

Technische und organisatorische Maßnahmen

der Advortal GmbH gemäß Art. 32 DSGVO

Stand: August 2026 · entspricht Anlage A zur Auftragsverarbeitungsvereinbarung, Version 2.0

Die Advortal GmbH, August-Bebel-Straße 3, 08412 Werdau, trifft die nachfolgenden technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Sie berücksichtigen den Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung und die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen.

Hinweis zur Abgrenzung: Die Advortal GmbH betreibt keine eigene Infrastruktur für die Plattform ActiveCampaign. Die Maßnahmen für Speicherung, Betrieb und Verfügbarkeit der Plattform werden von ActiveCampaign, LLC getroffen und sind in deren Sicherheitsdokumentation sowie im jeweils aktuellen SOC-2-Type-2-Bericht beschrieben. Die nachfolgenden Maßnahmen betreffen die Systeme, Endgeräte und Prozesse der Advortal GmbH.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

- Zugang zu Geschäftsräumen ausschließlich für autorisierte Personen; Schließsystem mit dokumentierter Schlüsselvergabe
- Sichere Aufbewahrung von Endgeräten und Datenträgern außerhalb der Nutzungszeiten
- Schutz mobiler Endgeräte durch Passwort oder biometrisches Verfahren
- Automatische Bildschirmsperre bei Inaktivität (max. 5 Minuten)
- Regelungen für mobiles Arbeiten und Home-Office (Sichtschutz, keine Nutzung fremder Netzwerke ohne VPN)

1.2 Zugangskontrolle

- Individuelle, personenbezogene Benutzerkonten; keine Sammel- oder Gruppenkonten
- Verbindliche Passwortrichtlinie (Mindestlänge, Komplexität, keine Mehrfachverwendung); Einsatz eines Passwortmanagers
- Mehr-Faktor-Authentifizierung für alle zentralen Systeme, insbesondere Google Workspace, das Advortal Reseller-Portal und ActiveCampaign
- Vollverschlüsselung der Festplatten aller Endgeräte (z. B. FileVault, BitLocker)
- Aktuelle Betriebssystem- und Sicherheitsupdates; Endpoint-Schutz gegen Schadsoftware
- Sofortige Sperrung nicht mehr benötigter Zugänge, spätestens am Tag des Ausscheidens einer Person

1.3 Zugriffskontrolle

- Rollen- und aufgabenbasiertes Berechtigungskonzept nach dem Need-to-know-Prinzip
- Zugriff auf Kundendaten ausschließlich im Rahmen von Support-, Beratungs- und Administrationsleistungen
- Keine Nutzung personenbezogener Daten des Verantwortlichen zu eigenen Zwecken
- Datenexporte nur anlassbezogen, Löschung unmittelbar nach Erledigung des Vorgangs
- Mindestens halbjährliche Überprüfung und Dokumentation bestehender Zugriffsrechte

1.4 Trennungskontrolle

- Mandantenbezogene Trennung innerhalb der eingesetzten Systeme; getrennte ActiveCampaign-Accounts je Kunde
- Kundenspezifische Zugriffsbeschränkungen; Zugriff nur im Rahmen des jeweiligen Kundenverhältnisses

- Trennung von Produktiv- und Testumgebungen

1.5 Pseudonymisierung und Verschlüsselung

- Transportverschlüsselung (TLS 1.2 oder höher) für sämtliche Datenübertragungen
- Verschlüsselung ruhender Daten auf Endgeräten und in den eingesetzten Cloud-Diensten
- Verwendung anonymisierter oder pseudonymisierter Beispieldaten in Dokumentationen und Schulungen

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

- Weitergabe personenbezogener Daten ausschließlich auf Weisung des Verantwortlichen oder auf gesetzlicher Grundlage
- Versand sensibler Inhalte nur verschlüsselt oder über geschützte Freigabelinks mit Ablaufdatum
- Keine Nutzung privater Endgeräte, privater E-Mail-Konten oder nicht freigegebener Cloud-Dienste
- Dokumentierte Vergabe und Entziehung von Zugriffsrechten

2.2 Eingabekontrolle

- Einsatz von Systemen mit Protokollierungsfunktion; Nachvollziehbarkeit von Änderungen über Benutzerkennungen
- Dokumentation wesentlicher Support- und Administrationsmaßnahmen im Ticketverlauf
- Aufbewahrung der Protokolle für einen angemessenen Zeitraum

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Nutzung professioneller Cloud-Dienste mit redundanter Auslegung
- Regelmäßige Datensicherung durch die eingesetzten Plattformanbieter; Prüfung der Wiederherstellbarkeit
- Aktueller Endpoint- und Malware-Schutz sowie zeitnahe Einspielung von Sicherheitsupdates
- Definierte Vertretungsregelungen für den Support
- Notfall- und Wiederanlaufkonzept für die Systeme der Advertal GmbH

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Datenschutz-Managementsystem mit Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO
- Mindestens jährliche Überprüfung und Fortschreibung der technischen und organisatorischen Maßnahmen
- Verpflichtung aller Beschäftigten auf Vertraulichkeit und das Datengeheimnis vor Aufnahme der Tätigkeit
- Regelmäßige Schulung und Sensibilisierung zu Datenschutz und Informationssicherheit mit Nachweisdokumentation
- Sorgfältige Auswahl, vertragliche Bindung und regelmäßige Überprüfung der Unterauftragsverarbeiter
- Ansprechpartner für Datenschutz benannt; Benennung eines Datenschutzbeauftragten, soweit gesetzlich erforderlich

5. Auftragskontrolle

- Schriftliche bzw. in Textform erteilte Weisungen; Dokumentation mündlicher Weisungen
- Verbindliche Auftragsverarbeitungsverträge mit allen Unterauftragsverarbeitern
- Kontrolle der Vertragserfüllung durch Unterauftragsverarbeiter, mindestens jährlich
- Klar geregelter Prozess zur Beendigung des Auftrags einschließlich Rückgabe und Löschung

6. Verfahren bei Verletzungen des Schutzes personenbezogener Daten

- Definierter interner Prozess zur Erkennung, Bewertung, Eskalation und Behandlung von Vorfällen
- Meldung an den Verantwortlichen unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung
- Dokumentation aller Vorfälle einschließlich Auswirkungen und ergriffener Abhilfemaßnahmen
- Nachbereitung und Ableitung von Verbesserungsmaßnahmen

7. Überprüfung

Die technischen und organisatorischen Maßnahmen werden mindestens jährlich überprüft und bei Bedarf angepasst, um ein angemessenes Schutzniveau dauerhaft sicherzustellen. Wesentliche Änderungen werden dokumentiert und den Verantwortlichen unverzüglich in Textform mitgeteilt.

Kontakt für Rückfragen: datenschutz@advertal.de