# Anlage 3: Technisch-organisatorische Maßnahmen

Für die Bereitstellung der venabo-Software im Rechenzentrum gelten zudem die TOMs der Hetzner GmbH
https://www.hetzner.com/AV/TOM.pdf

## M.1 Maßnahmen zur Vertraulichkeit

### M.1.1 Beschreibung der Zutrittskontrolle:

- Alarmanlage - Einsatz einer Einbruchmeldeanlage, Sicherheitsdienst
- Bewegungsmelder - Bewegungsmelder
- Empfang - Besucherkontrolle am Empfang
- Manuelles Schließsystem - Manuelles Schließsystem mit Schließzylinder
- Schlüsselverwaltung - Schlüsselregelung mit Dokumentation der Schlüssel mit Sicherheitsschlössern und entsprechende Besitznachweise
- Videoüberwachung - Videoüberwachung der Zugänge

### M.1.2 Beschreibung der Zugangskontrolle:

- Authentifikation mit Benutzer + Passwort - Authentifikation mit Benutzer + Passwort sowie 2FA, sofern möglich
- Benutzerberechtigungen - Benutzerberechtigungen verwalten (z.B. bei Eintritt, Änderung, Austritt)
- Firewall - Einsatz von Firewalls zum Schutz des Netzwerkes
- Sorgfältige Personalauswahl - Sorgfältige Auswahl von Reinigungspersonal
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren

### M.1.3 Beschreibung der Zugriffskontrolle:

- Berechtigungskonzept - Erstellen und Einsatz eines Berechtigungskonzepts
- Datenlöschung - Sichere Löschung von Datenträgern vor deren Wiederverwendung
- Passwortlichtlinien - Passwortrichtlinie inkl. Länge, Komplexität und Wechselhäufigkeit
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren

**M.1.4 Beschreibung der Weitergabekontrolle:**

- E-Mail-Verschlüsselung - E-Mail-Verschlüsselung mit Portal-Zugriff
- SSL / TLS Verschlüsselung - Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet

**M.1.5 Beschreibung des Trennungsgebots:**

- Logische Mandantentrennung - Logische Mandantentrennung (softwareseitig)
- Produktiv- und Testsystem - Trennung von Produktiv- und Testsystem

**M.1.6 Beschreibung der Pseudonymisierung:**

Eine Pseudonymisierung macht bei denen im Rahmen der Auftragsverarbeitung verarbeiteten personenbezogenen Daten keinen Sinn. Zudem hat der Auftraggeber über die Notwendigkeit einer Pseudonymisierung zu entscheiden und diese bei Bedarf umzusetzen.

**M.1.7 Beschreibung der Verschlüsselung:**

- Übertragung - Verschlüsselte Datenübertragung (z.B. E-Mailverschlüsselung nach S/Mime, VPN, verschlüsselte Internetverbindungen mittels TLS/SSL)

## M.2 Maßnahmen zur Integrität

**M.2.1 Beschreibung der Eingabekontrolle:**

- Personalisierte Benutzernamen - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Zugriffsrechte - Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.

## M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

**M.3.1 Beschreibung der Verfügbarkeitskontrolle:**

- Antivirensoftware - Einsatz von Antivirensoftware zum Schutz vor Malware
- Backup- und Recoverykonzept - Backup- und Recoverykonzept vorhanden
- Feuerlöschgeräte - Feuerlöschgeräte in Serverräumen
- Klimaanlage - Klimaanlage in Serverräumen

- Redundante Datenhaltung - Redundante Datenhaltung (z.B. gespiegelte Festplatten, RAID 1 oder höher, gespiegelter Serverraum)
- Unterbrechungsfreie Stromversorgung - (USV) Unterbrechungsfreie Stromversorgung

**M.3.2 Beschreibung der raschen Wiederherstellbarkeit:**

- Datenwiederherstellungen - Regelmäßige und dokumentierte Datenwiederherstellungen

## M.4 Weitere Maßnahmen zum Datenschutz

**M.4.1 Beschreibung der Auftragskontrolle:**

- Auswahl - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- AV-Vertrag - Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO.

**M.4.2 Beschreibung des Managementsystems zum Datenschutz:**

- DSB - Benennung eines Datenschutzbeauftragten
- Schulung - Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen.
- Verpflichtung - Verpflichtung auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO