

Anlage TOM

Unterauftragsverarbeiter und technisch-organisatorische Maßnahmen (Art. 28, 32 DSGVO) · Version 1.0 · Stand 20.08.2026

Diese Anlage ist Bestandteil von Teil C der Allgemeinen Geschäftsbedingungen der D&N Marketing GbR (Fassung 2.1). Änderungen der Unterauftragsverarbeiter erfolgen nach dem Verfahren in § 24 Abs. 2 der AGB (Ankündigung in Textform, vier Wochen, Widerspruchsrecht aus wichtigem datenschutzrechtlichem Grund).

A. Genehmigte Unterauftragsverarbeiter

Unternehmen	Sitz / Land	Leistung	Garantien bei Drittlandtransfer
Netlify, Inc.	San Francisco, USA	Hosting und Auslieferung der Website (CDN)	EU-US Data Privacy Framework; ergänzend EU-Standardvertragsklauseln
Hetzner Online GmbH	Gunzenhausen, Deutschland	Betrieb des Formular-Backends (Server-Infrastruktur)	entfällt (Verarbeitung in Deutschland)
IONOS SE	Montabaur, Deutschland	E-Mail-Versand der Formularanfragen (SMTP)	entfällt (Verarbeitung in EU/Deutschland)

Der jeweils projektbezogen eingesetzte Umfang ergibt sich aus dem Vertrag und dem Pflichtenheft; nicht eingesetzte Anbieter verarbeiten keine Daten des Kunden.

B. Technisch-organisatorische Maßnahmen der Agentur

- Zutritts- und Zugangskontrolle.** Verwaltungszugriff auf Server und Dienste ausschließlich über personengebundene Konten; Server-Zugang ausschließlich per SSH mit Public-Key-Authentifizierung, Passwort-Login deaktiviert; Zwei-Faktor-Authentifizierung für alle Verwaltungsoberflächen (Hosting, DNS, Repositories), soweit vom Anbieter unterstützt; Endgeräte der Gesellschafter mit Festplattenverschlüsselung und Sperrbildschirm.
- Zugriffskontrolle.** Berechtigungen nach dem Prinzip der minimalen Rechtevergabe; getrennte Konfiguration je Kunde im Formular-Backend (mandantengetrennte Endpunkte und Empfängeradressen); kein Zugriff von Subunternehmern auf Kundendaten ohne vertragliche Verpflichtung nach Art. 28 DSGVO.
- Übertragungskontrolle.** Transportverschlüsselung sämtlicher Verbindungen (HTTPS/TLS, erzwungen); Formularübermittlung an das Backend und Weiterleitung per E-Mail ausschließlich über verschlüsselte Verbindungen (TLS); keine Übermittlung an nicht benannte Empfänger.
- Eingabe- und Nachvollziehbarkeitskontrolle.** Protokollierung technischer Ereignisse des Formular-Backends (Zeitstempel, Status, Ziel) zur Störungsanalyse und Missbrauchsabwehr einschließlich Ratenbegrenzung; Löschung der technischen Protokolle spätestens nach 30 Tagen; Inhaltsdaten der Anfragen werden nach erfolgreicher Zustellung nicht dauerhaft gespeichert.
- Verfügbarkeitskontrolle.** Laufende Erreichbarkeitsüberwachung der Dienste mit Alarmierung; regelmäßige Sicherungen bzw. Snapshots der Server-Konfiguration; Wiederanlaufplan durch dokumentierte, versionierte Infrastruktur (Konfiguration und Quellcode in Repositories).
- Trennungskontrolle.** Logische Trennung der Daten verschiedener Kunden (getrennte Projekte, Repositories, Endpunkte und Versandkonfigurationen); Test- und Produktivumgebungen sind getrennt.
- Datenminimierung und Löschkonzept.** Verarbeitung nur der für den technischen Betrieb und die Anfrageübermittlung erforderlichen Daten; keine Analyse-, Marketing- oder Profilbildungswerkzeuge im Auftrag des Kunden ohne dessen dokumentierte Weisung; Löschung bzw. Rückgabe nach § 28 der AGB.
- Organisatorische Maßnahmen.** Verpflichtung aller mit der Verarbeitung befassten Personen zur Vertraulichkeit; bei Berufsgeheimnisträgern zusätzlich förmliche Verpflichtung nach § 203 StGB (siehe gesonderte Verschwiegenheitserklärung); regelmäßige Überprüfung dieser Maßnahmen und der eingesetzten Anbieter; Meldung von Datenschutzverletzungen nach § 26 der AGB.

