Technische und organisatorische Maßnahmen Verein

M.1 Maßnahmen zur Vertraulichkeit

Zu M.1.1 Beschreibung der Zutrittskontrolle:

- Der Verein trägt dafür Sorge, dass Unbefugte keinen Einblick oder Zugriff auf Datenverarbeitungsgeräte (z.B. PCs, Laptops, Monitore, Drucker, etc.) erlangen können, auf denen Daten der Mitglieder verarbeitet oder ausgegeben werden.
- Insbesondere muss eine Verarbeitung der Mitgliederdaten im öffentlichen Raum (ÖNV, Flugzeug, Internet-Café etc.) vermieden werden

Zu M.1.2 Beschreibung der Zugangskontrolle:

- Der zur Verarbeitung benutzte Rechner ist durch Benutzerkonto und Passwort geschützt
- Das Benutzerkonto ist so einzurichten, dass keine lokalen Administrationsrechte bestehen. Hierfür ist in der Benutzerverwaltung ein separates Administrationskonto zu erstellen. Durch diese Maßnahmen soll Angreifern erschwert werden, die Konfiguration des Rechners zu ändern und Schadsoftware zu installieren.
- Passwortlänge sollte mindestens 8 Stellen lang sein, besser über 10 Stellen
- Trivialpasswörter sind durch die Eingabe von Ziffern, Groß- und Kleinbuchstaben und Sonderzeichen zu vermeiden
- In den Passwörtern sind weder Wörter noch Ziffern- oder Zeichenfolgen enthalten, da diese mit entsprechenden Analysetools leicht decodiert werden können
- Passwörter sollten regelmäßig gewechselt werden außer, man setzt moderne Authentifizierungsmethoden ein (z.B. Hash and Salt-, Zwei Faktor-Authentifizierung)
- Passwörter müssen geheim gehalten werden

Zu M.1.3 Beschreibung der Zugriffskontrolle:

- Es werden Maßnahmen ergriffen, die verhindern, dass Unbefugte Zugriff auf die Mitgliederdaten erlangen können, z.B.
- Passwort geschützte Rechner für den Zugriff auf die VDST Mitgliederdatenbank und Daten, die aus der Mitgliederdatenbank heruntergeladen wurden
- Zugriff darf nur für Personen ermöglicht werden, die aufgrund ihrer Funktion im Verein mit der Verarbeitung der Mitgliederdaten betraut wurden

Zu M.1.4 Beschreibung der Weitergabekontrolle:

- Die Übertragung von Daten die aus der Mitgliederdatenbank heruntergeladen wurden per E-Mail erfolgt nur verschlüsselt (z.B. Verteilung der Mitgliederliste an Vorstände und Funktionäre). Dies kann z.B. durch eine passwortgeschützte Datei erfolgen.
- Der Versand oder Transport der oben genannten Daten auf mobilen Datenträger (USB-Sticks, Speicherkarten etc.) erfolgt nur verschlüsselt
- Der Zugriff bei Fernwartungs- bzw. Serviceleistungen auf Datenverarbeitungsanlagen des Vereins auf den o.g. Daten verarbeitet werden erfolgt nur über sicherer verschlüsselte Verbindungen

- Drahtlose Übertragung (z.B. WLAN) von personenbezogenen Daten der Mitglieder erfolgt nur verschlüsselt (die Verschlüsselung wird immer an den Stand der Technik angepasst))

Zu M.1.5 Beschreibung des Trennungsgebots:

- Bei der Verarbeitung wird sichergestellt, dass eine „Vermischung“ mit anderen personenbezogenen Daten und auch unbefugte Zugriffe Dritter (auch versehentlich) nicht möglich sind.

Zu M.1.6 Beschreibung der Pseudonymisierung:

- Trifft nicht zu

Zu M.1.7 Beschreibung der Verschlüsselung:

- Werden Mitgliederdaten aus der VDST Mitgliederdatenbank auf mobilen Geräten (Notebook, externe Datenträger, IPad etc.) gespeichert, müssen die Datenbestände verschlüsselt werden
- Die Weitergabe von Mitgliederdaten per E-Mail darf nur verschlüsselt erfolgen (z.B. verschlüsselte Datei)
- Funkverbindungen (Bluetooth, WLAN) müssen verschlüsselt eingerichtet werden und müssen dem Stand der Technik entsprechen

M.2 Maßnahmen zur Integrität

Zu M.2.1 Beschreibung der Eingabekontrolle:

- Wenn möglich, sollte die Zugriffe bei der Verarbeitung der Mitgliederdaten nachvollziehbar sein

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

Zu M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Es sind entsprechenden Datensicherungsverfahren (z.B. Sicherung auf ein USB-Laufwerk) eingerichtet, wenn der Verlust der Daten sich nachteilig für die Mitglieder auswirken könnte
- Die Sicherungsdaten werden nicht gemeinsam mit den Originaldaten aufbewahrt, damit diese unabhängig vor Verlust geschützt sind.
- Es wurden Schutzmaßnahmen getroffen, die Angriffe durch unbefugte Dritte verhindern (z.B. Virenschutz, Firewall)
- Es werden keine externen Geräte (Smartphones oder Tabletts) mit SIM-Karte im gleichen Netz betrieben, in dem die Mitgliederverwaltung und die Übertragung zum VDST durchgeführt wird

Zu M.3.2 Beschreibung der raschen Wiederherstellbarkeit:

- Es bestehen Pläne, wie fachkundige Dritte die notwendigen Daten, die aus der VDST Mitgliederverwaltung heruntergeladen wurden, wieder herstellen können

M.4 Weitere Maßnahmen zum Datenschutz

Zu M.4.1 Beschreibung der Auftragskontrolle:

- Sorgfältige Auswahl von Dienstleistern
- Überprüfung vor der Beauftragung, ob die Vorgaben des Datenschutzes eingehalten werden
- Vertrag zur Auftragsdatenverarbeitung gem. Art. 28 DS-GVO mit Regelungen zu den Rechten und Pflichten des Auftragnehmers
- Regelmäßige Überprüfung der Dienstleister

Zu M.4.2 Beschreibung des Managementsystems zum Datenschutz:

- Ein Konzept, wie die oben aufgeführten Maßnahmen umgesetzt werden, sollte dokumentiert und zur Absicherung des Vereinsvorstandes sicher aufbewahrt werden
- Alle Dokumentationen, Verfahrensbeschreibung, Auftragsdatenverarbeitungsvorgänge werden in einem übersichtlichen System verwaltet