

## Anlage 2 – Technische und organisatorische Maßnahmen

Die Auftragsverarbeiterin hat ein Informationssicherheitsmanagementsystem (ISMS) implementiert und ist nach ISO/IEC 27001 zertifiziert. Die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen (TOM) dienen dem Schutz der im Auftrag verarbeiteten personenbezogenen Daten und werden unter Berücksichtigung des jeweiligen Schutzbedarfs, des Stands der Technik sowie der identifizierten Risiken umgesetzt, regelmäßig auf ihre Wirksamkeit überprüft und bei Bedarf angepasst.

### Sicherheitskonzept der Auftragsverarbeiterin

#### Sicherheitsmanagement

Die Informationssicherheit wird durch ein risikobasiertes ISMS gesteuert. Hierzu gehören insbesondere:

- regelmäßige Bewertung und Behandlung von Informationssicherheitsrisiken,
- verbindliche Sicherheitsrichtlinien und interne Sicherheitsprozesse,
- Überwachung und Behandlung von Sicherheitsvorfällen und Schwachstellen,
- regelmäßige Überprüfung, Bewertung und Verbesserung der Wirksamkeit der Sicherheitsmaßnahmen,
- interne und externe Prüfungen und Audits.

#### Zutrittskontrolle

Unbefugter Zutritt zu Räumlichkeiten und Datenverarbeitungsanlagen wird verhindert durch:

- elektronische oder anderweitig geeignete Zutrittskontrollsysteme,
- individuell vergebene Zutrittsberechtigungen,
- Verwaltung und regelmäßige Überprüfung von Zutrittsberechtigungen,
- Protokollierung bzw. Nachvollziehbarkeit von Besucherzugängen,
- geeignete Maßnahmen zum Schutz der technischen Infrastruktur vor physischen Gefahren.

## Zugriffskontrolle

Unbefugter Zugriff auf Daten wird verhindert durch:

- rollenbasiertes Berechtigungskonzept
- individuelle Benutzerkonten
- regelmäßige Überprüfung von Berechtigungen
- Passwort-Richtlinie und Multi-Faktor-Authentifizierung
- Protokollierung sicherheitsrelevanter Zugriffe

## Weitergabekontrolle

Unbefugte Kenntnisnahme bei Übertragung oder Transport wird verhindert durch:

- verschlüsselte Datenübertragung
- VPN für externe Zugriffe
- Beschränkung des Datenzugriffs auf autorisierte Empfänger\*innen
- Protokollierung von Übermittlungsvorgängen, soweit erforderlich

## Eingabekontrolle

Nachträglich nachvollziehbar sind Eingabe, Änderung und Löschung durch:

- individuelle Benutzerkennungen
- Protokollierung sicherheitsrelevanter Änderungen
- Rechtekonzept für administrative und fachliche Änderungen

## Auftragskontrolle

Datenverarbeitung erfolgt nur auf Weisung durch:

- vertraglich dokumentierte Weisungen
- geregelte Prozesse zur Auftragsbearbeitung
- Verpflichtung der Beschäftigten auf Vertraulichkeit
- Kontrolle von Unterauftragnehmer\*innen

## Verfügbarkeitskontrolle

Schutz vor Verlust und Zerstörung erfolgt durch:

- Backup- und Restore-Konzept
- regelmäßige Datensicherungen
- Notfall- und Wiederherstellungsprozesse

## Trennungsgebot

Daten unterschiedlicher Zwecke werden getrennt verarbeitet durch:

- logische Mandantentrennung
- getrennte Test- und Produktionsumgebungen
- Berechtigungskonzept zur Zwecktrennung

## Sicherheitsmaßnahmen nach Vertragsbeendigung bzw. Beendigung des Auftragsverhältnisses:

Nach Beendigung des Auftrags werden personenbezogene Daten nach Weisung des\*der Auftraggeber\*in gelöscht oder zurückgegeben; gesetzliche Aufbewahrungspflichten bleiben unberührt.