Auftragsverarbeitungsvertrag

Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO

Stand: Juni 2026

zwischen:

dem Kunden der gastro.digital-Plattform (nachfolgend „Verantwortlicher“ oder „Auftraggeber“)
– gemäß den Angaben im Rahmen der Registrierung bzw. des Hauptvertrages –

und:

mes.mo GmbH, Herdweg 16, D-73035 Göppingen
– Auftragsverarbeiter (Auftragsnehmer) –

Präambel

Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, insbesondere die Anforderungen nach Artikel 28 EU-Datenschutzgrundverordnung („DSGVO"). Er findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragsverarbeiters oder durch ihn beauftragte weitere Auftragsverarbeiter mit personenbezogenen Daten des Verantwortlichen in Berührung kommen können.

Dieser Vertrag gilt ausschließlich für die Datenverarbeitung im Rahmen der gastro.digital-Plattform (Reservierungssystem, Gutscheinshop, Ticketverkauf, Online-Bestellungen sowie zugehörige Dienste). Auftragsverarbeiter ist die mes.mo GmbH, handelnd unter der Marke gastro.digital.

§ 1 Gegenstand und Dauer des Auftrags

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten von Kunden, Gästen und anderen Personengruppen des Verantwortlichen ausschließlich im Auftrag und nach Weisung des Verantwortlichen.

(2) Der Vertrag beginnt mit der Unterschrift beider Parteien und ist unbefristet gültig. Der Auftraggeber kann den Vertrag jederzeit ohne Frist kündigen bei schwerem Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften, bei Weigerung zur Erfüllung einer Weisung oder bei vertragswidriger Verweigerung von Kontrollrechten.

(3) Für die Rechtmäßigkeit der Datenverarbeitung und der Datenweitergabe an den Auftragsverarbeiter ist der Verantwortliche zuständig.

(4) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Betroffenenrechten gemäß Kapitel III DSGVO. Die Durchführung erfolgt ausschließlich auf Weisung des Verantwortlichen.

§ 2 Umfang der Weisungsbefugnisse

(1) Der Auftragsverarbeiter verarbeitet Daten ausschließlich im Rahmen der vertraglichen Bestimmungen und der Weisungen des Verantwortlichen. Eine Verarbeitung zu eigenen Zwecken ist ausgeschlossen. Änderungen im Verfahrensablauf bedürfen der Textform (§ 126b BGB).

(2) Der Auftragsverarbeiter ist zur Durchführung aller für die Leistungserbringung erforderlichen Verarbeitungsschritte berechtigt (z. B. Duplizieren für Datensicherung, Anlegen von Log-Files).

(3) Ist der Auftragsverarbeiter der Ansicht, eine Weisung verstoße gegen die DSGVO oder andere Datenschutzvorschriften, hat er den Verantwortlichen unverzüglich darauf hinzuweisen.

§ 3 Art und Zweck der Verarbeitung, Datenkategorien, Betroffenenkreis

(1) Umfang: wiederkehrend

(2) Art der Verwendung: Erfassung, Speicherung, Übermittlung, Löschung/Vernichtung, Sperrung, Nutzung.

(3) Verarbeitungszwecke und zugehörige Datenkategorien:

Tischreservierung

- Zweck: Entgegennahme, Bestätigung und Verwaltung von Tischreservierungen
- Betroffene: Gäste des Verantwortlichen
- Datenkategorien: Name, E-Mail-Adresse, Telefonnummer, Datum/Uhrzeit/Personenzahl, besondere Wünsche, IP-Adresse, Reservierungshistorie, Gästeprofil

Gutscheinverkauf

- Zweck: Verkauf, Ausgabe und Einlösung von Wertgutscheinen
- Betroffene: Käufer und Empfänger von Gutscheinen
- Datenkategorien: Name, Rechnungsadresse, E-Mail-Adresse, Zahlungsdaten, Name des Gutscheinempfängers (optional), Gutscheinwert, Einlösestatus

Veranstaltungstickets

- Zweck: Verkauf und Verwaltung von Eintrittskarten für Veranstaltungen
- Betroffene: Ticketkäufer und Veranstaltungsteilnehmer
- Datenkategorien: Name, Kontaktdaten, Rechnungsdaten, Zahlungsdaten, Ticketnummer/QR-Code

Online-Bestellungen (Speisen & Getränke)

- Zweck: Entgegennahme und Abwicklung von Bestell- und Lieferaufträgen
- Betroffene: Besteller
- Datenkategorien: Name, Lieferadresse, E-Mail-Adresse, Telefonnummer, Bestellinhalt, Zahlungsdaten

Anzahlungen und Kreditkartengarantie

- Zweck: Absicherung von Reservierungen durch Anzahlung oder Kreditkartenhinterlegung
- Betroffene: Reservierende Gäste
- Datenkategorien: Name, Zahlungsdaten (Kreditkartenautorisierung über Stripe), Reservierungsdaten, Stornodaten

§ 4 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

(1) Der Auftragsverarbeiter gewährleistet die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme durch geeignete technische und organisatorische Maßnahmen gemäß der beigefügten TOM-Anlage.

(2) Der Auftragsverarbeiter verfügt über die erforderliche Herrschaft über die Datenverarbeitungsanlagen.

(3) Der Datenschutzkontakt des Auftragsverarbeiters informiert den Verantwortlichen unverzüglich bei wesentlichen Änderungen der technischen und organisatorischen Sicherheitsmaßnahmen.

Datenschutzkontakt des Auftragsverarbeiters: datenschutz@mesmo.de

§ 5 Unterauftragsverhältnisse (weitere Auftragsverarbeiter)

(1) Der Auftragsverarbeiter ist berechtigt, zur Erfüllung seiner vertraglichen Leistungen weitere Auftragsverarbeiter gemäß Art. 28 DSGVO einzusetzen.

(2) Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung zum Einsatz weiterer Unterauftragsverarbeiter.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Kalendertage vor dem geplanten Einsatz eines neuen Unterauftragsverarbeiters in Textform.

(4) Der Verantwortliche ist berechtigt, dem Einsatz eines neuen Unterauftragsverarbeiters innerhalb von 30 Kalendertagen aus wichtigem datenschutzrechtlichem Grund zu widersprechen.

(5) Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Zustimmung als erteilt.

(6) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die mindestens den Anforderungen dieses Vertrages entsprechen.

(7) Eine aktuelle Liste der eingesetzten Unterauftragsverarbeiter ist Bestandteil dieses Vertrages (Anlage 2) und wird vom Auftragsverarbeiter gepflegt.

§ 6 Mandantenfähigkeit

Der Auftragsverarbeiter stellt sicher, dass Daten verschiedener Auftraggeber physisch oder logisch getrennt verarbeitet werden und keine gegenseitige Einsichtnahme möglich ist.

§ 7 Einsatz von Cloud- und KI-Diensten

(1) Der Auftragsverarbeiter ist berechtigt, Cloud- und Plattformdienste zur Erbringung seiner Leistungen einzusetzen.

(2) KI-Dienste (insbesondere OpenAI und Anthropic) werden vom Auftragsverarbeiter primär für interne betriebliche Zwecke eingesetzt, beispielsweise zur Unterstützung interner Arbeitsprozesse und technischer Datenpflegemaßnahmen wie dem Import und der Anpassung von Reservierungsdaten. Eine dauerhafte oder systematische Verarbeitung von Gästedaten des Verantwortlichen durch KI-Dienste findet nicht statt.

(3) Soweit im Rahmen technischer Datenpflegeprozesse ausnahmsweise personenbezogene Daten des Verantwortlichen verarbeitet werden, erfolgt dies ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen und nicht zu Analyse-, Marketing-, Benchmarking- oder Trainingszwecken.

(4) Personenbezogene Daten des Verantwortlichen werden nicht zum Training allgemeiner KI-Modelle verwendet.

(5) Der Auftragsverarbeiter stellt sicher, dass eingesetzte KI- und Cloud-Dienstleister den Anforderungen der DSGVO entsprechen und geeignete Garantien gemäß Kapitel V DSGVO vorliegen, soweit eine Drittlandübermittlung erfolgt.

(6) Der Auftragsverarbeiter informiert den Verantwortlichen auf Anfrage über die im Rahmen der Leistungserbringung eingesetzten KI-Dienste.

§ 8 Datengeheimnis

(1) Der Auftragsverarbeiter stellt sicher, dass alle mit der Verarbeitung befassten Personen zur Vertraulichkeit verpflichtet sind und Daten ausschließlich auf Weisung verarbeiten.

(2) Auskünfte über Daten des Verantwortlichen dürfen nur mit dessen vorheriger schriftlicher Zustimmung erteilt werden.

(3) Mitarbeiter werden regelmäßig in den anwendbaren Datenschutzvorschriften geschult.

§ 9 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO und erstellt selbst ein Verzeichnis nach Art. 30 Abs. 2 DSGVO.

(2) Die Verarbeitung erfolgt in der Europäischen Union, dem Europäischen Wirtschaftsraum oder auf Grundlage geeigneter Garantien gemäß Kapitel V DSGVO, insbesondere Angemessenheitsbeschlüssen der Europäischen Kommission oder Standardvertragsklauseln. Jede Verarbeitung außerhalb dieser Grundlagen bedarf vorheriger Zustimmung des Verantwortlichen in Textform.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten gemäß Art. 32–36 DSGVO.

§ 10 Rechte der betroffenen Personen

Werden Betroffenenrechte beim Auftragsverarbeiter geltend gemacht, leitet dieser die Anfrage unverzüglich an den Verantwortlichen weiter. Die Wahrung der Betroffenenrechte liegt beim Verantwortlichen. Der Auftragsverarbeiter unterstützt gemäß § 1 Abs. 4 dieses Vertrags.

§ 11 Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter räumt dem Verantwortlichen alle erforderlichen Auskunfts-, Einsichts- und Kontrollrechte gemäß Art. 28 Abs. 3h DSGVO ein. Ordentliche Betriebsprüfungen sind maximal einmal alle 24 Monate nach vorheriger Anmeldung in Textform möglich; der Auftragsverarbeiter ermöglicht den Beginn innerhalb von 3 Kalenderwochen. Anlassbezogene Prüfungen bei konkretem Verdacht eines Datenschutzverstoßes oder auf behördliche Anforderung hin sind jederzeit ohne Einhaltung der Mindestfrist möglich.

(2) Der Auftragsverarbeiter erteilt auf Anforderung in Textform innerhalb angemessener Frist alle für die Prüfung erforderlichen Auskünfte.

(3) Als Nachweis kann der Auftragsverarbeiter Testate, Berichte unabhängiger Instanzen oder Zertifizierungen gemäß Art. 42 DSGVO vorlegen. Der Verantwortliche akzeptiert solche Nachweise als gleichwertig zu einer Vor-Ort-Prüfung, sofern sie die relevanten Verarbeitungstätigkeiten abdecken.

(4) Vor-Ort-Prüfungen, die über die in Abs. 1 genannte Häufigkeit hinausgehen oder einen Aufwand von mehr als einem Arbeitstag verursachen, werden dem Verantwortlichen zu den tatsächlich anfallenden Kosten des Auftragsverarbeiters in Rechnung gestellt, es sei denn, die Prüfung ist durch einen konkreten Verdacht eines Datenschutzverstoßes des Auftragsverarbeiters veranlasst. Der Auftragsverarbeiter weist den voraussichtlichen Aufwand vor Beginn der Prüfung in Textform aus.

§ 12 Informationspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Bekanntwerden eines Datenschutzvorfalls, bei Datenschutzverletzungen, Unregelmäßigkeiten bei der Verarbeitung oder Verstößen gegen diesen Vertrag, soweit die erforderlichen Informationen zu diesem Zeitpunkt vorliegen.

(2) Vorfälle gemäß Art. 33 Abs. 2 DSGVO werden unverzüglich mitgeteilt, unabhängig von der Verursachung.

(3) Gefährdungen der Daten durch Pfändung, Insolvenz oder Maßnahmen Dritter werden dem Verantwortlichen unverzüglich gemeldet.

§ 13 Berichtigung, Löschung und Rückgabe von Daten

(1) Nach Beendigung des Auftrags werden Daten und Unterlagen nach Wahl des Verantwortlichen gelöscht, zurückgegeben oder vernichtet, sofern keine gesetzlichen Aufbewahrungspflichten bestehen.

(2) Berichtigung, Löschung oder Einschränkung erfolgen ausschließlich auf Weisung des Verantwortlichen und werden protokolliert.

(3) Die physische Vernichtung erfolgt mindestens nach DIN 66399 Sicherheitsstufe 3.

§ 14 Haftung

(1) Der Auftragsverarbeiter haftet dem Verantwortlichen für Schäden durch unzulässige oder unrichtige Verarbeitung personenbezogener Daten im Rahmen des Auftragsverhältnisses, insbesondere bei Abweichung von Weisungen.

(2) Die Haftung des Auftragsverarbeiters ist der Höhe nach begrenzt auf den sechsfachen monatlichen Nettovergütungsbetrag, den der Verantwortliche im Monat vor dem schadensbegründenden Ereignis an den Auftragsverarbeiter entrichtet hat. Die Begrenzung gilt je Schadensfall und Kalenderjahr.

(3) Die Haftungsbegrenzung gilt nicht bei Vorsatz oder grober Fahrlässigkeit, bei Verletzung von Leben, Körper oder Gesundheit sowie bei zwingenden gesetzlichen Haftungstatbeständen.

(4) Eine Haftung für mittelbare Schäden, entgangenen Gewinn oder Folgeschäden ist – soweit gesetzlich zulässig – ausgeschlossen.

(5) Im Übrigen gelten die gesetzlichen Haftungsbestimmungen.

§ 15 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform (§ 126b BGB). Die Textform gilt auch für Weisungen, Anmeldungen zu Prüfungen und sonstige Erklärungen im Rahmen dieses Vertrags.

(2) Es gilt das Recht der Bundesrepublik Deutschland.

(3) Dokumentationen zur ordnungsgemäßen Datenverarbeitung sind über das Vertragsende hinaus aufzubewahren. Die Vertragsparteien wahren auch nach Vertragsende unbegrenzt Stillschweigen über bekannt gewordene Daten und Sachverhalte.

§ 16 Wirksamkeit und Abschluss

Hinweis: Eine handschriftliche Unterzeichnung ist nur erforderlich, sofern keine digitale Zustimmung gemäß den nachfolgenden Absätzen erfolgt ist. Im Regelfall wird dieser Vertrag durch die digitale Registrierung oder Zustimmung auf kunden.gastro.digital wirksam.

Diese Vereinbarung wird wirksam durch:

- handschriftliche Unterzeichnung beider Vertragsparteien, oder
- digitale Zustimmung im Rahmen des Online-Registrierungsprozesses auf kunden.gastro.digital, oder
- ausdrückliche Einbeziehung in den zwischen den Parteien geschlossenen Hauptvertrag.

Die elektronische Form gemäß Art. 28 Abs. 9 DSGVO ist ausdrücklich zugelassen.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
für den Verantwortlichen (Auftraggeber):	für den Auftragsverarbeiter: Jens Walburg, Geschäftsführer mes.mo GmbH

Anlage 1 – Technisch-organisatorische Maßnahmen (Art. 32 DSGVO)

1. Zugangs- und Zugriffskontrolle

– Zugang zu kritischen Systemen nur für autorisierte Personen; rollenbasierte Berechtigungen nach dem Least-Privilege-Prinzip
– Starke Passwortrichtlinien (Mindestlänge, Komplexität); keine erzwungenen regelmäßigen Passwortänderungen bei Einsatz starker Passwörter
– Mehr-Faktor-Authentifizierung (MFA) für zentrale Administrationskonten externer Plattformdienste (AWS, Cloudflare, Stripe, Mailgun) ist aktiv, soweit verfügbar
– Für die gastro.digital-Anwendung wird MFA schrittweise eingeführt
– Protokollierung aller Zugriffe auf produktionsrelevante Systeme und personenbezogene Daten
– Regelmäßige Überprüfung und Entzug nicht mehr benötigter Zugriffsrechte

2. Verschlüsselung und Übertragungssicherheit

– Verschlüsselung der Datenübertragung via SSL/TLS (HTTPS)
– Verschlüsselung gespeicherter personenbezogener Daten auf Servern und Datenträgern (Encryption at Rest, AWS RDS)
– Pseudonymisierung wo technisch sinnvoll und möglich

3. Verfügbarkeit, Backup und Wiederherstellung

– Redundante Serverstrukturen (AWS Multi-AZ, eu-central-1)
– Automatisierte tägliche Datensicherungen mit definierten Backup-Retentionszeiträumen
– Regelmäßige Restore-Tests zur Überprüfung der Wiederherstellbarkeit
– Monitoring und automatisierte Alarmierung bei Systemausfällen (Sentry)
– Firewall und DDoS-Schutz über Cloudflare

4. Patch- und Schwachstellenmanagement

– Zeitnahe Installation sicherheitsrelevanter Software- und Systemupdates (Patch-Management)
– Regelmäßige Überprüfung eingesetzter Abhängigkeiten und Bibliotheken auf bekannte Schwachstellen
– Strukturierter Prozess zur Bewertung und Priorisierung sicherheitsrelevanter Updates

5. Zugriff auf Produktionsdaten

– Zugriff auf Produktionsdatenbanken nur für einen eingeschränkten Kreis autorisierter Entwickler
– Direktzugriffe auf Produktionsdaten werden protokolliert
– Verarbeitung von Echtdaten zu Testzwecken wird vermieden; wo möglich werden anonymisierte oder synthetische Daten verwendet

6. Incident-Management

– Definierter interner Prozess zur Erkennung, Meldung und Bearbeitung von Datenschutzvorfällen
– Benachrichtigung des Verantwortlichen unverzüglich, spätestens innerhalb von 48 Stunden nach Bekanntwerden eines meldepflichtigen Vorfalls (siehe § 12)
– Dokumentation aller Sicherheitsvorfälle und ergriffener Maßnahmen

7. Regelmäßige Überprüfung

– Regelmäßige interne Überprüfung der technischen und organisatorischen Maßnahmen
– Datenschutzkontakt: datenschutz@mesmo.de (Björn Walburg)
– Schulung der Mitarbeiter zu Datenschutz und Informationssicherheit

Anlage 2 – Liste der genehmigten Subunternehmer (Stand: Juni 2026)

Unternehmen	Zweck	Verarbeitungsort
1. Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxemburg	Hosting, Datenbanken, Speicher, Netzwerk- und Cloud-Infrastruktur	Europäische Union
2. Cloudflare, Inc. 101 Townsend St San Francisco, CA 94107, USA	DNS, CDN, DDoS-Schutz, Web Application Firewall, Performance-Optimierung	EU und USA EU-US DPF (aktiv zertifiziert) + SCCs als Fallback
3. Sentry, Inc. 45 Fremont Street, 8th Floor San Francisco, CA 94105, USA	Fehleranalyse, Monitoring, Performance-Analyse	EU und USA EU-US DPF (aktiv zertifiziert) + SCCs als Fallback
4. Mailgun Technologies, Inc. 112 E Pecan St #1135 San Antonio, TX 78205, USA	Versand transaktionaler E-Mails	EU und USA EU-Standardvertragsklauseln (SCCs)
5. Stripe Payments Europe Ltd. 1 Grand Canal Street Lower Dublin, Irland	Zahlungsabwicklung (Kreditkarte, Kreditkartenautorisierung/Setup Intent) Nur bei Partnern mit aktivierter Zahlungsfunktion	Europäische Union
6. PayPal (Europe) S.à r.l. et Cie, S.C.A. 22-24 Boulevard Royal L-2449 Luxemburg	PayPal-Zahlungsabwicklung Nur bei Partnern mit aktivierter Zahlungsfunktion	EU und USA (SCCs)
7. OpenAI, LLC 3180 18th Street San Francisco, CA 94110, USA	Interne betriebliche Prozesse und technische Datenpflege (z. B. Import/Anpassung von Reservierungsdaten). Keine dauerhafte oder systematische Verarbeitung von Gästedaten. Keine Nutzung zu Trainings-, Analyse- oder Marketingzwecken.	USA EU-US DPF (aktiv zertifiziert) + SCCs als Fallback
8. Anthropic, PBC 548 Market St, PMB 90375 San Francisco, CA 94104, USA	Interne betriebliche Prozesse und technische Datenpflege (z. B. Import/Anpassung von Reservierungsdaten). Keine dauerhafte oder systematische Verarbeitung von Gästedaten. Keine Nutzung zu Trainings-, Analyse- oder Marketingzwecken.	USA EU-US DPF (aktiv zertifiziert) + SCCs als Fallback

Allgemeiner Hinweis: Subunternehmer unter den Ziffern 5 und 6 werden ausschließlich für Partner mit aktivierter Zahlungsfunktion eingesetzt. Subunternehmer unter den Ziffern 7 und 8 werden ausschließlich für interne betriebliche Prozesse, technische Datenpflege sowie – sofern vertraglich aktiviert – für KI-gestützte Funktionen eingesetzt. Eine dauerhafte oder systematische Verarbeitung von Gästedaten findet nicht statt.