Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO für Shopvento

Fassung 1.1, gültig ab 7. November 2026

Anlage zu den Allgemeinen Geschäftsbedingungen für Shopvento ("AGB")

§ 1 Parteien, Abschluss

(1) Verantwortlicher (Art. 4 Nr. 7 DSGVO) ist der Kunde, der sich nach den AGB für Shopvento registriert hat, mit den bei der Registrierung angegebenen Daten ("Kunde").

(2) Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) ist die digital cuisine GmbH & Co. KG, Hanomagstraße 9, 30449 Hannover, eingetragen im Handelsregister des Amtsgerichts Hannover unter HRA 203017 ("digital cuisine").

(3) Dieser Vertrag wird bei der Registrierung durch eine gesonderte Checkbox in elektronischer Form angenommen (Art. 28 Abs. 9 DSGVO) und mit dem Hauptvertrag geschlossen. Die Annahme wird mit Zeitpunkt, handelnder Person, Kunde und Versionskennung protokolliert. digital cuisine hält die Fassung auf shopvento.de zum Abruf und Speichern bereit und versendet die angenommene Fassung als PDF mit der Bestätigungsmail. Für die aktive Bestätigung neuer Fassungen bei der nächsten Anmeldung im Backoffice gilt ergänzend § 25 AGB.

§ 2 Gegenstand, Rangverhältnis

(1) Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien aus dem Vertrag über die Nutzung der Plattform Shopvento nach den AGB ("Hauptvertrag").

(2) Für datenschutzrechtliche Fragen geht dieser Vertrag dem Hauptvertrag vor. Im Übrigen gilt der Hauptvertrag.

(3) Gegenstand, Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus Anlage A, auch für Zusatzmodule. Für ein Zusatzmodul gilt der jeweilige Abschnitt der Anlage A ab dessen Buchung.

(4) digital cuisine verarbeitet die Daten ausschließlich zur Erbringung der Leistungen nach dem Hauptvertrag und nicht für eigene Zwecke.

§ 3 Dauer

Dieser Vertrag gilt für die Laufzeit des Hauptvertrags und endet mit ihm; er ist nicht gesondert kündbar. Pflichten, die ihrer Natur nach über das Vertragsende hinauswirken, insbesondere nach §§ 9 und 10, bleiben bis zur vollständigen Löschung bestehen.

§ 4 Weisungen

(1) digital cuisine verarbeitet personenbezogene Daten nur nach dokumentierten Weisungen des Kunden. Der Hauptvertrag und die Einstellungen, die der Kunde in der Plattform vornimmt, bilden die vollständige Erstweisung.

(2) Weitere Weisungen erteilt der Kunde in Textform an die in Anlage B genannte Adresse. Weisungsberechtigt sind der Inhaber des Kundenkontos und Nutzer mit Administratorrechten. Mündliche Weisungen bei Dringlichkeit bestätigt der Kunde unverzüglich in Textform.

(3) Hält digital cuisine eine Weisung für datenschutzwidrig, informiert sie den Kunden unverzüglich und darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.

(4) Ist digital cuisine nach Unionsrecht oder dem Recht eines Mitgliedstaats zu einer weitergehenden Verarbeitung verpflichtet, teilt sie dies dem Kunden vorher mit, sofern das Recht die Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

(5) Sicherheitskritische Maßnahmen nach § 7 Abs. 3 AGB sind von der Erstweisung gedeckt.

(6) Weisungen, die über den Leistungsumfang des Hauptvertrags hinausgehen, kann digital cuisine ablehnen oder gegen Vergütung nach Aufwand gemäß Preisliste ausführen.

§ 5 Pflichten von digital cuisine

(1) digital cuisine verpflichtet alle zur Verarbeitung befugten Personen zur Vertraulichkeit, soweit sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Satz 2 lit. b DSGVO), auch über das Ende ihrer Tätigkeit hinaus.

(2) digital cuisine trifft die nach Art. 32 DSGVO erforderlichen Maßnahmen nach Anlage C. Sie darf sie durch gleichwertige oder bessere Maßnahmen ersetzen; das Schutzniveau darf nicht unterschritten werden.

(3) digital cuisine unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte betroffener Personen nach Kapitel III DSGVO und bei den Pflichten nach Art. 32 bis 36 DSGVO. Anträge betroffener Personen, die bei digital cuisine eingehen, leitet sie unverzüglich an den Kunden weiter. Unterstützung, die über die Funktionen der Plattform und die Bereitstellung vorhandener Informationen hinausgeht, wird nach Aufwand gemäß Preisliste vergütet, es sei denn, digital cuisine hat den Anlass zu vertreten.

(4) digital cuisine meldet dem Kunden jede Verletzung des Schutzes personenbezogener Daten unverzüglich, in der Regel innerhalb von 24 Stunden nach Kenntnis, in Textform an die E-Mail-Adresse des Kundenkontos. Die Meldung enthält, soweit verfügbar, die Angaben nach Art. 33 Abs. 3 DSGVO; fehlende Angaben werden nachgereicht. digital cuisine ergreift unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung nachteiliger Folgen. Meldungen an die Aufsichtsbehörde und Benachrichtigungen betroffener Personen obliegen dem Kunden.

(5) digital cuisine

- hat eine Datenschutzbeauftragte bestellt (Anlage B),
- führt ein Verzeichnis nach Art. 30 Abs. 2 DSGVO,

- informiert den Kunden unverzüglich über Maßnahmen einer Aufsichtsbehörde, die diese Verarbeitung betreffen, und über Gefährdungen der Daten durch Maßnahmen Dritter, insbesondere Pfändung, Beschlagnahme oder Insolvenzverfahren,
- erstellt Kopien der Daten nur, soweit dies für die Datensicherung nach § 9 AGB, die Bearbeitung von Supportanfragen oder gesetzliche Aufbewahrungspflichten erforderlich ist.

§ 6 Pflichten des Kunden

(1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Rechtsgrundlage und die Information seiner Gäste und Beschäftigten, etwa in der Datenschutzerklärung seiner Storefront.

(2) Der Kunde teilt digital cuisine unverzüglich mit, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt, und hält die Angaben in seinem Kundenkonto aktuell.

(3) Die Verarbeitung kann besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO umfassen, insbesondere krankheitsbedingte Abwesenheiten von Beschäftigten und Angaben zu Unverträglichkeiten von Gästen in Freitextfeldern (Anlage A). Der Kunde ist für die erforderliche Rechtsgrundlage nach Art. 6 und Art. 9 DSGVO sowie die Information der betroffenen Personen verantwortlich und beschränkt die Angaben auf das Erforderliche. Für Gesundheitsangaben von Gästen kommt in der Regel die ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO in Betracht, für Beschäftigtendaten Art. 9 Abs. 2 lit. b DSGVO in Verbindung mit § 26 Abs. 3 BDSG. Der Kunde berücksichtigt bei der Erfassung, dass Notizen zu privaten Veranstaltungen für alle seine Backoffice-Nutzer im jeweiligen Standortumfang lesbar sind (Anlage C). Eine Verarbeitung von Daten nach Art. 10 DSGVO ist nicht vorgesehen.

§ 7 Unterauftragsverarbeiter

(1) Der Kunde erteilt die allgemeine Genehmigung zum Einsatz weiterer Auftragsverarbeiter (Art. 28 Abs. 2 Satz 2 DSGVO). Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter ergeben sich aus Anlage D und gelten als genehmigt.

(2) digital cuisine informiert den Kunden über beabsichtigte Änderungen mindestens 30 Kalendertage vorab per E-Mail an die Adresse des Kundenkontos und in der Liste der Unterauftragsverarbeiter auf shopvento.de. Der Kunde kann binnen 14 Kalendertagen nach Zugang in Textform widersprechen; ohne Widerspruch gilt die Änderung als genehmigt.

(3) Bei Widerspruch suchen die Parteien eine einvernehmliche Lösung. Kommt sie nicht zustande, kann der Kunde den Hauptvertrag zum Zeitpunkt des Wirksamwerdens der Änderung kündigen.

(4) digital cuisine verpflichtet jeden Unterauftragsverarbeiter vertraglich auf gleichwertige Datenschutzpflichten (Art. 28 Abs. 4 DSGVO) und haftet für dessen Pflichterfüllung.

(5) Keine Unterauftragsverarbeitung sind

- Nebenleistungen Dritter ohne vorgesehenen Zugriff auf Daten des Kunden, etwa Telekommunikationsleistungen,
- Dienste, die der Kunde selbst beauftragt und an die Plattform anbinden lässt, insbesondere sein Stripe-Konto für Zahlungen seiner Gäste, ready2order, Google, DHL, sein eigenes WhatsApp-Konto und ein eigenes E-Mail-Versandkonto, das er anstelle des Versands von digital cuisine nutzt. Für diese Dienste ist der Kunde im Verhältnis zum jeweiligen Anbieter selbst verantwortlich. Er benötigt insbesondere ein

eigenes WhatsApp-Konto und ist für die Einhaltung der WhatsApp-Nutzungsbedingungen verantwortlich. Die Verarbeitung durch das von digital cuisine auf eigenen Servern betriebene WhatsApp-Gateway und die Speicherung der Nachrichten in der Plattformdatenbank sind dagegen Bestandteil dieser Auftragsverarbeitung und des Hostings nach Anlage D; WhatsApp/Meta bleibt der vom Kunden selbst beauftragte Anbieter.

§ 8 Ort der Verarbeitung

(1) Die Plattformdaten des Kunden (Datenbank, hochgeladene Dateien, Datensicherungen) werden bei Hetzner Online GmbH in Rechenzentren in Deutschland (Nürnberg/Falkenstein) gespeichert. Der Plattformserver und die Plattform-Datensicherung werden vor dem Go-live eingerichtet. Unberührt bleibt die Verarbeitung einzelner Daten durch die Unterauftragsverarbeiter nach Anlage D an den dort genannten Orten.

(2) Eine Verarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur durch die in Anlage D ausgewiesenen Unterauftragsverarbeiter und nur unter den Voraussetzungen der Art. 44 ff. DSGVO.

§ 9 Nachweise und Kontrollen

(1) digital cuisine stellt dem Kunden die Dokumentation nach Anlage C und die verfügbaren Informationen zum Nachweis ihrer Pflichten kostenlos zur Verfügung. Vorhandene Testate oder Berichte unabhängiger Stellen können ergänzend vorgelegt werden, soweit sie die betreffende Verarbeitung abdecken.

(2) Reichen diese Nachweise im Einzelfall nicht aus, kann der Kunde einmal je Kalenderjahr mit einer Ankündigungsfrist von 30 Kalendertagen während der Geschäftszeiten eine Prüfung selbst oder durch einen zur Verschwiegenheit verpflichteten Dritten durchführen, der nicht im Wettbewerb mit digital cuisine steht. Bei einer Verletzung des Schutzes personenbezogener Daten oder auf Anordnung einer Aufsichtsbehörde ist eine anlassbezogene Prüfung ohne diese Beschränkungen zulässig.

(3) Die Kosten eines vom Kunden beauftragten Prüfers trägt der Kunde. Nur bei einer Vor-Ort-Prüfung, die keine wesentlichen Mängel ergibt, vergütet der Kunde den erforderlichen und angemessenen Aufwand von digital cuisine nach der vereinbarten Preisliste. Die Kosten dürfen die Ausübung des Kontrollrechts nicht faktisch verhindern. Die Bereitstellung von Unterlagen und Informationen nach Abs. 1 bleibt kostenlos. Die Befugnisse der Aufsichtsbehörden (Art. 58 DSGVO) bleiben unberührt.

§ 10 Rückgabe und Löschung

(1) digital cuisine stellt dem Kunden zum Ende des Hauptvertrags einmal einen vollständigen Export seiner Daten einschließlich der zugehörigen Dateien und Metadaten in einem strukturierten, maschinenlesbaren Format bereit; dies ist mit dem vereinbarten Entgelt abgegolten. Auch während der Laufzeit stellt digital cuisine einen solchen Export auf Anforderung bereit. Der Kunde kann die Bereitstellung unter support@shopvento.de anfordern, auch bei gesperrtem Zugang, und die bereitgestellten Daten bis zur Löschung abrufen. Beim Anbieterwechsel gelten zusätzlich § 15 Abs. 3 bis 5 AGB und das Register unter https://shopvento.de/data-act (Veröffentlichung vor dem Go-live).

(2) digital cuisine löscht alle personenbezogenen Daten des Kunden drei Monate nach Ende des Hauptvertrags, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Beim Anbieterwechsel ist der Abrufzeitraum nach § 15 Abs. 5 AGB zu wahren; endet er später, wird nach seinem Ablauf gelöscht. Bei einer

ohne kostenpflichtiges Abonnement beendeten Testphase werden die aktiven Daten nach den Fristen des § 4 Abs. 3 AGB gelöscht und das Testarchiv 90 Kalendertage nach Testende. Sicherungskopien bleiben ausschließlich für Sicherungszwecke bis zum Auslaufen im regulären Sicherungszyklus nach § 9 Abs. 1 AGB erhalten und werden nicht anderweitig verwendet. Die Löschung wird auf Anforderung in Textform mit Datum bestätigt.

(3) Dokumentationen zum Nachweis der ordnungsgemäßen Verarbeitung darf digital cuisine entsprechend den gesetzlichen Aufbewahrungsfristen aufbewahren.

§ 11 Zurückbehaltungsrecht

Ein Zurückbehaltungsrecht an den personenbezogenen Daten des Kunden ist ausgeschlossen.

§ 12 Haftung

(1) Im Außenverhältnis gilt Art. 82 DSGVO. Im Innenverhältnis gilt ergänzend § 19 AGB, soweit Art. 82 DSGVO nicht entgegensteht.

(2) Die Parteien informieren einander unverzüglich über geltend gemachte Ansprüche betroffener Personen und über Verfahren der Aufsichtsbehörden zu dieser Verarbeitung und stimmen ihre Verteidigung ab.

§ 13 Schlussbestimmungen

(1) Änderungen dieses Vertrags richten sich nach § 25 AGB; Änderungen der Unterauftragsverarbeiter nach § 7.

(2) Ist eine Bestimmung unwirksam, bleibt die Wirksamkeit der übrigen unberührt; an ihre Stelle tritt die gesetzlich zulässige Regelung, die dem verfolgten Zweck am nächsten kommt.

(3) Recht und Gerichtsstand richten sich nach § 27 AGB.

Anlage A: Beschreibung der Verarbeitung

A.1 Allgemein

Angabe	Inhalt
Gegenstand	Bereitstellung und Betrieb der Plattform Shopvento als Software-as-a-Service nach dem Hauptvertrag
Art der Verarbeitung	Erheben über Storefront und Backoffice, Speichern, Ordnen, Auslesen, Verwenden, Versenden von Nachrichten an Gäste, Übermitteln an die vom Kunden angebundenen Dienste, Sichern, Wiederherstellen, Löschen
Zweck	Erbringung der Leistungen nach dem Hauptvertrag, insbesondere Reservierungen, Buchungen, Bestellungen, Gutscheine, Kommunikation mit Gästen, Verwaltung des Betriebs und Support

Angabe	Inhalt
Dauer	Laufzeit des Hauptvertrags zuzüglich der Fristen nach § 10
Besondere Kategorien (Art. 9 DSGVO)	Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) werden nicht gezielt abgefragt. Sie können verarbeitet werden, soweit der Auftraggeber sie erfasst, insbesondere Abwesenheitsgründe von Beschäftigten (z. B. Krankheit, Mutterschutz) sowie Angaben in Freitextfeldern (z. B. Unverträglichkeiten von Gästen). Es gilt § 6 Abs. 3.
Daten nach Art. 10 DSGVO	nein

A.2 Grundfunktionen (Storefront und Backoffice)

Kategorien betroffener Personen	Arten personenbezogener Daten
Gäste und Endkunden des Kunden (Reservierende, Besteller, Ticketkäufer, Teilnehmende, Schenkende und Empfangende von Gutscheinen)	Stamm- und Kontaktdaten (Name, E-Mail-Adresse, Telefonnummer, Rechnungs- und Lieferadresse); Reservierungs-, Buchungs- und Bestelldaten einschließlich Anmerkungen und Notizen zu privaten Veranstaltungen, gegebenenfalls mit Angaben zu Unverträglichkeiten; Gutscheine und Gutscheincodes; Stornierungen und Erstattungen; Kundenkonten; Inhalte von Nachrichten an Gäste; Zahlungs- und Transaktionsdaten ohne vollständige Karten- oder Kontodaten
Besucher der Storefront	Protokoll- und Verbindungsdaten (IP-Adresse, Zeitstempel, User-Agent); Signale von Cloudflare Turnstile zum Bot-Schutz bei Reservierung, Buchung, Checkout und Newsletter-Anmeldung
Beschäftigte und sonstige Nutzer des Kunden	Benutzerkonten, Rollen, Zugangsdaten, Protokoll- und Aktivitätsdaten

A.3 Module (nach gebuchtem Leistungsumfang)

Modul	Kategorien betroffener Personen	Arten personenbezogener Daten
Personalplanung und Zeiterfassung	Beschäftigte des Kunden	Name, Kontaktdaten, Rolle, Qualifikationen, Dienstpläne, Arbeits- und Pausenzeiten, Abwesenheiten einschließlich gesundheitsbezogener Abwesenheitsgründe (z. B. Krankheit, Mutterschutz)
Kassenanbindung ready2order	Gäste, Beschäftigte des Kunden	Verkaufs- und Belegdaten aus dem Kassensystem, soweit sie Personenbezug haben, etwa Namen von Bedienungen
WhatsApp	Gäste, Beschäftigte des Kunden	Telefonnummer, Profilname, Nachrichteninhalte, Zeitstempel, Sitzungsdaten des auf eigenen Servern betriebenen Gateways; Speicherung der Nachrichten in der Plattformdatenbank
Google Business	Gäste, Bewertende	Daten aus dem Google-Unternehmensprofil des Kunden, soweit die Anbindung sie abruft, etwa Bewertungen mit Namen

Modul	Kategorien betroffener Personen	Arten personenbezogener Daten
Warenwirtschaft	Ansprechpartner von Lieferanten	Name, Kontaktdaten, Bestell- und Lieferdaten
DHL-Versand	Empfangende von Sendungen	Name, Lieferadresse, E-Mail-Adresse und Telefonnummer, soweit an DHL übermittelt, Sendungsnummer und Sendungsstatus
B2B-Portal	Ansprechpartner von Geschäftskunden des Kunden	Name, Kontaktdaten, Firma, Rechnungs- und Lieferadressen, Bestelldaten, Zugangsdaten
Wissensdatenbank	Beschäftigte des Kunden, in Inhalten genannte Personen	Eingestellte Dokumente und Inhalte, Autor und Zeitpunkt; keine KI-Verarbeitung im Wissensdatenbank-Modul

Anlage B: Ansprechpartner

Rolle	Kunde	digital cuisine
Weisungen, Meldungen zu Sicherheitsvorfällen	Inhaber des Kundenkontos, erreichbar unter der E-Mail-Adresse des Kundenkontos; Änderungen pflegt der Kunde im Backoffice	Sascha-Matthias Kulawik, Geschäftsführer; Weisungen sowie Datenschutz- und Sicherheitsmeldungen an datenschutz@shopvento.de
Datenschutzbeauftragte	nach Angabe des Kunden	Carina Paulsen, datenschutz@shopvento.de

Anlage C: Technische und organisatorische Maßnahmen

Die Maßnahmen gelten für Shopvento. Stand 06.11.2026. Die Plattform ist noch nicht live; ein Plattform-Produktivserver besteht noch nicht. „Umgesetzt“ beschreibt den nachgewiesenen Produktstand, „Geplant vor Go-live“ die vorgesehene Betriebseinrichtung. Eine geplante Maßnahme wird damit nicht als bereits vorhanden zugesagt.

1. Organisation

- Umgesetzt: Plattformbetreiber nutzen eine gesonderte Betreiberkonsole mit TOTP-Authentifizierung für Mandantenstatus, Lizenzen und Testphasen. Die Konsole zeigt keine operativen Geschäftsdaten an.
- Vertragliche Vorgaben: Weisungen, Vertraulichkeit, Unterstützung und Meldungen richten sich nach §§ 4 und 5; die Ansprechpartner stehen in Anlage B. Die Pflichten der Unterauftragsverarbeiter ergeben sich aus § 7. Diese Verweise ersetzen keinen Nachweis einer technischen Umsetzung.

2. Vertraulichkeit

Zutritt zu Rechenzentren und Büros

- Geplant vor Go-live: Plattformserver, Datenbanken und Kundendateien bei Hetzner Online GmbH in Deutschland (Nürnberg/Falkenstein); verschlüsselte externe Sicherungen bei Hetzner Object Storage in Deutschland. Konkrete eigene Büro-Zutrittsmaßnahmen sind hier mangels Nachweises nicht

beschrieben.

Zugang zu Systemen

- Umgesetzt: Die Betreiberkonsole ist von den Kundenkonten getrennt und durch TOTP geschützt.
- Umgesetzt: Mandantenbezogene MCP-Zugriffe benötigen einen API-Schlüssel des jeweiligen Kunden. Administratoren und Manager können diese Schlüssel erstellen; ein fremder Mandantenschlüssel wird abgewiesen.

Zugriff auf Daten

- Umgesetzt: Der Kunde vergibt innerhalb der Plattform Benutzerrollen. Beschäftigte sehen nur die eigenen Abwesenheiten; gesundheitsbezogene Gründe anderer Beschäftigter und zugehörige Einzelheiten sind nur für Administratoren und Manager im berechtigten Standortumfang sichtbar. Manager eines fremden, lediglich gemeinsam genutzten Standorts sehen gesundheitsbezogene Abwesenheiten nur als „abwesend“, ohne Notiz oder Nachweis. Kalenderexporte zeigen sie als „Abwesend“; Gesundheitskategorien erlauben keine zusätzlichen Notizen.
- Umgesetzt: Notizen zu privaten Veranstaltungen sind für alle Backoffice-Rollen des Kunden im jeweils berechtigten Standortumfang lesbar, auch für Nutzer mit reinen Leserechten. Schreiben können Administratoren und Manager. Eine Beschränkung des Lesens auf Administratoren und Manager besteht hier nicht.
- Umgesetzt: Betreiberwerkzeuge für Sicherung und Wiederherstellung ermöglichen vollständigen Datenbankzugriff; diese Funktionen sind im Plattformbetrieb nicht über Kunden-HTTP- oder MCP-Routen verfügbar.

Trennung

- Umgesetzt: Jeder Kunde hat eine eigene PostgreSQL-Datenbank, getrennt von der Kontrolldatenbank; die Anwendungslaufzeit wird gemeinsam genutzt. Anfragen werden anhand des aufgerufenen Hosts dem Kunden zugeordnet und bei fehlender oder gesperrter Zuordnung abgewiesen. Die Laufzeit verwendet eine gemeinsame Datenbankrolle für die Kundendatenbanken.
- Umgesetzt: Jeder Kunde besitzt einen eigenen JWT-Signaturschlüssel und einen eigenen Schlüssel zum Schutz gespeicherter Geheimnisse. Diese Schlüssel sind in der Kontrollebene verschlüsselt gespeichert.
- Bestätigte Abgrenzung des Betriebs: Der Thomas-Krenn-CI-Host verarbeitet keine Produktivdaten. digital cuisine solutions S.L. in Jerez erhält keinen Zugriff auf Shopvento-Produktivdaten.

Verschlüsselung und Pseudonymisierung

- Umgesetzt: Anbieter-Zugangsdaten und Mandantenschlüssel werden mit Fernet verschlüsselt gespeichert. Geschäftsdaten, Veranstaltungsnotizen und Abwesenheiten sind nicht auf Feldebene verschlüsselt.
- Nicht umgesetzt: Verschlüsselung der Serverdatenträger oder Datenbanken im Ruhezustand. Eine Verschlüsselung des zugrunde liegenden Hetzner-Speichers ist nicht verifiziert und wird nicht zugesagt.
- Geplant vor Go-live: TLS am Cloudflare-Proxy und zum Ursprungsserver mit „Full (strict)“ und Origin-CA-Zertifikat. Eine TLS-Verschlüsselung zwischen Anwendung und PostgreSQL ist nicht nachgewiesen; sie wird nicht behauptet.
- Geplant vor Go-live: clientseitig mit restic verschlüsselte Sicherungen nach Abschnitt 4.

3. Integrität

Weitergabe

- Umgesetzt: Stripe-Aufrufe werden auf das jeweilige verbundene Kundenkonto begrenzt; Aufrufe ohne diese Zuordnung werden abgewiesen.
- Umgesetzt: Der Storefront-Zugriff über den Edge-Pfad benötigt einen gemeinsamen geheimen Header.
- Geplant vor Go-live: PostgreSQL und PgBouncer nur im internen Docker-Netz ohne öffentlichen Datenbankport. Zugriff auf den Ursprungsserver über Port 443 nur aus den Cloudflare-Netzen, kein öffentlicher Port 80.

Eingabe

- Umgesetzt: Rollen begrenzen Lese- und Schreibrechte nach Abschnitt 2. Eine lückenlose Protokollierung sämtlicher Eingaben, Änderungen und Löschungen ist durch die vorliegenden Fakten nicht belegt und wird nicht zugesagt.

4. Verfügbarkeit und Belastbarkeit

- Geplant vor Go-live: tägliche Sicherung um 02:00 Uhr aller Datenbanken des Plattformclusters einschließlich Kontrolldatenbank und Kundendatenbanken sowie der Kundendateien. Datenbankexport im PostgreSQL-Custom-Format mit zusätzlichen globalen Datenbankobjekten.
- Geplant vor Go-live: verschlüsselte externe Speicherung mit restic bei Hetzner Object Storage in Deutschland; Aufbewahrung von sieben täglichen, vier wöchentlichen, zwölf monatlichen und zwei jährlichen Sicherungsständen. Sicherungskopien laufen nach diesem Rotationszyklus aus.
- Geplant vor Go-live: Nachweis einer erfolgreichen Wiederherstellung vor öffentlicher Freigabe. Die tägliche Sicherung bedeutet im Störungsfall einen möglichen Datenverlust von bis zu 24 Stunden; eine zeitpunktgenaue Wiederherstellung ist nicht vorgesehen.
- Umgesetzt: mandantenbezogene Sicherung und Wiederherstellung durch Betreiber-CLI; keine Freigabe dieser Sicherungsrouten über Kunden-HTTP oder MCP im Plattformbetrieb.
- Umgesetzt im Produkt: serverseitige Prüfung von Turnstile bei Reservierungen, Veranstaltungsbuchungen, Checkout einschließlich Gutscheinen, Newsletter-Anmeldungen und Plattformregistrierung.
- Geplant vor Go-live: Cloudflare als Reverse Proxy und ein von digital cuisine betriebenes Turnstile-Widget für diese Storefront-Formulare und die Registrierung. Die zentrale Konfiguration der Schlüssel für Plattformkunden ist vor Freischaltung einzurichten; ein fehlender Schlüssel führt bei geschützten Buchungs- und Bestellfunktionen zur Ablehnung.

5. Überprüfung und Vorfälle

- Geplant vor Go-live: Prüfung des Sicherungs- und Wiederherstellungsablaufs anhand des Wiederherstellungsnachweises nach Abschnitt 4.
- Vertragliche Meldepflicht: digital cuisine informiert den Kunden nach § 5 Abs. 4 unverzüglich, in der Regel innerhalb von 24 Stunden nach Kenntnis einer Datenschutzverletzung. Meldungen des Kunden gehen an datenschutz@shopvento.de. Ein bereits eingerichteter umfassender Vorfallprozess wird damit nicht behauptet.

Anlage D: Unterauftragsverarbeiter

Unternehmen	Sitz, Verarbeitungsort	Leistung	Grundlage
Hetzner Online GmbH	Gunzenhausen, Deutschland; Rechenzentren Nürnberg/Falkenstein, Object Storage in Deutschland	Server- und Datenbankinfrastruktur, Dateien, Hosting des von digital cuisine selbst betriebenen WhatsApp-Gateways und verschlüsselte externe Datensicherung; Einrichtung für die Plattform vor Go-live geplant	Art. 28 Abs. 4 DSGVO, EU-intern
Cloudflare, Inc.	San Francisco, USA; weltweites Netz	Reverse Proxy, DDoS-Schutz und TLS-Terminierung für die Storefront; Turnstile für Reservierung, Buchung, Checkout und Newsletter-Anmeldung; Verarbeitung von Verbindungsdaten. Das gemeinsame Widget schützt auch die Registrierung, bei der digital cuisine selbst Verantwortlicher ist.	Art. 28 Abs. 4 DSGVO; bei Drittlandübermittlung Art. 45 DSGVO (EU-U.S. Data Privacy Framework), soweit anwendbar, andernfalls Standardvertragsklauseln
Brevo GmbH	Köpenicker Str. 126, 10179 Berlin, Deutschland; Verarbeitung nach den vereinbarten Datenschutzbedingungen	Transaktionsnachrichten an Gäste über das Brevo-Konto von digital cuisine, insbesondere Buchungsbestätigungen; Empfängeradresse, Nachrichteninhalt und Zustelldaten. Keine Newsletter über dieses Konto, kein Öffnungs- oder Klick-Tracking für Transaktionsmails; Abschaltung des Trackings im Konto vor Go-live vorgesehen. Eigene Systemmails an den Kunden versendet digital cuisine als Verantwortlicher.	Art. 28 Abs. 4 DSGVO; etwaige Drittlandübermittlungen nur nach Art. 44 ff. DSGVO
Microsoft (Microsoft 365)	Verarbeitungsorte nach den vereinbarten Microsoft-Datenschutzbedingungen; mögliche Drittlandverarbeitung, insbesondere USA	Support-Postfach und Bearbeitung von Support-E-Mails einschließlich darin enthaltener Kundendaten; keine Aussage über ein zusätzliches Ticketsystem	Art. 28 Abs. 4 DSGVO; bei Drittlandübermittlung EU-U.S. Data Privacy Framework, soweit anwendbar, andernfalls Standardvertragsklauseln
Anthropic (Claude)	USA	KI-gestützte Bearbeitung von Supportanfragen und Abfragen von Kundendaten über MCP durch digital cuisine; Verarbeitung der dafür übermittelten Anfragen und Daten. Keine KI-Verarbeitung innerhalb des Wissensdatenbank-Moduls.	Art. 28 Abs. 4 DSGVO; bei Drittlandübermittlung Standardvertragsklauseln beziehungsweise EU-U.S. Data Privacy Framework, soweit jeweils anwendbar

Die Liste beschreibt die für den Plattformbetrieb vorgesehenen Unterauftragsverarbeiter. Vor ihrem Zugriff auf Kundendaten müssen die Vereinbarungen nach § 7 Abs. 4 und die jeweils erforderlichen Übermittlungsgrundlagen vorliegen.

WhatsApp/Meta ist als vom Kunden selbst beauftragter Dienst nach § 7 Abs. 5 kein Unterauftragsverarbeiter von digital cuisine. Die eigene Gateway-Verarbeitung und Nachrichtenspeicherung sind von dieser AVV erfasst. Der Thomas-Krenn-CI-Host und digital cuisine solutions S.L. sind mangels Verarbeitung von Shopvento-Produktivdaten nicht in dieser Liste enthalten.