

Lösch- und Aufbewahrungskonzept – Majestic-Webs Loyalty

für produktive Daten, Konten, Loyalty-Karten und Protokolle

Stand: 11. Oktober 2026

1. Grundsatz

Personenbezogene Daten werden nur so lange gespeichert, wie sie für den jeweiligen Verarbeitungszweck erforderlich sind oder gesetzliche Aufbewahrungspflichten bestehen. Nach Wegfall des Zwecks werden Daten gelöscht, anonymisiert oder – soweit eine gesetzliche Aufbewahrungspflicht besteht – für andere Zwecke gesperrt.

2. Datenkategorien und Löschereignisse

Datenkategorie	Regelfall / Löschereignis
Interessenten- und Anfragedaten	Löschung nach Abschluss der Kommunikation, sofern kein Vertrag zustande kommt und keine berechtigten Nachweisinteressen oder gesetzlichen Pflichten entgegenstehen.
Vertrags- und Rechnungsdaten	Aufbewahrung entsprechend den jeweils geltenden handels- und steuerrechtlichen Pflichten; danach Löschung.
Unternehmenskonto und Ansprechpartner	Nach Vertragsende und Ablauf erforderlicher Nachlauf- und Nachweisfristen; gesetzlich aufzubewahrende Bestandteile bleiben gesperrt erhalten.
Mitarbeiterkonten	Deaktivierung bei Entzug der Berechtigung; Löschung personenbezogener Profildaten nach Wegfall des Zwecks, soweit Audit- oder Nachweispflichten keine begrenzte weitere Speicherung erfordern.
Endkunden-/CustomerCard-Daten	Nach Weisung des verantwortlichen Unternehmenskunden, bei Löschung des Loyalty-Programms oder nach Vertragsende entsprechend der vereinbarten Export-/Löschphase.
Stempel- und Prämientransaktionen	Nach Maßgabe des verantwortlichen Unternehmenskunden und der für das Bonusprogramm erforderlichen Nachweisfristen; anschließend Löschung oder Anonymisierung.
Einladungstokens und Passwort-Reset-Tokens	Nach Nutzung, Ablauf oder Widerruf unverzüglich technisch entwerten; nicht mehr benötigte Token-Daten löschen.
Sitzungen (Logins)	Löschung bei Abmeldung, Passwortwechsel, Deaktivierung des Kontos oder Sperrung des Unternehmens; im Übrigen Ablauf der Gültigkeit nach Ziffer 3.

Wallet-Registrierungen (Geräteerkennung, Push-Token)	Löschung, sobald der Pass vom Gerät entfernt wird, der Push-Dienst das Gerät als abgemeldet meldet oder die zugehörige Karte gelöscht wird.
Logos und Designdaten	Löschung des bisherigen Logos beim Ersetzen oder Entfernen; im Übrigen mit Löschung des Unternehmenskontos.
Server- und Sicherheitslogs	Nur solange speichern, wie dies für Betrieb, Fehleranalyse und Sicherheitszwecke erforderlich ist; längere Speicherung nur bei konkretem Sicherheitsvorfall oder rechtlicher Pflicht.
Supportdaten	Nach Abschluss des Supportfalls und Ablauf erforderlicher Nachweisfristen löschen oder anonymisieren, soweit keine Vertrags- oder Rechtsgründe entgegenstehen.
Backups	Löschung durch turnusmäßiges Überschreiben gemäß Backup-Zyklus; bis dahin keine reguläre produktive Nutzung gelöschter Datensätze.

3. Technische Gültigkeits- und Speicherfristen

Für die folgenden technischen Daten gelten feste Fristen, die in der Plattform hinterlegt sind:

Datum	Frist
Sitzung ohne „Angemeldet bleiben“	Gültig bis zum Schließen des Browsers, längstens 12 Stunden
Sitzung mit „Angemeldet bleiben“	Gültig 30 Tage
Einladungslink	Gültig 7 Tage, nur einmal verwendbar; eine neue Einladung macht ältere Links ungültig
Link zum Zurücksetzen des Passworts	Gültig 60 Minuten, nur einmal verwendbar
Zähler zur Begrenzung von Anmelde- und Anfrageversuchen	Zeitfenster von höchstens 60 Minuten; Einträge werden regelmäßig nach wenigen Tagen gelöscht
Cookie mit der Kartenkennung auf dem Gerät des Endkunden	2 Jahre, jederzeit im Browser löschtbar

4. Vertragsende

Nach Vertragsende wird der produktive Zugriff des Unternehmenskunden deaktiviert. Personenbezogene Auftragsdaten werden nach Weisung des Kunden gelöscht oder zurückgegeben, soweit keine gesetzliche Pflicht zur weiteren Speicherung besteht. Öffentliche Loyalty-Seiten und aktive Stempelfunktionen können deaktiviert werden.

Mit der Löschung eines Unternehmens werden die zugehörigen Stempelkarten, Transaktionen, Prämieinlösungen, Mitgliedschaften, Einladungen, Wallet-Registrierungen und unternehmensbezogenen Protokolleinträge gemeinsam gelöscht.

5. Betroffenenanfragen

Bei berechtigten Löschersuchen werden betroffene Datensätze identifiziert und gelöscht oder anonymisiert, soweit keine gesetzlichen Ausnahmen oder Aufbewahrungspflichten entgegenstehen. Bei Auftragsdaten erfolgt die Bearbeitung grundsätzlich auf dokumentierte Weisung des verantwortlichen Unternehmenskunden.

6. Backups

Daten, die im Produktivsystem gelöscht wurden, können bis zum Ablauf des regulären Backup-Zyklus noch in Sicherungskopien enthalten sein. Diese Daten werden nicht wieder in den produktiven Betrieb übernommen, außer dies ist zur Wiederherstellung nach einem Störfall erforderlich. In diesem Fall werden zuvor wirksam gelöschte Datensätze nach Wiederherstellung erneut gelöscht, soweit technisch und organisatorisch erforderlich.

7. Dokumentation

Wesentliche Löschvorgänge, insbesondere mandantenbezogene Löschungen nach Vertragsende oder Betroffenenanfragen, werden in angemessenem Umfang dokumentiert, ohne dadurch unnötig neue personenbezogene Daten zu erzeugen.