

Technische und organisatorische Maßnahmen (TOMs)

gemäß Art. 32 DSGVO – Majestic-Webs Loyalty

Stand: 11. Oktober 2026

1. Ziel und Geltungsbereich

Diese technischen und organisatorischen Maßnahmen beschreiben das für Majestic-Webs Loyalty vorgesehene Schutzkonzept. Die Maßnahmen werden risikoorientiert umgesetzt und fortlaufend an technische und organisatorische Entwicklungen angepasst.

2. Vertraulichkeit

2.1 Zutrittskontrolle

- Zugriff auf produktive Systeme erfolgt grundsätzlich remote über abgesicherte Administrationszugänge; physische Rechenzentrumsmaßnahmen werden durch die eingesetzten Hostinganbieter gewährleistet.
- Lokale Arbeitsgeräte werden gegen unbefugte Nutzung gesichert und bei Abwesenheit gesperrt.

2.2 Zugangskontrolle

- individuelle Benutzerkonten für administrative und betriebliche Zugriffe
- sichere Passwortspeicherung mittels geeigneter kryptografischer Hash-Verfahren (scrypt mit individuellem Salt je Passwort)
- Mindestlänge für Passwörter von zehn Zeichen und Ablehnung leicht zu erratender Passwörter
- rollenbasierte Berechtigungen
- zeitlich begrenzte, kryptografisch zufällige Einladungstokens, die nur einmal verwendbar sind und nur als Prüfwert gespeichert werden
- Session-Schutz durch sichere Cookies und geeignete Ablaufmechanismen; Sitzungen werden serverseitig geführt und bei Abmeldung, Passwortwechsel oder Sperrung beendet
- Rate-Limiting und Schutz gegen automatisierte Login-Versuche
- Mehrfaktor-Authentisierung für besonders privilegierte Zugänge, soweit technisch verfügbar und eingerichtet
- unverzügliche Sperrung kompromittierter oder nicht mehr benötigter Zugänge

2.3 Zugriffskontrolle und Mandantentrennung

- serverseitige Autorisierungsprüfung bei geschützten Aktionen
- Mandantenzuordnung von Benutzern, Karten, Transaktionen und Standorten
- keine ausschließliche Vertrauensentscheidung anhand clientseitig übermittelter Merchant- oder Karten-IDs
- Datenbankzugriff ausschließlich serverseitig; kein unmittelbarer Zugriff aus dem Browser auf die Datenbank
- Minimalprinzip bei Rollen und Berechtigungen
- Trennung von internen Majestic-Webs-Administrationsrechten und Händlerrechten
- regelmäßige Überprüfung privilegierter Zugänge

2.4 Trennungskontrolle

- logische Trennung von Mandantendaten über eindeutige Unternehmenskennungen und serverseitige Zugriffskontrollen
- Trennung von Test- und Produktivumgebungen, soweit technisch erforderlich
- getrennte Behandlung von Authentifizierungs-, Anwendungs- und Transaktionsdaten nach Zweck
- keine Nutzung von Kundendaten zu eigenen Werbezwecken ohne gesonderte Rechtsgrundlage

3. Integrität

3.1 Weitergabekontrolle

- TLS/HTTPS für die Übertragung zwischen Browser, Plattform und APIs; unverschlüsselte Aufrufe werden auf HTTPS umgeleitet (HSTS)
- verschlüsselte bzw. abgesicherte API-Kommunikation mit Wallet- und Infrastrukturpartnern
- sichere Verwaltung von API-Schlüsseln, Zertifikaten und Service-Account-Credentials
- keine Speicherung geheimer Schlüssel im öffentlich ausgelieferten Clientcode
- Protokollierung wesentlicher administrativer Änderungen und Loyalty-Transaktionen

3.2 Eingabekontrolle

- Transaktionshistorie für Stempel- und Prämienvorgänge
- Audit-Logs für wesentliche administrative Änderungen
- Zeitstempel und handelndes Benutzerkonto bei sicherheits- oder abrechnungsrelevanten Vorgängen
- Validierung von Eingaben und strukturierte Fehlerbehandlung

4. Verfügbarkeit und Belastbarkeit

- regelmäßige Datensicherungen nach dem für die Produktivumgebung festgelegten Backup-Konzept
- Wiederherstellungsverfahren für wesentliche Datenbestände
- Monitoring technischer Fehler und Verfügbarkeitsprobleme
- Sicherheits- und Abhängigkeitsupdates
- Schutz vor übermäßigen Anfragen durch Rate-Limits, wo risikoadäquat
- Nutzung skalierbarer Hosting- und Datenbankdienste
- Notfallmaßnahmen bei kompromittierten Zugangsdaten oder Wallet-Zertifikaten

5. Wiederherstellbarkeit

- Backups werden in einem festgelegten Zyklus erstellt oder durch den eingesetzten Infrastrukturprovider bereitgestellt.
- Wiederherstellungsprozesse werden bei wesentlichen Architekturänderungen und in angemessenen Abständen überprüft.
- Produktionsänderungen werden so durchgeführt, dass eine Wiederherstellung oder Rückkehr zu einem stabilen Zustand möglich bleibt, soweit technisch angemessen.

6. Verfahren zur regelmäßigen Überprüfung

- regelmäßige Überprüfung von Abhängigkeiten und Sicherheitsupdates
- Code- und Konfigurationsprüfung bei sicherheitsrelevanten Änderungen
- Überprüfung von Rollen und Berechtigungen

- Auswertung sicherheitsrelevanter Logs bei konkreten Anlässen
- Prüfung von Backup- und Wiederherstellungsprozessen
- Anpassung der TOMs bei wesentlichen Änderungen der Verarbeitung oder Risikolage

7. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

- pseudonyme Kundenkarten ohne verpflichtende Namens-, E-Mail- oder Telefonnummernerfassung in der Grundfunktion
- zufällige, nicht fortlaufende öffentliche Tokens
- Datenminimierung bei Wallet-Passdaten
- Beschränkung öffentlich sichtbarer Informationen auf die für das Loyalty-Programm erforderlichen Inhalte
- ausschließlich technisch erforderliche Cookies; keine Analyse-, Tracking- oder Werbetechnologien ohne Einwilligung
- keine Einbindung externer Schriftarten, Skripte oder Medien von Servern Dritter
- rollenbasierte Standardberechtigungen
- Lösch- und Deaktivierungsfunktionen für Karten und Konten

8. Schutz von Zugangsdaten und Geheimnissen

- Secrets, private Schlüssel, Wallet-Zertifikate und Service-Account-Schlüssel werden ausschließlich serverseitig gespeichert.
- Zugriff auf produktive Geheimnisse ist auf erforderliche Personen und Systeme beschränkt.
- Geheimnisse werden bei Verdacht auf Kompromittierung unverzüglich ersetzt oder widerrufen.
- Private Schlüssel und Zertifikate werden nicht in öffentlichen Repositories gespeichert.

9. Software- und Anwendungssicherheit

- serverseitige Eingabevalidierung
- parameterisierte Datenbankzugriffe bzw. sichere ORM-Verwendung
- Schutz gegen Cross-Site-Scripting durch Framework- und Ausgabehärtung
- CSRF-Schutz bei zustandsändernden browserbasierten Vorgängen, soweit erforderlich
- Security Header und sichere Cookie-Konfiguration
- Dateiapload-Prüfung hinsichtlich Typ, Größe und zulässiger Verwendung
- Schutz gegen IDOR durch serverseitige Mandanten- und Objektberechtigungsprüfung
- Rate-Limits für sensible Endpunkte
- keine sicherheitsrelevanten Entscheidungen ausschließlich im Frontend

10. Incident Management

- Erfassung und Bewertung sicherheitsrelevanter Vorfälle
- Eindämmung und Behebung erkannter Schwachstellen
- Sicherung erforderlicher Protokolle zur Ursachenanalyse
- Information betroffener Verantwortlicher bei Datenschutzverletzungen ohne unangemessene Verzögerung
- Dokumentation wesentlicher Datenschutzverletzungen

- Rotation kompromittierter Zugangsdaten und Schlüssel

11. Löschung und Datenlebenszyklus

- Löschung oder Anonymisierung nach Wegfall des Verarbeitungszwecks und Ablauf gesetzlicher Pflichten
- Löschung von Endkundendaten nach Weisung des Verantwortlichen bzw. den vereinbarten Löschregeln
- Deaktivierung nicht mehr benötigter Konten und Tokens
- Backup-Daten werden im Rahmen des regulären Überschreibungs- und Löschzyklus entfernt
- gesetzlich aufzubewahrende Daten werden für andere Zwecke gesperrt

12. Unterauftragnehmer

Unterauftragnehmer werden nach Eignung, Sicherheitsniveau und datenschutzrechtlicher Zulässigkeit ausgewählt. Soweit sie personenbezogene Daten im Auftrag verarbeiten, werden Verträge nach Art. 28 DSGVO geschlossen. Drittlandübermittlungen werden nur unter Beachtung der Art. 44 ff. DSGVO vorgenommen.

13. Organisatorische Maßnahmen

- Vertraulichkeitsverpflichtung für zugriffsberechtigte Personen
- Need-to-know-Prinzip
- Dokumentation wesentlicher Sicherheits- und Datenschutzprozesse
- regelmäßige Sensibilisierung der mit Administration und Entwicklung betrauten Personen
- geregeltes Berechtigungsmanagement bei Eintritt, Rollenwechsel und Ausscheiden
- Kontaktroute für Datenschutz- und Sicherheitsmeldungen