Technische und organisatorische Maßnahmen VDST

M.1 Maßnahmen zur Vertraulichkeit

Zu M.1.1 Beschreibung der Zutrittskontrolle:

- Räume, in denen Daten der Mitglieder verarbeitet oder gespeichert werden, können nicht betreten werden. Hier sind entsprechende Zutrittskontrollsysteme (Schlüssel, Chipkarte) eingesetzt.
- Datenverarbeitungsgeräte (Monitore, Drucker, etc.) auf denen Daten der Mitglieder verarbeitet oder ausgegeben werden sind so aufgestellt, dass keinen Einblick oder Zugriff durch Unbefugte möglich ist.

Zu M.1.2 Beschreibung der Zugangskontrolle:

- Passwortregeln sind in einer allgemein gültigen Policy geregelt
- Pro Benutzer ein entsprechendes Benutzerkonto
- Passwortlänge von mindestens 16 Stellen
- Verhinderung von Trivialpasswörtern durch die Pflicht zur Eingabe von Ziffern, Groß- und Kleinbuchstaben sowie Sonderzeichen
- Werden Daten von Mitgliedern auf mobilen Datenträgern gespeichert, werden diese verschlüsselt.

Zu M.1.3 Beschreibung der Zugriffskontrolle:

- Verwaltung von Berechtigungen mit differenzierten Berechtigungen
- Gruppenkonzept
- Dokumentation von Berechtigungen

Zu M.1.4 Beschreibung der Weitergabekontrolle:

- Die Übertragung von sensiblen personenbezogenen Daten per Email darf nur verschlüsselt erfolgen
- Die Verbindung zu und von den Netzen des VDST darf nur verschlüsselt erfolgen
- Der Versand oder Transport von personenbezogenen Daten auf mobilen Datenträger (Sicherungsbänder, USB-Sticks, Speicherkarten etc.) darf nur verschlüsselt erfolgen
- Der Zugriff bei Fernwartungs- bzw. Serviceleistungen auf Datenverarbeitungsanlagen des VDST darf nur über sicherer verschlüsselte Verbindungen erfolgen
- Drahtlose Übertragung (WLAN) von personenbezogenen Daten der Mitglieder darf nur verschlüsselt erfolgen

Zu M.1.5 Beschreibung des Trennungsgebots:

- Vereinsbezogene logische Datentrennung
- Physikalische Trennung durch Speicherung in einem externen Rechenzentrum
- Zugriffsberechtigungen

Zu M.1.6 Beschreibung der Pseudonymisierung:

- Es gibt derzeit keine Anwendung, die eine Pseudonymisierung notwendig macht

Zu M.1.7 Beschreibung der Verschlüsselung:

- Verschlüsselte Datenübertragung (VPN, verschlüsselte Internetverbindungen via TLS/SSL)

M.2 Maßnahmen zur Integrität

Zu M.2.1 Beschreibung der Eingabekontrolle:

- Zugriffsrechte
- Systemseitige Protokollierungen von Logins
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

Zu.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Einrichtung von entsprechenden Datensicherungsverfahren wie z.B. Bandsicherung, Datenspiegelung, Snapshot
- Räumliche Trennung der Sicherungsdaten. Diese muss so gestaltet sein, dass auch Katastrophen-Ereignisse nicht zum Verlust von Daten führen.
- Einsatz von unterbrechungsfreien Stromversorgungen, die gewährleistet, dass Daten nicht während der Speicherung oder Übertragung verloren gehen.
- Einrichtung von Schutzmaßnahmen, die Angriffe durch unbefugte Dritte verhindern (Virenschutz, Firewall, Spyware Detection etc.)

Zu M.3.2 Beschreibung der raschen Wiederherstellbarkeit:

- IT-Notfallpläne und Wiederanlaufpläne
- Regelmäßige Datenwiederherstellungen

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
- Benennung eines Datenschutzbeauftragten (sofern gesetzlich gefordert)

Zu M.4.2 Beschreibung des Managementsystems zum Datenschutz:

- IT-Sicherheitskonzept
- Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen
- Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO)
- Durchführung regelmäßiger interner Audits durch den DSB
- Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (audatis MANAGER)