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 [umgesetzt]
- Bewegungsmelder - Bewegungsmelder [umgesetzt]
- Empfang - Besucherkontrolle am Empfang [umgesetzt]
- Manuelles Schließsystem - Manuelles Schließsystem mit Schließzylinder [umgesetzt]
- Schlüsselverwaltung - Schlüsselregelung mit Dokumentation der Schlüssel mit Sicherheitsschlössern und entsprechende Besitznachweise [umgesetzt]
- Videoüberwachung - Videoüberwachung der Zugänge [umgesetzt]

M.1.2 Beschreibung der Zugangskontrolle:

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

M.1.3 Beschreibung der Zugriffskontrolle:

- Berechtigungskonzept - Erstellen und Einsatz eines Berechtigungskonzepts [umgesetzt]
- Datenlöschung - Sichere Löschung von Datenträgern vor deren Wiederverwendung [umgesetzt]
- Einsatz von Aktenvernichtern - Einsatz von Aktenvernichtern (min. Sicherheitsstufe 3 und Schutzklasse 2) [umgesetzt]
- Einsatz von Dienstleistern - Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit DIN 66399 Zertifikat) [umgesetzt]

- Passwortlichtlinien - Passwortrichtlinie inkl. Länge, Komplexität und Wechselhäufigkeit [umgesetzt]
- Sichere Aufbewahrung - Sichere Aufbewahrung von Datenträgern [umgesetzt]
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren [umgesetzt]
- Verschlüsselung von Smartphones - Verschlüsselung von Smartphones mit dem Stand der Technik entsprechenden Verfahren [umgesetzt]

M.1.4 Beschreibung der Weitergabekontrolle:

- E-Mail-Verschlüsselung - E-Mail-Verschlüsselung mit Portal-Zugriff [umgesetzt]
- SSL / TLS Verschlüsselung - Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet [umgesetzt]
- VPN-Tunnel - Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen [umgesetzt]

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung - Logische Mandantentrennung (softwareseitig) [umgesetzt]
- Netzwerksegmentierung - Trennung von Netzwerken / Netzsegmenten; mind. Trennung vom Gäste- und Produktivnetzwerk [umgesetzt]
- Produktiv- und Testsystem - Trennung von Produktiv- und Testsystem [umgesetzt]

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:

- Speicherung - Verschlüsselte Datenspeicherung (z.B. Dateiverschlüsselung nach AES256 Standard) [umgesetzt]
- Übertragung - Verschlüsselte Datenübertragung (z.B. E-Mailverschlüsselung nach S/Mime, VPN, verschlüsselte Internetverbindungen mittels TLS/SSL) [umgesetzt]

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) [umgesetzt]
- Protokollierung - Protokollierung der Eingabe, Änderung und Löschung von Daten [umgesetzt]
- Zugriffsrechte - Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe. [umgesetzt]

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Antivirensoftware - Einsatz von Antivirensoftware zum Schutz vor Malware [umgesetzt]
- Auslagerung Datensicherung - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort [umgesetzt]
- Backup- und Recoverykonzept - Erstellen eines Backup- und Recoverykonzepts [umgesetzt]
- Feuerlöschgeräte - Feuerlöschgeräte in Serverräumen [umgesetzt]
- Klimaanlage - Klimaanlage in Serverräumen [umgesetzt]
- Redundante Datenhaltung - Redundante Datenhaltung (z.B. gespiegelte Festplatten, RAID 1 oder höher, gespiegelter Serverraum) [umgesetzt]
- Schutzsteckdosenleisten - Schutzsteckdosenleisten in Serverräumen [umgesetzt]
- Unterbrechungsfreie Stromversorgung - (USV) Unterbrechungsfreie Stromversorgung [umgesetzt]

M.3.2 Beschreibung der raschen Wiederherstellbarkeit:

- Datenwiederherstellungen - Regelmäßige und dokumentierte Datenwiederherstellungen [umgesetzt]

M.4 Weitere Maßnahmen zum Datenschutz

M.4.1 Beschreibung der Auftragskontrolle:

- Auswahl - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) [umgesetzt]
- AV-Vertrag - Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO. [umgesetzt]
- Laufende Überprüfung - Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten [umgesetzt]

M.4.2 Beschreibung des Managementsystems zum Datenschutz:

- Audits - Durchführung regelmäßiger interner Audits [umgesetzt]
- DSB - Benennung eines Datenschutzbeauftragten [umgesetzt]
- Managementsystem Datenschutz - Managementsystem zum Datenschutz (z.B. in Anlehnung an ISO 27701) [umgesetzt]
- Schulung - Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen. [umgesetzt]
- Software Voreinstellungen - Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO) [umgesetzt]
- Verpflichtung - Verpflichtung auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 DS-GVO [umgesetzt]