

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

Folgende Maßnahmen sind am Vereinsstandort, A-1080 Wien, Josefstädterstraße 72, umgesetzt sowie von etwaig in Anspruch genommenen Auftragsverarbeitern und/oder von Verantwortlichen im Sinne der DSGVO an deren Standorten umgesetzt:

## **Vertraulichkeit:**

- **Zutrittskontrolle:**  
Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch Sicherheitsschlüssel mit Schlüsselregelung, elektrische Türöffner, Alarmanlagen und Festlegung von Sicherheitszonen.
- **Zugangskontrolle:**  
Schutz vor unbefugter Systembenutzung durch Kennwörter, einschließlich entsprechender Policy, ggf. Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern, Einsatz von VPN-Technologie.
- **Zugriffskontrolle:**  
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten.
- **Daten-Klassifikationschema:**  
Gemäß ges. Verpflichtungen bzw. Selbsteinschätzung in geheim/vertraulich/intern/öffentlich.

## **Integrität:**

- **Weitergabekontrolle:**  
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung, VPN und ggf. elektronischer Signatur.
- **Eingabekontrolle:**  
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch Protokollierung, Dokumentenmanagement.

## **Verfügbarkeit und Belastbarkeit:**

- **Verfügbarkeitskontrolle:**  
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung, regelmäßige Updates der Systeme, Virenschutz, Firewall, Security Checks auf Infrastruktur- und Applikationsebene, mehrstufiges Sicherheitskonzept mit Auslagerung der Sicherungen an einen externen Standort, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern.

## **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung:**

- **Überprüfung der Einhaltung von Informationssicherheit:**  
Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen, Incident-Response-Management und datenschutzfreundliche Voreinstellungen.
- **Auftragskontrolle:**  
Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Verantwortlichen durch eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl der Auftragsverarbeiter, Vorabüberzeugungspflicht und Nachkontrollen.