TOM - MASSNAHMEN

STAND 25.10.2026

Technische und organisatorische Maßnahmen

Anlage zum AVV · Art. 32 DSGVO · Stand 25.10.2026. Beschreibung der Anwendung und der ergänzenden Betreiberpflichten.

1. Zugang und Berechtigungen

Betreiberzugang mit Passwort-Hash und Passwortprüfung, Begrenzung fehlgeschlagener Anmeldeversuche und Inaktivitätsbegrenzung. Sitzungskennungen werden nach Anmeldung erneuert. Kunden erhalten keine Benutzerkonten, sondern einen privaten, zufälligen Ergebniszugang. Zugriff setzt die passende Sitzung oder den individuellen Ergebnislink voraus. Produktive System-, Hosting- und Mailzugänge sind auf berechtigte Personen zu beschränken. Eine Mehrfaktoranmeldung dieser Anwendung wird nicht zugesagt.

2. Sitzungen und Webschutz

Sitzungscookies mit HttpOnly und SameSite, bei HTTPS zusätzlich Secure. Produktiv ist ausschließlich HTTPS zu verwenden. Zustandsändernde Anfragen benötigen eine CSRF-Prüfung. Ausgaben fremder Seitentexte und KI-Entwürfe werden als Text maskiert. Content-Security-Policy, Frame-Schutz und Schutz gegen MIME-Sniffing ergänzen diese Maßnahmen. Sie ersetzen keine laufende Sicherheitswartung des Hostings.

3. Datenspeicherung und Geheimnisse

Private Daten liegen in durch Webserverregeln gesperrten Verzeichnissen. JSON-Dateien werden unter Dateisperre und mit atomarem Austausch gespeichert. Lokale Dateirechte werden beschränkt. API- und Mailgeheimnisse werden mit AES-256-GCM serverseitig verschlüsselt; der zugehörige Schlüssel ist separat geschützt zu sichern. Analysedaten selbst sind nicht durchgängig als verschlüsselte Datenbank gespeichert. Eine vollständige Verschlüsselung sämtlicher Hostbackups wird nicht behauptet.

4. Trennung und Zweckbindung

Private Kundenanalysen haben eigene zufällige Kennungen und getrennte Zugriffsberechtigungen. Der öffentliche Vorschaudienst gibt vor Freischaltung nur drei echte Seitenresultate aus. Rechnungs- und Vertragsnachweise werden von der zeitlich begrenzten Ergebnisbereitstellung getrennt aufbewahrt. Betreiberprojekte und öffentliche Pay-&-Go-Analysen sind getrennte Funktionsbereiche.

5. Sichere Abrufe und Dienstverbindungen

Nur öffentliche HTTP-/HTTPS-Adressen innerhalb der autorisierten Website; private Netzwerkadressen, fremde Weiterleitungen, Zugangsdaten in URLs und unzulässige Protokolle werden blockiert. DNS-Ziele werden gegen private Adressen geprüft und für den Abruf fest zugeordnet. robots.txt-Regeln werden vor Inhaltsabrufen geprüft. PayPal-Zahlungen werden serverseitig nach

Händler, Währung, Betrag und Bestellzuordnung abgeglichen. TLS-Prüfung für SMTP ist aktiviert.

6. Nachvollziehbarkeit und Manipulationsschutz

Bestellungen, Freischaltungen, Belegerstellung und Versandstatus werden gespeichert. Fortlaufende Belegnummern und eindeutige Zahlungsreferenzen verhindern doppelte Zuordnung. Geschenkcodes sind nur als Prüfsumme gespeichert, zeitlich begrenzt und einmalig verwendbar; parallele Einlösung wird unter Dateisperre abgeglichen. Vertragsfassungen werden zur Bestellung gespeichert und PDFs archiviert. Geheimnisse und vollständige Geschenkcodes werden nicht in Vorgangsprotokolle geschrieben.

7. Fristen und Löschung

Nicht gebuchte Analyse: 24 Stunden Ergebniszugriff. Gebuchte Analyse: 7 Kalendertage. Danach werden Analyseinhalte im regelmäßigen Bereinigungslauf entfernt. Für unbezahlte Bestellversuche ohne Rechnung gilt grundsätzlich eine Bereinigung nach 30 Tagen. Einträge der gehashten IP-Zuordnung werden nach Ablauf ihres 24-stündigen Zeitfensters im nächsten regelmäßigen Bereinigungslauf entfernt. Beleg- und Vertragsnachweise können gesetzlichen Aufbewahrungsfristen unterliegen. Der tägliche serverseitige Wartungsaufruf ist einzurichten und zu überwachen; ein ergänzender Bereinigungslauf erfolgt bei Anwendungsaufrufen. Die Bereinigung zeitlich begrenzter Analysedaten ist von der Fristenkontrolle des Beleg- und Vertragsarchivs zu unterscheiden. Gesetzliche Aufbewahrungsfristen, Auskunfts- und Löschanfragen sowie das Ende zulässiger Aufbewahrungszwecke erfordern zusätzlich eine nachvollziehbare betriebliche Prüfung; eine vollautomatische gesetzliche Archivbereinigung wird nicht zugesagt. Bei neuen Bestellungen wird die zugesagte Frist von 7 Kalendertagen zusammen mit der Vertragsfassung gespeichert und erst bei erstmaliger erfolgreicher Freischaltung, einschließlich einer gültigen Geschenkfreischaltung, in einen festen Ablaufzeitpunkt umgesetzt. Altbestellungen behalten ihre Zusage. Erneutes Öffnen verlängert die Frist nicht. Linkaufnahme, Ergebnis-API, KI-Anforderung, Einzel-/Sammel- und Datenexport prüfen den Zugriff serverseitig. Abgelaufene Ergebnisdaten werden beim nächsten vorhandenen Wartungs-/Bereinigungslauf entfernt; Vertrags- und Belegdaten sind davon getrennt. Backupaufbewahrung und Wiederherstellung richten sich nach dem gesondert dokumentierten betrieblichen Konzept. Websiteabrufe, ausdrücklich angeforderte OpenAI-Verarbeitung, PayPal-Zahlungsabgleich und transaktionaler E-Mail-Versand sind von einer nicht angebotenen Ranking-/Suchvolumenauswertung zu unterscheiden.

8. Verfügbarkeit, Backups und Betriebsverantwortung

Der Betreiber stellt ein angemessenes Backup-, Wiederherstellungs- und Updateverfahren für Webspace, private Daten, PDFs und Verschlüsselungsschlüssel sicher. Wiederherstellungen und die Aktualität von Schutzregeln sind regelmäßig zu prüfen. Konkrete Hostingregion, Backuprotation, Serverprotokollfristen und berechtigte Administratoren sind im tatsächlichen Betrieb zu dokumentieren. Dieses Softwarepaket führt keine unabhängige Kontrolle der Hostingverträge aus und verspricht keine durchgeführte Zertifizierung oder eine bestimmte Verfügbarkeitsquote.

9. Vertraulichkeit und Vorfallbearbeitung

Zugriffsberechtigte Personen sind zur Vertraulichkeit zu verpflichten. Datenschutzanfragen und Sicherheitsmeldungen werden über info@dist-net.com bearbeitet. Der Betreiber dokumentiert Vorfälle, prüft ihren Umfang und informiert betroffene Auftraggeber ohne unangemessene Verzögerung. Änderungen von Dienstleistern oder wesentlichen Schutzmaßnahmen werden entsprechend dem AVV behandelt.