese Liste wird regelmäßig überprüft und aktualisiert. Der Auftraggeber wird über Änderungen benachrichtigt.

---

## Vertragsabschluss

Dieser Vertrag wird zwischen den Parteien elektronisch geschlossen. Der Auftraggeber erklärt die Annahme dieses Vertrags durch aktive Zustimmung im Onboarding-Prozess der Kiosa-Plattform (Click-Wrap-Verfahren). Das Akzept-Datum, die Vertragsversion und der Akzept-Hash werden im System des Auftragsverarbeiters dokumentiert und sind dem Auftraggeber auf Anfrage zugänglich.

Eine handschriftliche Unterschrift ist nicht erforderlich.

---

*Version 2.0 — Stand: Mai 2026 (Banking-Erweiterung). Vorgänger-Version 1.0 (März 2026). Erweiterungen gegenüber 1.0: §§ 2.6–2.10 (Banking-/Rechnungs-Verarbeitung), §§ 3.6–3.10 (Banking-Datenkategorien), § 4.3–4.4 (zusätzliche Betroffene-Kategorien), § 7 (Banking-spezifische TOMs), § 8 (Stripe + BANKSapi-Klarstellung), § 12.4–12.5 (10-Jahres-Aufbewahrung + Pseudonymisierung). Juli 2026: Unterauftragsverarbeiter OpenServ Labs Ltd (Cashflow-/Banking-AI-Layer) ergänzt; Klarstellung Anbietersitz UK / Inferenz-Server EU/EWR (Angemessenheitsbeschluss Art. 45 DSGVO).*