

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Majestic-Webs Loyalty

Stand: 11. Oktober 2026

zwischen

dem im Auftrag bezeichneten Unternehmenskunden – nachfolgend „Verantwortlicher“ –

und

Majestic-Webs GbR, Breitenfelderstraße 28, 20251 Hamburg, Deutschland, vertreten durch Lajos Theodoridis und Jonas Thomsen, gemeinsam vertretungsberechtigt – nachfolgend „Auftragsverarbeiter“ –

§ 1 Gegenstand und Dauer

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Zusammenhang mit Bereitstellung, Hosting, Betrieb, Wartung und Support von Majestic-Webs Loyalty.

(2) Die Dauer dieser Vereinbarung entspricht der Dauer des Hauptvertrags. Pflichten, die ihrer Natur nach fortwirken, insbesondere Vertraulichkeits- und Löschpflichten, bleiben bis zu ihrer Erfüllung bestehen.

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung umfasst insbesondere Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung an technisch erforderliche Unterauftragnehmer, Abgleichen, Einschränken, Löschen und Vernichten, soweit dies zur technischen Bereitstellung des Loyalty-Systems erforderlich ist.

- Bereitstellung digitaler Stempelkarten und öffentlicher Loyalty-Seiten
- Verwaltung von Kartenkennungen, Stempelständen und Prämienstatus
- Verarbeitung und Protokollierung von Stempel- und Einlösevorgängen
- Bereitstellung von Mitarbeiter- und Händlerzugängen
- QR-/NFC-Weiterleitung und technische Kartenidentifikation
- Erzeugung, Ausgabe und Aktualisierung von Apple-Wallet- und Google-Wallet-Pässen
- Hosting, Datenbankbetrieb, Backup, Monitoring, Fehleranalyse und Support
- Missbrauchs-, Sicherheits- und Betrugsprävention im Rahmen der Plattformfunktion

§ 3 Kategorien betroffener Personen

- Endkunden und Nutzer der digitalen Stempelkarten
- Beschäftigte, Mitarbeiter und sonstige berechtigte Nutzer des Verantwortlichen
- Ansprechpartner des Verantwortlichen, soweit deren Daten im Auftrag verarbeitet werden

§ 4 Arten personenbezogener Daten

- Pseudonyme bzw. zufällige Kartenkennungen und Tokens
- Stempelstand, Prämienstatus und Loyalty-Programmdaten
- Transaktionsdaten zu Stempeln und Prämieeinlösungen

- Zeit-, Standort- und Unternehmenszuordnungen
- Namen, geschäftliche E-Mail-Adressen und Benutzernamen der Mitarbeiter und berechtigten Nutzer
- Mitarbeiterkennungen, Rollen und Berechtigungen
- Technische Nutzungs-, Sicherheits- und Protokolldaten, insbesondere IP-Adresse, Zeitstempel und Geräte-/Browserinformationen, soweit anfallend
- Wallet-bezogene technische Kennungen und Passinformationen, soweit für die Ausgabe und Aktualisierung erforderlich
- Support- und Fehlerdaten, soweit sie Daten des Verantwortlichen oder seiner Endkunden enthalten

Besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO sind nicht Gegenstand der Verarbeitung. Der Verantwortliche stellt sicher, dass solche Daten nicht in die Plattform eingegeben werden.

§ 5 Weisungsgebundenheit

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, soweit keine gesetzliche Verpflichtung zu einer darüber hinausgehenden Verarbeitung besteht.

(2) Die Weisungen ergeben sich zunächst aus Hauptvertrag, Leistungsbeschreibung, dieser Vereinbarung und den Einstellungen des Verantwortlichen im Dashboard. Einzelweisungen können in Textform erteilt werden.

(3) Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtlich unzulässig, informiert er den Verantwortlichen unverzüglich und kann die Ausführung bis zur Bestätigung oder Änderung aussetzen.

§ 6 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass zur Verarbeitung befugte Personen auf Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und nur im erforderlichen Umfang Zugriff erhalten.

§ 7 Sicherheit der Verarbeitung

Der Auftragsverarbeiter trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung und der Risiken angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die zum Zeitpunkt des Vertragsschlusses geltenden Maßnahmen ergeben sich aus der Anlage „Technische und organisatorische Maßnahmen (TOMs)“.

Der Auftragsverarbeiter darf TOMs weiterentwickeln oder durch gleichwertige bzw. wirksamere Maßnahmen ersetzen, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

§ 8 Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen angemessen bei der Erfüllung seiner Pflichten, insbesondere bei Betroffenenrechten, Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und Konsultationen mit Aufsichtsbehörden, soweit die Verarbeitung durch den Auftragsverarbeiter betroffen ist.

§ 9 Betroffenenrechte

Gehen Anträge betroffener Personen beim Auftragsverarbeiter ein, die erkennbar Daten des Verantwortlichen betreffen, wird der Auftragsverarbeiter den Antrag grundsätzlich nicht eigenständig inhaltlich beantworten, sondern unverzüglich an den Verantwortlichen weiterleiten, soweit keine gesetzliche Pflicht zu einer eigenen Antwort besteht. Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen Möglichkeiten bei Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit.

§ 10 Datenschutzverletzungen

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, soweit Daten des Verantwortlichen betroffen sind. Die Mitteilung enthält, soweit verfügbar, die zur Erfüllung der Pflichten nach Art. 33 und 34 DSGVO erforderlichen Informationen. Der Auftragsverarbeiter ergreift angemessene Maßnahmen zur Eindämmung und Behebung.

§ 11 Unterauftragnehmer

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung zum Einsatz weiterer Auftragsverarbeiter, soweit diese für Hosting, Datenbank, E-Mail, Monitoring, Backup, Wallet-Anbindung oder sonstige technische Betriebsleistungen erforderlich sind. Die bei Vertragsschluss eingesetzten Unterauftragnehmer ergeben sich aus Anlage 2 und gelten als genehmigt.

(2) Der Auftragsverarbeiter führt eine aktuelle Liste der eingesetzten Unterauftragnehmer und informiert den Verantwortlichen über beabsichtigte wesentliche Änderungen. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Tagen nach Mitteilung widersprechen. Können die Parteien keine zumutbare Lösung finden, kann die betroffene Leistung nach Maßgabe des Hauptvertrags beendet werden.

(3) Der Auftragsverarbeiter verpflichtet Unterauftragnehmer vertraglich zu Datenschutzpflichten, die den Anforderungen des Art. 28 DSGVO entsprechen.

§ 12 Drittlandübermittlungen

Verarbeitungen außerhalb des Europäischen Wirtschaftsraums erfolgen nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Der Auftragsverarbeiter stellt insbesondere sicher, dass ein Angemessenheitsbeschluss, geeignete Garantien oder eine andere zulässige Übermittlungsgrundlage besteht und erforderlichenfalls ergänzende Maßnahmen getroffen werden.

§ 13 Nachweise und Kontrollen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage die Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Pflichten aus Art. 28 DSGVO nachzuweisen.

(2) Kontrollen und Audits sind mit angemessener Vorankündigung, während üblicher Geschäftszeiten und unter Wahrung von Betriebs- und Geschäftsgeheimnissen durchzuführen. Vor-Ort-Kontrollen sind auf das erforderliche Maß zu beschränken und können durch geeignete Nachweise, Zertifikate, Prüfberichte oder Remote-Audits ersetzt werden, soweit diese einen gleichwertigen Nachweis ermöglichen.

§ 14 Löschung und Rückgabe

Nach Abschluss der vertraglichen Leistungen löscht oder gibt der Auftragsverarbeiter personenbezogene Daten nach Wahl des Verantwortlichen zurück, soweit keine gesetzliche Pflicht zur weiteren Speicherung besteht. Daten in Sicherungskopien werden im Rahmen des regulären Backup-Zyklus überschrieben oder gelöscht und bis dahin gegen produktive Nutzung gesperrt. Gesetzlich aufzubewahrende Daten werden von sonstigen Daten getrennt und nur für den gesetzlichen Zweck weiterverarbeitet.

§ 15 Verantwortlichkeit

Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung, die Rechtsgrundlagen, Informationspflichten, Festlegung zulässiger Zwecke, Datenminimierung und die Rechtmäßigkeit seiner Weisungen verantwortlich.

§ 16 Schlussbestimmungen

Änderungen und Ergänzungen dieser Vereinbarung bedürfen mindestens der Textform, soweit nicht gesetzlich eine strengere Form erforderlich ist. Im Übrigen gelten die Bestimmungen des Hauptvertrags.

Anlage 1 – Beschreibung der Verarbeitung

Merkmal	Beschreibung
Gegenstand	Betrieb eines digitalen Stempelkarten- und Loyalty-Systems
Dauer	Laufzeit des Hauptvertrags zuzüglich technisch und gesetzlich erforderlicher Nachlaufzeiten
Zweck	Ausgabe und Verwaltung digitaler Kundenkarten, Stempel- und Prämienverwaltung, Wallet-Integration, Support und Sicherheit
Betroffene	Endkunden; Mitarbeiter und berechtigte Nutzer des Verantwortlichen
Daten	Karten-/Tokenkennungen, Stempel- und Prämienstatus, Transaktionen, Mitarbeiter-/Rolleninformationen, technische Protokolldaten, Wallet-Passdaten

Anlage 2 – Unterauftragnehmer

Die jeweils aktuelle Liste der für Majestic-Webs Loyalty eingesetzten Unterauftragnehmer wird dem Verantwortlichen vor Beginn der produktiven Verarbeitung bereitgestellt und während der Vertragslaufzeit in aktueller Fassung elektronisch zugänglich gemacht.

Zum Stand dieser Vereinbarung werden folgende Unterauftragnehmer eingesetzt:

Unterauftragnehmer	Leistung
Vercel Inc., 440 N Barranca Avenue #4133, Covina, CA 91723, USA	Hosting der Plattform, Auslieferung der Seiten, Ausführung der Serverfunktionen, Server-Logfiles

Supabase, Inc., 970 Toa Payoh North #07-04, Singapur 318992	Datenbank (PostgreSQL) und Dateispeicher für Logos
Plus Five Five, Inc. („Resend“), 2261 Market Street #5039, San Francisco, CA 94114, USA	Versand transaktionaler E-Mails (Einladungen, Passwort-Zurücksetzung, Bestätigungen, Benachrichtigungen)

Soweit diese Unterauftragnehmer Daten außerhalb des Europäischen Wirtschaftsraums verarbeiten, erfolgt dies auf Grundlage des Angemessenheitsbeschlusses der Europäischen Kommission zum EU-U.S. Data Privacy Framework, soweit der jeweilige Unterauftragnehmer hiernach zertifiziert ist, und im Übrigen auf Grundlage der Standardvertragsklauseln der Europäischen Kommission.

Apple (Apple Distribution International Ltd.) und Google (Google Ireland Limited) verarbeiten Daten im Zusammenhang mit Apple Wallet bzw. Google Wallet in eigener datenschutzrechtlicher Verantwortlichkeit und sind keine Unterauftragnehmer im Sinne dieser Vereinbarung.

Anlage 3 – Technische und organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen ergeben sich aus dem gesonderten Dokument „Technische und organisatorische Maßnahmen (TOMs) gemäß Art. 32 DSGVO – Majestic-Webs Loyalty“ in der bei Vertragsschluss geltenden Fassung. Es ist Bestandteil dieser Vereinbarung.

Unterschriften

Verantwortlicher

Unternehmen: _____

Name/Funktion: _____

Ort, Datum: _____

Unterschrift: _____

Auftragsverarbeiter

Majestic-Webs GbR

Breitenfelderstraße 28, 20251 Hamburg, Deutschland

Vertreten durch: Lajos Theodoridis und Jonas Thomsen, gemeinsam vertretungsberechtigt

Ort, Datum: _____

Unterschrift Lajos Theodoridis: _____

Unterschrift Jonas Thomsen: _____