Technisch-Organisatorische Maßnahmen zum Schutz der Daten

Verantwortliche/r:
Auftragsverarbeiter/in:

Bereich	Maßnahme	verantwortlich
Grundsätzlich	Der Verein trifft technische wie organisatorische Maßnahmen, die die Vertraulichkeit, Integrität und Verfügbakriet personenbezogener Daten sicherstellen.	Vereinsleitung
Allgemeine Sicherheit	Der selbstständige/unbeaufsichtigte Zugang zu den Vereinsräumlichkeiten ist ausschließlich Mitarbeiter/innen und einzelnen Vereinsfunktionär/innen gestattet. Andere Personen (Vereinsmitglieder, Besucher/innen,...) werden jedenfalls von Vereinsmitarbeiter/innen begleitet - der alleinige Aufenhalt dieser Personen in den Vereinsräumlichkeiten darf nur in Räumen ohne Zugang zu personenbezogenen Daten gestattet werden. Die Zugänglichkeit von personenbezogenen Daten (elektronisch wie physisch) für Dritte ist abzusichern (keine herumliegende Akten, versperrte Kästen, versperrte Räume, PCs in abgesichertem Zustand...).	Vereinsleitung
IT-Sicherheit Verein	Die Aufstellung des Servers/zentralen Datenspeichers hat entsprechend sicher zu erfolgen Den Zugang zum Netzwerk über das Internet entpsrechend zu sichern WLAN Zugänge absichern (mindestens WPA2, Gästenetz und Vereinsnetz müssen getrennt sein) Alle Datenzugänge über segmentierte Zugangsberechtigungen schützen *(z.B. passwortgeschützte Ordner, passwortgeschützter Programmzugang)* Bei Verlassen des Arbeitsplatzes PC-Zugang sperren PCs dürfen nur von autorisierten Personen in Betrieb genommen werden Mobile Endgeräte und Datenträger (USB-Stick) verschlüsseln und regelmäßig löschen Bei Rückgabe von Kopiergeräten auf allfällige integrierte Speicher achten (Festplatte zurückbehalten). Gleiches gilt für alle Geräte mit integrierter Datenspeicherung Aktuelle Servicepacks zeitnah zum Erscheinen installieren *(zB Sicherheits-Updates für Betriebssoftware und Programme)* Virenschutz auf allen Endgeräten installieren und aktuell halten Firewalls (auch der Endgeräte) aktivieren Für E-Mail Transport mindestens "Versand- und Empfangsverschlüsselung" konfigurieren Logs sind regelmäßig auszuwerten Endgeräte von Dritten keinen Zugang zum Vereinsnetz geben "Fremde" Datenträger vor "Anschließen" qualifiziert überprüfen Eine Datensicherung inklusive regelmäßiger Verifizierung einrichten Sicherungsdatenträger verschlüsseln und sicher aufbewahren	
Organisatorische Maßnahmen	Aufnahmen bzw. Aufzeichnungen im Rahmen von Veranstaltungen Alle Zugänge zu EDV Systemen als personenbezogene Zugänge Zugangsdaten keinesfalls weitergeben, autorisierte Zugänge nur persönlich verwenden Private E-Mails über den Vereinsaccount - Regelung erforderlich? Alle Vereinsmitrabeiter/innen sowie zugangsberechtigte Vereinsfunktionär/innen über die rechtlichen Grundlagen und erforderlichen Maßnahmen informieren. *Die Richtlinie "Datenschutz / Datensicherheit / Informationssicherheit" unterzeichnen lassen.* Vereinsmitarbeiter/innen und Vereinsfunktionär/innen regemäßig über Datenschutz schulen jede Weitergabe von personenbezogenen Daten ist vom Leitungsorgan des Vereins zu autorisieren	

falls von qualifizierten Vereinsmitarbeiter/innen temporär Daten z.B: zu Veranstaltungen für Auswertungen auf "eigenen" Laptops verarbeitet werden, gelten hinsichtlich Datenschutztechnologie dieselben Voraussetzungen wie für Vereins-Geräte (Verschlüsselung, geschützter Zugang, Virenschutz,...). Bei AUsscheiden des/der Mitarbeiters/in sind sämtliche "Vereins-Daten" vom z.B. eigenen Laptop sofort sicher und vollständig zu löschen und dies dem Verein schriftlich zu bestätigen.

E-Mails an mehr als 5 Empfänger NICHT mit offenen Zieladressen versenden (wenn dann bcc)

Speziell beim Handling von E-Mails und generell im Bereich mit direkter Verbindung zum Internet ist im Hinblick auf eine Vielzahl spezieller Risiken (Viren, Trojaner, Phishing,..) höchste Sorgfalt erforderlich. Trotz vorhandener Schutzeinrichtungen ist jedenfalls eine vernünftige Beurteilung z.B. "der zu öffnenden E-Mail, des übermittelten Attachments" erforderlich

Papierdokumente mit personenbezogenen Daten müssen vor Entsorgung "geshreddert" werden. Alternativ ist eine Entsorgung über Spzialunternehmen möglich.

Vor der Entsorgung, Verkauf,... von Datenträgern (gilt auch für PCs, alle Arten von Mobilgeräten / mobilen Speichermedien) ist eue qualifizierte Datenlöschung vorzunehmen

Vorbereitung einer Checkliste zum Umgang mit Zwischenfällen (bis hin zu DataBreach Vorfällen), jedenfalls aber unverzüglich das Leitungsorgan informieren

Vor Weitergabe von personenbezogenen Daten an nicht-Berechtigte Dritte mit diesen einen Vertrag zur Auftragsdatenvereinbarung abschließen

Eine Übersicht über die abgeschlossenen Auftragsverarbeitungsvereinbarungen erstellen und aktull halten