Anlage 2: Technische und Organisatorische Maßnahmen (TOMs) gemäß Art. 32 DSGVO

Diese Anlage beschreibt die spezifischen Technischen und Organisatorischen Maßnahmen (TOMs) von We Make Marketing.

---

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

Zutrittskontrolle:

- Büroräume: Zugangsbeschränkung durch Schlüssel/Zutrittssystem.
- Server-Infrastruktur: Für die Server-Infrastruktur verweisen wir auf die TOMs unseres Hosting-Partners SpeedIT Solutions UG (haftungsbeschränkt) https://www.speedit.org/, die entsprechende Maßnahmen zum Schutz der Rechenzentren und Serverräume umfassen.

Zugangskontrolle:

- Einsatz von individuellen Benutzernamen und sicheren Passwörtern (mind. 12 Zeichen, Komplexitätsregeln).
- Multifaktor-Authentifizierung (MFA) für kritische Systeme (z.B. interne Verwaltung, FTP, Datenbankzugänge).
- Automatische Sperrung von Zugängen bei Inaktivität.
- Firewalls zum Schutz der internen Netzwerke.
- Verschlüsselung von mobilen Endgeräten und externen Speichermedien.

Zugriffskontrolle:

- Rollen- und Berechtigungskonzepte (least privilege principle) für Mitarbeiter.
- Zugriff auf Kundendaten nur durch befugte Mitarbeiter für die Erfüllung des Auftrags.
- Protokollierung von administrativen Zugriffen auf Systeme und Kundendaten.
- VPN-Nutzung für Fernzugriffe.

Trennungskontrolle:

- Logische Trennung von Kundendaten, sofern technisch möglich und erforderlich.
- Trennung von Entwicklung-, Test- und Produktivumgebungen.

---

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

Weitergabekontrolle:

- Verschlüsselung (TLS/SSL) für die Übertragung von Daten (z.B. Website-Traffic, E-Mail-Kommunikation, FTP-Verbindungen).
- Sichere Dateiübertragungsprotokolle (z.B. SFTP statt FTP).
- Klare Prozesse für den Datenaustausch mit Kunden und Subunternehmern.

Eingabekontrolle:

- Protokollierung von Änderungen an Systemkonfigurationen und Datenbanken.
- Versionierung von Code und Website-Inhalten.

---

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

Verfügbarkeitskontrolle:

- Regelmäßige Datensicherungen (Backups) der Websites und Datenbanken des Auftraggebers sofern mit uns vertraglich vereinbart.
- Redundante Systeme auf Seiten des Hosting-Partners.
- Stromversorgungssicherheit (USV/Notstrom auf Seiten des Hosting-Partners).

Wiederherstellbarkeit:

- Regelmäßige Tests der Backup-Wiederherstellung.
- Notfallkonzepte für den Ausfall wichtiger Systeme.

---

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

Datenschutz-Management:

- Regelmäßige Überprüfung der Einhaltung der internen Datenschutzrichtlinien.
- Regelmäßige Schulung der Mitarbeiter in Datenschutzthemen.
- Dokumentation der Verarbeitungstätigkeiten (Verfahrensverzeichnis).
- Datenschutz-Folgenabschätzungen bei Bedarf.

Auftragsverarbeiter-Kontrolle:

- Sorgfältige Auswahl und regelmäßige Überprüfung von Unterauftragsverarbeitern (z.B. durch Prüfung von deren AVVs, Zertifikaten, Informationen auf deren Webseiten).

Datenschutzbeauftragter:

- Ein Datenschutzbeauftragter ist aktuell nicht gesetzlich vorgeschrieben.

Stand: 30.05.2025 Version 1.0