Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO — Stand: 8. August 2026

VERSION	GÜLTIG AB	STAND	FREIGEGEBEN VON
2026-08-10	10.08.2026	10.08.2026	

> *Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV“) wird mit Abschluss des Hauptvertrags über die Nutzung der dyshi-Plattform (gemäß AGB) zwischen dem Kunden (nachfolgend „Verantwortlicher“) und dem Anbieter (nachfolgend „Auftragsverarbeiter“) verbindlich vereinbart, soweit der Auftragsverarbeiter im Rahmen der Leistungserbringung personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.*

§ 1 Gegenstand und Dauer der Verarbeitung

Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Erbringung der im Hauptvertrag vereinbarten Leistungen (Betrieb des Speisekarten-CMS und der zugehörigen Veröffentlichungs- und Bewertungsinfrastruktur).

Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags.

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung personenbezogener Daten umfasst insbesondere folgende Tätigkeiten:

- Erfassen, Speichern und Anzeigen von Daten, die der Verantwortliche im CMS hinterlegt;
- Erfassen und Speichern von Nutzungsdaten der Gäste des Verantwortlichen, die die veröffentlichten Speisekarten aufrufen;
- Erfassen, Speichern und Anzeigen von Bewertungen, Reviews und sonstigen nutzergenerierten Inhalten;
- Versand transaktionaler E-Mails an Mitarbeiter und Gäste des Verantwortlichen;
- Bereitstellung der Plattform und damit verbundener Funktionen.
- KI-gestützte Verarbeitung hochgeladener Speisekarten und Bilder auf dokumentierte Veranlassung des Verantwortlichen.

Zweck der Verarbeitung ist die Erbringung der vertraglichen Leistungen gegenüber dem Verantwortlichen.

§ 3 Art der personenbezogenen Daten

Gegenstand der Verarbeitung sind insbesondere folgende Datenkategorien:

- Stammdaten der Mitarbeiter des Verantwortlichen (Name, E-Mail-Adresse, Rolle innerhalb der Organisation);
- Stammdaten von Gästen des Verantwortlichen, soweit diese sich auf der Plattform registrieren (Name, E-Mail-Adresse, optionales Profilbild);

- Inhaltsdaten (Bewertungen, Kommentare, Bilder), die vom Verantwortlichen oder von Gästen eingestellt werden;
- Nutzungs- und Protokolldaten (IP-Adresse, User-Agent, Zeitstempel, Geräteinformationen), soweit zur Bereitstellung der Plattform erforderlich;
- Kommunikationsdaten im Rahmen transaktionaler E-Mails (z. B. Bestätigungs- und Passwort-Reset-Mails).
- Bild-, Dokument- und extrahierte Inhaltsdaten im Rahmen des Menü-Scans und der KI-gestützten Bildoptimierung.

§ 4 Kreis der betroffenen Personen

- Mitarbeiter und Beauftragte des Verantwortlichen mit Zugang zum CMS;
- Gäste und Besucher der vom Verantwortlichen veröffentlichten Speisekarten-Seiten;
- registrierte Endnutzer der Plattform, die Inhalte zu den Restaurants des Verantwortlichen einstellen.

§ 5 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich,

- personenbezogene Daten ausschließlich im Rahmen der dokumentierten Weisungen des Verantwortlichen zu verarbeiten, sofern er nicht durch das Unionsrecht oder das Recht eines Mitgliedstaates, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist;
- sicherzustellen, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- die erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO zu ergreifen (siehe Anlage 1);
- den Verantwortlichen unverzüglich zu informieren, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt;
- den Verantwortlichen bei der Erfüllung von Pflichten aus Art. 32 bis 36 DSGVO sowie bei der Beantwortung von Anträgen betroffener Personen (Art. 12 ff. DSGVO) zu unterstützen, soweit dies erforderlich und möglich ist;
- dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung zu stellen und Überprüfungen gemäß § 8 zu ermöglichen;
- eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntniserlangung, an den Verantwortlichen zu melden.

§ 6 Pflichten des Verantwortlichen

Der Verantwortliche

- ist im Rahmen seiner Verantwortlichkeit nach der DSGVO allein für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich;
- erteilt sämtliche Weisungen in Textform; mündliche Weisungen sind unverzüglich in Textform zu bestätigen;
- informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt;

- benennt einen Ansprechpartner für datenschutzbezogene Fragen.

§ 7 Unterauftragsverarbeiter

Der Verantwortliche erteilt dem Auftragsverarbeiter mit Abschluss dieses AVV eine allgemeine schriftliche Genehmigung zur Hinzuziehung von Unterauftragsverarbeitern. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 2 aufgeführt.

Der Auftragsverarbeiter wird den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragsverarbeiter mit einer Vorlaufzeit von mindestens 30 Tagen in Textform informieren. Der Verantwortliche kann der Änderung innerhalb dieser Frist aus wichtigem Grund widersprechen. Im Falle eines berechtigten Widerspruchs steht dem Auftragsverarbeiter ein Sonderkündigungsrecht in Bezug auf den Hauptvertrag zu, soweit eine Leistungserbringung ohne den betreffenden Unterauftragsverarbeiter nicht zumutbar ist.

Der Auftragsverarbeiter verpflichtet die Unterauftragsverarbeiter vertraglich auf die in diesem AVV niedergelegten Pflichten, soweit diese auf die jeweilige Verarbeitung anwendbar sind.

§ 8 Kontrollrechte des Verantwortlichen

Der Verantwortliche ist berechtigt, sich von der Einhaltung der vertraglichen und gesetzlichen Pflichten durch den Auftragsverarbeiter zu überzeugen. Der Auftragsverarbeiter stellt hierfür auf Anfrage geeignete Nachweise zur Verfügung, insbesondere

- aktuelle Testate, Audits oder Zertifizierungen anerkannter Prüfstellen;
- die Dokumentation der technischen und organisatorischen Maßnahmen nach Anlage 1;
- auf Verlangen eine schriftliche Selbstauskunft.

Sofern im Einzelfall Vor-Ort-Kontrollen erforderlich sind, sind diese mit einer angemessenen Vorlaufzeit von mindestens vier Wochen anzukündigen und so durchzuführen, dass der Betriebsablauf des Auftragsverarbeiters nicht über das erforderliche Maß hinaus gestört wird. Mehr als eine Kontrolle pro Kalenderjahr ist nur bei konkreten Anhaltspunkten für einen Verstoß, nach einer Datenschutzverletzung oder auf Anordnung einer Aufsichtsbehörde zulässig. Gesetzlich erforderliche Nachweise und eine angemessene Erstprüfung sind mit der vereinbarten Vergütung abgegolten. Nur darüber hinausgehenden, nachweisbaren und angemessenen Aufwand einer vom Verantwortlichen veranlassten Kontrolle darf der Auftragsverarbeiter berechnen, sofern die Kontrolle keinen Verstoß ergibt.

§ 9 Löschung und Rückgabe nach Beendigung

Nach Beendigung des Hauptvertrags wird der Auftragsverarbeiter die im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Verantwortlichen zurückgeben oder löschen, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Personenbezogene Daten, die aufgrund gesetzlicher Aufbewahrungspflichten weiter gespeichert werden, werden für die Dauer der Aufbewahrungspflicht gesperrt und ausschließlich zu diesem Zweck weiterverarbeitet.

Im Übrigen gilt § 10 der AGB (Anbieterwechsel, Datenexport und Löschung) entsprechend.

§ 10 Haftung

Für die Haftung gelten die Regelungen des Hauptvertrags sowie Art. 82 DSGVO. Im Innenverhältnis haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen nur, soweit er die ihm nach diesem AVV oder nach der DSGVO obliegenden Pflichten verletzt hat.

§ 11 Schlussbestimmungen

Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV vor, soweit es um die Verarbeitung personenbezogener Daten geht.

Änderungen und Ergänzungen dieses AVV bedürfen der Textform. Es gilt das Recht der Bundesrepublik Deutschland.

Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anlage 1 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Der Auftragsverarbeiter trifft die folgenden technischen und organisatorischen Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus:

Vertraulichkeit

- Zutrittskontrolle: Hosting in Rechenzentren mit dokumentierter Zutrittsregelung (siehe Anlage 2 für die eingesetzten Anbieter);
- Zugangskontrolle: Authentifizierung über E-Mail und Passwort, Speicherung von Passwörtern ausschließlich als gesalzener kryptografischer Hash sowie Begrenzung von Anmeldeversuchen;
- Zugriffskontrolle: rollenbasiertes Berechtigungskonzept (Organization- und Admin-Plugin von Better Auth), Trennung der Mandanten auf Datenbankebene;
- Trennungskontrolle: logische Trennung der Daten unterschiedlicher Verantwortlicher durch Mandantenkennungen.

Integrität

- Weitergabekontrolle: Verschlüsselung der Übertragung mittels TLS (HTTPS);
- Eingabekontrolle: Protokollierung sicherheitsrelevanter Aktionen (Audit-Logs).

Verfügbarkeit und Belastbarkeit

- regelmäßige automatisierte Backups der Datenbank;
- Monitoring der Systeme auf Verfügbarkeit und Sicherheitsereignisse;
- Schutz vor Verlust durch Redundanz auf Speicherebene.

Verfahren zur regelmäßigen Überprüfung

- regelmäßige Aktualisierung eingesetzter Software-Komponenten;
- Datenschutz-Management durch den Auftragsverarbeiter, einschließlich eines dokumentierten Verfahrens zur Reaktion auf Datenschutzvorfälle.

Der Auftragsverarbeiter überprüft die Angemessenheit dieser Maßnahmen regelmäßig und nach wesentlichen Änderungen der Verarbeitung. Wesentliche nachteilige Änderungen werden dem Verantwortlichen vorab mitgeteilt.

Anlage 2 — Liste der Unterauftragsverarbeiter

Zum Zeitpunkt des Vertragsschlusses werden folgende Unterauftragsverarbeiter eingesetzt:

Anbieter	**Zweck**	**Sitz / Datenstandort**
Lettermint B.V.	Versand transaktionaler E-Mails	Niederlande (EU)
Cloudflare, Inc.	CDN, DDoS-Schutz, Objektspeicher (R2) für Bilder	EU/USA (EU-US Data Privacy Framework und Standardvertragsklauseln)
Hetzner Online GmbH	Server-Hosting, Datenbankbetrieb	Deutschland (EU)
Google Ireland Limited / Google LLC	KI-gestützter Menü-Scan und Bildverarbeitung (Gemini API und Vertex AI)	EU/USA (EU-US Data Privacy Framework und Standardvertragsklauseln)
OpenRouter, Inc.	Vermittlung der KI-gestützten Verarbeitung (Menü-Scan und Bildverarbeitung), wenn der primäre KI-Dienstleister nicht verfügbar oder überlastet ist	USA (Standardvertragsklauseln)

> *Stripe verarbeitet Zahlungs- und Abrechnungsdaten für den Anbieter und ist nicht als Unterauftragsverarbeiter für die vom Kunden verantworteten Restaurant- und Gästedaten in dieser Liste aufgeführt. Einzelheiten enthält die Datenschutzerklärung.*