WINTER
DIGI SVS & STEUERN
Präzise Richtung, klare Zukunft – digital berechnet.

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

1. Zutrittskontrolle

- Serverbetrieb ausschließlich in professionellen Rechenzentren mit physischem Zutrittschutz.
- Eigene Arbeitsumgebung ist nur durch berechtigte Personen zugänglich (Schlüssel, Zutrittskontrolle).
- Keine lokalen Server oder Datenträger mit sensiblen Daten außerhalb gesicherter Infrastruktur.

2. Zugangskontrolle

- Benutzerkonten mit individuellen Anmeldeinformationen.
- Starke Passwortrichtlinien.
- Automatische Sitzungszeitlimits.

3. Zugriffskontrolle

- Rollen- und Berechtigungskonzept innerhalb der SaaS-Plattform.
- Zugriff auf produktive Systeme nur für den Administrator (Auftragnehmer selbst).
- Logging und Monitoring von administrativen Zugriffen.

4. Weitergabekontrolle

- Datenübertragungen ausschließlich über verschlüsselte Kanäle (HTTPS/TLS, SFTP).
- Keine Weitergabe an Dritte ohne schriftliche Weisung des Auftraggebers.

5. Eingabekontrolle

- Protokollierung relevanter Änderungen in der Anwendung (Protokollierung).
- Benutzerbezogene Authentifizierung bei allen administrativen Tätigkeiten.
- Regelmäßige Kontrolle und Auswertung von Systemlogs.

6. Auftragskontrolle

- Keine Auftragsdatenverarbeitung im Sinne von Art. 28 Abs. 3 lit. b DSGVO ohne entsprechende Weisung des Auftraggebers.

7. Verfügbarkeitskontrolle

- Wöchentliche automatische Backups der Kundendaten.
- Backups werden verschlüsselt gespeichert.
- Notfallplan zur Wiederherstellung bei Systemausfall.

8. Trennungsgebot

- Logische Mandantentrennung in der SaaS-Anwendung.
- Keine Vermischung von Test- und Produktivdaten.

9. Datenschutzmanagement & Kontrolle

- Regelmäßige Überprüfung der Sicherheitsmaßnahmen.
- Sofortige Meldung von Datenschutzvorfällen an Auftraggeber nach Art. 33 DSGVO.
- Verwendung ausschließlich von Hostingpartnern mit ISO 27001- oder gleichwertiger Zertifizierung.

Die getroffenen Maßnahmen stellen sicher, dass personenbezogene Daten gemäß Art. 32 DSGVO durch geeignete technische und organisatorische Maßnahmen geschützt sind. Die Maßnahmen werden regelmäßig überprüft und an den Stand der Technik angepasst.