Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO

Verantwortlicher:
K-KISS GmbH
Juri-Gagarin-Ring 160
99084 Erfurt

Gültig ab: 05.05.2025
Letzte Überprüfung: 05.05.2025

1. Zugangskontrolle

Ziel: Unbefugte Nutzung von Datenverarbeitungssystemen verhindern.
Maßnahmen:

- Passwortschutz gemäß interner Passwort-Richtlinie
- Zwei-Faktor-Authentifizierung für Hosting- und CMS-Zugang

2. Zugriffskontrolle

Ziel: Sicherstellen, dass nur Berechtigte auf Daten zugreifen.
Maßnahmen:

- Rollenkonzept im CMS
- Individuelle Benutzerkonten
- Zugriffprotokollierung auf Server- und Anwendungsebene

3. Weitergabekontrolle

Ziel: Unbefugte Datenweitergabe verhindern.
Maßnahmen:

- Datenübertragung nur über TLS-verschlüsselte Verbindungen (HTTPS, SFTP)
- Abschluss von Auftragsverarbeitungsverträgen mit Dritten
- Verschlüsselte E-Mail-Kommunikation bei sensiblen Daten

4. Eingabekontrolle

Ziel: Nachvollziehbarkeit von Änderungen an Daten sicherstellen.
Maßnahmen:

- Protokollierung von Login-Vorgängen und Datenänderungen
- Änderungsdokumentation in CMS und Datenbank
- Nur benannte Administratoren mit Berechtigung zur Datenänderung

5. Auftragskontrolle

Ziel: Kontrolle bei externer Datenverarbeitung.
Maßnahmen:

- Schriftliche Verträge mit Auftragsverarbeitern gem. Art. 28 DSGVO
- Auswahl nach DSGVO-Konformität (z. B. Standardvertragsklauseln bei US-Anbietern)
- Regelmäßige Prüfung der technischen und organisatorischen Maßnahmen der Auftragsverarbeiter

6. Verfügbarkeitskontrolle

Ziel: Schutz gegen zufällige Datenverluste oder -zerstörung.
Maßnahmen:

- Tägliche, automatisierte Backups
- Backups werden verschlüsselt und georedundant gespeichert

7. Trennungsgebot

Ziel: Sicherstellen, dass Daten für unterschiedliche Zwecke getrennt verarbeitet werden.
Maßnahmen:

- Getrennte Datenbanken für Kunden- und Analyse-Daten
- Trennung von Test- und Produktivumgebungen
- Keine Weiterverarbeitung zu inkompatiblen Zwecken

8. Verschlüsselung

Ziel: Schutz der Daten bei Speicherung und Übertragung.
Maßnahmen:

- TLS-Verschlüsselung für alle Datenübertragungen
- Verschlüsselung von sensiblen Daten im Ruhezustand
- Verwendung sicherer Hashing-Verfahren für Passwörter

9. Datenschutz durch Technikgestaltung & datenschutzfreundliche Voreinstellungen

Ziel: Umsetzung der Datenschutzgrundsätze bei der Gestaltung von Systemen.
Maßnahmen:

- Cookie-Banner mit Opt-In-Verfahren
- Deaktivierung aller nicht notwendigen Dienste vor Einwilligung
- Datensparsame Gestaltung von Formularen