mouza

Fassung 1.0 · Stand 16. November 2026

Vertrag zur Auftragsverarbeitung

Vertragsparteien

Dieser Vertrag wird geschlossen zwischen dem Kunden, der diesem Vertrag online zustimmt (Verantwortlicher, im Folgenden „Auftraggeber“), und Mouza Studio, Inhaber Moufid Zahed, Schützenstraße 27, 67061 Ludwigshafen am Rhein, E-Mail info@mouza.studio (Auftragsverarbeiter, im Folgenden „Auftragnehmer“).

Name und Anschrift des Auftraggebers und das zugehörige Angebot stehen in der Vertragsübersicht, die zusammen mit diesem Vertrag angezeigt wird.

§ 1 Gegenstand, Abschluss und Dauer

(1) Der Auftragnehmer erstellt und betreibt für den Auftraggeber eine Website mit Online-Buchung bzw. Automatisierungen (Hauptvertrag: Projektvertrag laut Angebot und Wartungs- bzw. Hostingvertrag). Dabei verarbeitet er personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag regelt die Rechte und Pflichten der Parteien dabei nach Art. 28 Abs. 3 DSGVO.

(2) Der Auftraggeber schließt diesen Vertrag beim Abschicken des Online-Fragebogens, indem er den Pflicht-Haken setzt. Vor dieser Zustimmung übernimmt und verarbeitet der Auftragnehmer keine personenbezogenen Daten im Auftrag, auch keine Zugänge zu Postfach, Kalender oder Branchensoftware.

(3) Der Vertrag endet mit dem letzten Hauptvertrag, der eine Verarbeitung im Auftrag vorsieht. Die Pflichten nach § 11 (Löschung, Rückgabe) und § 4 Abs. 4 (Vertraulichkeit) gelten darüber hinaus.

(4) Dieser Vertrag gilt nicht für Daten, die der Auftragnehmer als eigener Verantwortlicher verarbeitet, insbesondere Kontakt-, Vertrags- und Zahlungsdaten des Auftraggebers selbst (siehe Datenschutzerklärung unter https://mouza.studio/datenschutz.html).

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Art der Verarbeitung: Erheben (über Formulare und Buchung der Website), Speichern, Organisieren, Auslesen, Abfragen, Übermitteln an den Auftraggeber (z. B. Buchungsbenachrichtigung per E-Mail), Versenden von Bestätigungen und Erinnerungen an Endkunden im Namen des Auftraggebers, Sichern, Wiederherstellen, Exportieren und Löschen.

(2) Zweck: Bereitstellung und Betrieb der Website, Online-Buchung und Automatisierungen des Auftraggebers; Wartung, Fehlerbehebung und Support; Datensicherung; im Projekt die Übernahme bestehender Daten, soweit beauftragt.

(3) Kategorien betroffener Personen:

- Endkunden, Patienten bzw. Klienten und Interessenten des Auftraggebers (z. B. Personen, die einen Termin buchen oder ein Formular absenden),
- Beschäftigte des Auftraggebers (z. B. als buchbare Mitarbeiter, Nutzer eines Verwaltungsbereichs),
- Besucher der Website (technische Zugriffsdaten),
- weitere Personengruppen, die sich aus dem Angebot oder den Angaben im Fragebogen ergeben.

(4) Art der Daten:

- Kontaktdaten (Name, E-Mail, Telefon, ggf. Anschrift),
- Buchungsdaten (gebuchte Leistung, Termin, Mitarbeiter, Notizen bzw. Freitext der betroffenen Person),
- Kommunikationsdaten (Inhalte von Formularanfragen, Bestätigungs- und Erinnerungs-E-Mails),
- Nutzungs- und Protokolldaten (IP-Adresse, Zeitpunkt, aufgerufene Seiten; Server-Logs),
- Zugangsdaten von Nutzern des Auftraggebers zur Lösung,
- weitere Datenarten, die sich aus dem Angebot oder den Angaben im Fragebogen ergeben.

(5) Besondere Kategorien (Art. 9 DSGVO): Die Lösung ist grundsätzlich nicht dafür ausgelegt, Gesundheitsdaten oder andere besondere Kategorien personenbezogener Daten zu verarbeiten. Bei Praxen, Therapeuten und anderen Gesundheitsberufen kann jedoch schon die Tatsache einer Terminbuchung ein Gesundheitsdatum sein. Für diese Auftraggeber gilt zusätzlich die Zusatzvereinbarung für Praxen und Gesundheitsberufe (https://mouza.studio/vertrag/avv_praxis), wenn der Auftragnehmer sie für den Auftraggeber vorsieht und der Auftraggeber ihr zustimmt. Fallen bei anderen Auftraggebern solche Daten an, teilt der Auftraggeber das vorher mit; die Parteien vereinbaren dann ergänzende Maßnahmen.

(6) Ort der Verarbeitung: Ausschließlich in der Europäischen Union bzw. im Europäischen Wirtschaftsraum (Rechenzentren in Frankfurt am Main). Eine Verarbeitung in einem Drittland findet nur unter den Voraussetzungen der Art. 44 ff. DSGVO statt (siehe Anlage 2).

§ 3 Weisungen

(1) Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, auch bei Übermittlungen in ein Drittland, es sei denn, er ist durch Unionsrecht oder deutsches Recht dazu verpflichtet; in diesem Fall teilt er dem Auftraggeber diese Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(2) Die Weisungen ergeben sich aus diesem Vertrag und dem Hauptvertrag. Einzelweisungen erteilt der Auftraggeber in Textform an support@mouza.studio. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, informiert er den Auftraggeber unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO). Er darf die Ausführung aussetzen, bis der Auftraggeber die Weisung bestätigt oder ändert.

§ 4 Vertraulichkeit

(1) Der Auftragnehmer setzt bei der Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Derzeit verarbeitet ausschließlich der Inhaber Moufid Zahed die Daten.

(2) Vertriebsmitarbeiter, die der Auftragnehmer für seinen eigenen Vertrieb einsetzt, erhalten keinen Zugriff auf Daten des Auftraggebers.

(3) Setzt der Auftragnehmer künftig weitere Personen ein, verpflichtet er sie vorher schriftlich zur Vertraulichkeit und informiert den Auftraggeber.

(4) Die Vertraulichkeit gilt über das Ende dieses Vertrags hinaus.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie durch gleichwertige oder bessere Maßnahmen ersetzen. Das Schutzniveau darf nicht unterschritten werden. Wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber mit.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen (Art. 28 Abs. 2 DSGVO). Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter stehen in Anlage 2 und gelten als genehmigt.

(2) Der Auftragnehmer informiert den Auftraggeber mindestens 4 Wochen vorher in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Auftraggeber kann innerhalb von 14 Tagen nach Zugang aus wichtigem datenschutzrechtlichen Grund in Textform widersprechen. Können sich die Parteien nicht einigen, kann jede Partei den betroffenen Hauptvertrag und diesen Vertrag mit einer Frist von einem Monat außerordentlich kündigen. Gilt die Zusatzvereinbarung für Praxen und Gesundheitsberufe, ist stattdessen die vorherige Zustimmung des Auftraggebers nötig.

(3) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten, wie sie in diesem Vertrag festgelegt sind (Art. 28 Abs. 4 DSGVO). Er haftet gegenüber dem Auftraggeber für die Einhaltung durch den Unterauftragsverarbeiter.

(4) Keine Unterauftragsverarbeitung sind Nebenleistungen, bei denen Dritte nicht auf personenbezogene Daten des Auftraggebers zugreifen (z. B. Telekommunikationsdienste für die reine Übertragung, Zertifizierungsstellen für SSL-Zertifikate).

§ 7 Unterstützung bei Rechten der betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten Maßnahmen dabei, Anträge betroffener Personen zu beantworten (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch; Art. 12 bis 22 DSGVO), z. B. durch Export oder Löschung einzelner Datensätze.

(2) Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter und beantwortet sie nicht selbst, außer auf Weisung.

(3) Unterstützung, die über einfache Exporte oder Löschungen hinausgeht, kann der Auftragnehmer nach vorheriger Ankündigung nach Aufwand berechnen, sofern der Aufwand nicht durch einen Verstoß des Auftragnehmers entsteht.

§ 8 Unterstützung bei Pflichten nach Art. 32 bis 36 DSGVO

(1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen bei der Sicherheit der Verarbeitung, bei Meldungen von Datenschutzverletzungen, bei einer Datenschutz-Folgenabschätzung und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde.

(2) Datenschutzverletzungen: Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis, in Textform an die E-Mail-Adresse, die der Auftraggeber zuletzt mitgeteilt hat. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO (Art der Verletzung, Kategorien und ungefähre Zahl der Betroffenen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen, Ansprechpartner).

Informationen, die noch fehlen, liefert er nach, sobald sie vorliegen. Die Meldung an die Aufsichtsbehörde und die Benachrichtigung Betroffener bleiben Sache des Auftraggebers.

§ 9 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Rechtsgrundlage, die Information der Betroffenen (Datenschutzerklärung der Website) und gegebenenfalls Einwilligungen.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

(3) Der Auftraggeber nennt dem Auftragnehmer die gewünschten Löschfristen für Daten in der Lösung (z. B. für vergangene Buchungen). Ohne Vorgabe werden Buchungsdaten 12 Monate nach dem Termin gelöscht oder anonymisiert; andere Daten löscht der Auftragnehmer auf Weisung.

§ 10 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zur Verfügung, die nötig sind, um die Einhaltung der Pflichten aus Art. 28 DSGVO nachzuweisen (Art. 28 Abs. 3 lit. h DSGVO), insbesondere eine aktuelle Fassung der Anlagen 1 und 2.

(2) Der Auftraggeber oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer, der kein Wettbewerber des Auftragnehmers ist, kann Kontrollen durchführen, in der Regel durch Einsicht in Unterlagen und Auskünfte. Vor-Ort-Kontrollen werden mit einer Frist von mindestens 14 Tagen angekündigt, finden während der Servicezeiten laut Wartungs- bzw. Hostingvertrag statt und dürfen den Betrieb nicht unverhältnismäßig stören. Bei Rechenzentren der Unterauftragsverarbeiter genügen deren Zertifikate und Prüfberichte (z. B. ISO 27001).

(3) Den Aufwand für Kontrollen, die über die Bereitstellung von Unterlagen hinausgehen, kann der Auftragnehmer angemessen in Rechnung stellen, es sei denn, die Kontrolle ergibt einen erheblichen Verstoß des Auftragnehmers.

§ 11 Löschung und Rückgabe nach Vertragsende

(1) Nach Ende der Verarbeitung im Auftrag gibt der Auftragnehmer nach Wahl des Auftraggebers alle Daten zurück (Export in einem gängigen, maschinenlesbaren Format) und/oder löscht sie, sofern nicht nach Unionsrecht oder deutschem Recht eine Pflicht zur Speicherung besteht (Art. 28 Abs. 3 lit. g DSGVO). Die Rückgabe hängt nicht von der Bezahlung offener Beträge ab.

(2) Den Export stellt der Auftragnehmer innerhalb von 14 Tagen nach Anforderung bereit. Trifft der Auftraggeber keine Wahl, löscht der Auftragnehmer die Daten 30 Tage nach Vertragsende.

(3) Daten in verschlüsselten Datensicherungen werden nicht einzeln gelöscht, sondern mit dem Ablauf der Aufbewahrungsfristen der Sicherungen überschrieben, spätestens nach 400 Tagen. Bis dahin werden sie nicht weiter verarbeitet, außer für eine vom Auftraggeber gewünschte Wiederherstellung.

(4) Der Auftragnehmer bestätigt die Löschung auf Anfrage in Textform.

§ 12 Haftung

Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Innenverhältnis gelten die Haftungsregelungen des Hauptvertrags (§ 14 der AGB), soweit Art. 82 DSGVO nicht zwingend etwas anderes bestimmt.

§ 13 Schlussbestimmungen

(1) Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes dem Hauptvertrag vor.

(2) Änderungen bedürfen der Textform; die Zustimmung per Klick über einen vom Auftragnehmer zugesandten Link genügt. Dieser Vertrag kann in elektronischem Format geschlossen werden (Art. 28 Abs. 9 DSGVO).

(3) Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam.

(4) Es gilt deutsches Recht.

(5) Mouza Studio speichert Zeitpunkt, Fassung, E-Mail-Adresse, IP-Adresse und Browserkennung der Zustimmung und schickt dem Auftraggeber eine Bestätigung mit diesem Vertrag und den Anlagen als PDF.

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

Kundenlösungen werden nach demselben Muster eingerichtet wie das Verwaltungssystem von Mouza Studio und sind in die nächtliche Datensicherung aufgenommen.

1. Vertraulichkeit

Zutrittskontrolle

- Server ausschließlich in Rechenzentren des Unterauftragsverarbeiters (Frankfurt am Main) mit dessen physischen Sicherungsmaßnahmen; kein eigener Serverraum.
- Arbeitsgerät des Inhabers in verschlossenen Räumen, mit Festplattenverschlüsselung.

Zugangskontrolle

- Anmeldung am Verwaltungsbereich mit Passkey (Gerätebindung, biometrisch bzw. PIN). Notfallzugang nur mit Passwort und einmaligem Code an eine zweite E-Mail-Adresse (10 Minuten gültig).
- Server-Zugang nur per SSH mit Schlüssel, keine Anmeldung mit Passwort.
- Dienste sind nur lokal erreichbar; von außen erreichbar ist nur der Webserver über HTTPS.
- Zugangsdaten und Schlüssel liegen in einer Konfigurationsdatei, die nur der Administrator und der jeweilige Dienst lesen dürfen, nie im Quellcode.

Zugriffskontrolle

- Rollen- und Rechtekonzept im Verwaltungsbereich: nur der Inhaber sieht Kundendaten; Vertriebsrollen sehen nur ihre freigegebenen Lead-Listen, keine Kunden-, Finanz- oder Postfachdaten.
- Kundenseiten (Angebot, Fragebogen, Abo) nur über geheime, zufällige Links; jede Seite bekommt nur die eigenen Daten.
- Zugangsdaten aus Fragebögen werden mit AES verschlüsselt gespeichert.

Trennungskontrolle

- Jede Anwendung (jedes Projekt) auf dem Server läuft getrennt: eigener Linux-Benutzer ohne Login-Shell, eigene Verzeichnisse mit eingeschränkten Rechten, eigene PostgreSQL-Datenbank mit eigener Rolle und Anmeldung nur über lokalen Socket, Entzug der Standardrechte für alle anderen Rollen, eigener Systemdienst mit eingeschränktem Dateisystemzugriff, eigene Webserver-Konfiguration und eigene Logdateien.
- Trennung von Test- und Echtdaten; Zahlungen im Testmodus getrennt vom Livemodus.

Pseudonymisierung

- Wo für den Zweck möglich, z. B. Auswertungen ohne Namen.

2. Integrität

Weitergabekontrolle

- Transportverschlüsselung per TLS (HTTPS, automatische Erneuerung der Zertifikate) für Website, Verwaltungsbereich und Schnittstellen; E-Mail-Versand mit TLS und Absender-Authentifizierung (SPF, DKIM, DMARC).
- Datensicherungen werden vor dem Verlassen des Servers mit AES-256-GCM verschlüsselt.
- Zugriff auf den Sicherungsspeicher nur mit eigenem, eingeschränktem Zugang (nur Hochladen und Lesen, kein Löschen) und nur von der IP-Adresse des Servers.

Eingabekontrolle

- Protokoll aller Änderungen im Verwaltungsbereich (wer, was, wann), auch bei Änderungen über Schnittstellen.
- Server-Logs werden 14 Tage aufbewahrt.

3. Verfügbarkeit und Belastbarkeit

- Jede Nacht automatische, verschlüsselte Sicherung der Kunden-Websites einschließlich Datenbanken und Dateien sowie des Verwaltungssystems bei Amazon Web Services im Rechenzentrum Frankfurt am Main; Aufbewahrung täglich 35 Tage, wöchentlich 120 Tage, monatlich bis 400 Tage; Versionierung aktiv.
- Zusätzlich Server-Snapshots beim Rechenzentrumsbetreiber.
- Automatische Meldung, wenn eine Sicherung länger als 36 Stunden fehlt.
- Wiederherstellung dokumentiert und getestet.
- Überwachung der Erreichbarkeit der Kundenseiten etwa alle 5 Minuten sowie der Zertifikats- und Domainlaufzeiten, mit automatischer Störungsmeldung.
- Automatischer Neustart der Dienste bei Absturz.
- Zeitnahe Sicherheitsupdates für Betriebssystem und Laufzeitumgebung; Sicherheitsupdates des Betriebssystems werden automatisch eingespielt.

4. Verfahren zur regelmäßigen Überprüfung

- Überprüfung dieser Maßnahmen mindestens einmal jährlich und nach wesentlichen Änderungen am Aufbau.
- Test der Wiederherstellung mindestens einmal jährlich.
- Datenschutzfreundliche Voreinstellungen: Kundenlösungen erheben nur die Daten, die für Buchung bzw. Anfrage nötig sind; keine Tracking-Dienste ohne Weisung des Auftraggebers.
- Auftragskontrolle: Unterauftragsverarbeiter nur mit eigenem Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO; Weisungen des Auftraggebers werden im Ticket dokumentiert.

Anlage 2: Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung	Garantien
Hostinger International Ltd., 61 Lordou Vironos Street, 6023 Larnaka, Zypern	Bereitstellung des virtuellen Servers (Rechenzentrum), auf dem die Lösung läuft; E-Mail-Postfächer und E-Mail-Versand	Rechenzentrum Frankfurt am Main, Deutschland	Vertrag zur Auftragsverarbeitung des Anbieters (Art. 28 DSGVO)

Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg	Speicher für die verschlüsselte Datensicherung (Amazon S3)	Rechenzentrum Frankfurt am Main (Region eu-central-1), Deutschland	Vertrag zur Auftragsverarbeitung des Anbieters (AWS Data Processing Addendum mit Standardvertragsklauseln); Daten werden vor der Übertragung verschlüsselt, AWS hat keinen Schlüssel; Muttergesellschaft in den USA unter dem EU-US Data Privacy Framework zertifiziert

Weitere Unterauftragsverarbeiter werden nur nach dem Verfahren in § 6 hinzugezogen.

Die Zahlungen zwischen Auftraggeber und Auftragnehmer wickelt Stripe Payments Europe Ltd. (Dublin, Irland) ab. Stripe verarbeitet dabei nur Zahlungsdaten des Auftraggebers selbst, keine Daten seiner Endkunden, und ist dafür eigener Verantwortlicher. Stripe ist daher kein Unterauftragsverarbeiter im Sinne dieses Vertrags; Näheres steht in der Datenschutzerklärung von Mouza Studio.