1: Technische und Organisatorische Maßnahmen

1) Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Office

- Manuelles Schließsystem mit Sicherheitsschlössern
- Schlüsselregelung
- Dokumente befinden sich in versperrten Kästen, zu denen nur ausgewählte Mitarbeiter einen Schlüssel besitzen
- Sorgfältige Auswahl der Reinigungskraft

2) Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Rechenzentrum – VABO-N Manager: Backoffice, Mobile App

- Server befinden sich in der EU und USA
- Benutzerberechtigungsverwaltung durch IT Office Dienstleister
- Passwortvergabe/ Passwortregeln durch IT Office Dienstleister
- PC: Authentifikation mit Benutzer + Passwort
- Einsatz von Anti-Viren Software
- Einsatz von Firewalls
- Einsatz von Mobile Device Management durch IT Office Dienstleister
- Einsatz von VPN-Technologie für Firmen Laptops
- Gehäuseverriegelung der Standrechner

3) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Einsatz von Aktenvernichtern
- Verwaltung der Benutzerrechte durch externe Systemadministratoren durch IT Office und den Dienstleister Auftragsabwicklung
- Benutzerprofile mit Lese-, Verarbeitungs-, Änderungsrechten
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.
- Anzahl der Administratoren auf das „Notwendigste“ reduziert

4) **Weitergabekontrolle**
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Dokumente werden höchstpersönlich dem Steuerberater übermittelt
- E-Mail Teilverschlüsselung
- VPN Tunnel

5) **Eingabekontrolle**
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen und Passwörtern

6) **Auftragskontrolle**
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere Datensicherheit)
- Schriftliche Weisung an den Auftragnehmer – Auftragsdatenverarbeitungsvertrag i.S.d. § 11 Abs.2 BDSG
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis §5 BDSG
- Vertragsstrafen bei Verstößen

7) **Verfügbarkeitskontrolle**
Maßnahmen, für die Gewährleistung, dass personenbezogene Daten gegen zufällige Zerstörung und Verlust geschützt sind.

- Aufbewahrung von Datensicherung an einem ausgelagerten Ort
- Backup- & Recovery Konzept Office Server
- Separates Testsystem der Datenwiederherstellung
- Serverräume nicht unter sanitären Anlagen

8) Trennungsgebot

Maßnahmen, für die Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Getrennte Speicherung auf gesonderten Systemen und Datenträgern
- Trennung von Produktiv- und Test-System
- Logische Mandantentrennung
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
  Festlegung von Datenbankrechten
- Datenbankrechte bei Serverzugriff und Backoffice Bevollmächtigungen