**Diese Checkliste dient der Kontrolle der technischen und organisatorischen Maßnahmen im Bereich Datenschutz im Verein und stellt die Mindestanforderungen dar. Bitte zutreffendes mit (Ja) ankreuzen und falls nicht zutreffend (Nein) entsprechende Maßnahmen einleiten. Sollten einige Maßnahmen nicht anwendbar sein, wie z.B. keine Nutzung einer Cloud oder VPN usw. mit NR (nicht relevant) ankreuzen.**

1. Zugangskontrolle

Die Zugangskontrolle soll verhindern, dass Unbefugte Zugang zu Verarbeitungsanlagen erhalten, mit denen die Verarbeitung durchgeführt wird.

|  |  |  |  |
| --- | --- | --- | --- |
| **Umsetzung** | **Ja** | **Nein** | **NR** |
| Das Vereinsbüro ist abgeschlossen. |  |  |  |
| Den Schlüssel zum Vereinsbüro haben nur die autorisierte Personen |  |  |  |
| Sensible Daten (Tauglichkeitszeugnisse, Personalunterlagen, Eigenerklärungen usw.) sind zusätzlich in einem (*abgeschlossenen*) Schrank abgelegt, Zugang haben autorisierte Personen |  |  |  |
| Sorgfältige Auswahl Reinigungspersonal |  |  |  |
| *Sonstiges…* |  |  |  |

1. Zugriffs- und Benutzerkontrolle

Die Zugriffskontrolle soll gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

|  |  |  |  |
| --- | --- | --- | --- |
| **Umsetzung** | **Ja** | **Nein** | **NR** |
| Vereinscomputer sind Passwortgeschützt |  |  |  |
| Zugriff haben nur der Ausschuss bzw. autorisierte Personen |  |  |  |
| Verwaltung der Rechte durch gesetzlichen Vertreter (Präsident) oder Vertreter |  |  |  |
| Benutzungsberechtigungskonzept bei Onlinedatenbank zur Mitgliederverwaltung (durch Voreinstellung des Softwareherstellers) |  |  |  |
| Benutzungsberechtigungskonzept bei Steuererklärungssoftware |  |  |  |
| Benutzungsberechtigungskonzept bei Buchhaltungssoftware |  |  |  |
| Regelmäßiger Passwortwechsel |  |  |  |
| Postfach-Zugriff eingeschränkt (Es haben nur die Personen auf das Postfach Zugriff die für die Besetzung der Position zuständig sind.) |  |  |  |
| Zugriff zur Cloud ist nur mit einem Passwort möglich. Unterschiedliche und sensible Bereiche der Cloud haben jeweils andere Passwörter. |  |  |  |
| Ausscheidende Personen haben keinen Zugriff mehr auf Daten |  |  |  |
| Zugriff des externen Systemadministrators bzw. Technikers ausschließlich zur Wartung und unter Aufsicht |  |  |  |
| *Sonstiges…* |  |  |  |

1. Zuverlässigkeit/Wiederherstellbarkeit

Die Zuverlässigkeit soll gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden. Die Wiederherstellbarkeit soll gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

|  |  |  |  |
| --- | --- | --- | --- |
| **Umsetzung** | **Ja** | **Nein** | **NR** |
| Vereinscomputer verfügt über Antivirenprogramm / Firewall |  |  |  |
| Das Antivirenprogramm wird in regelmäßigen Abständen aktualisiert |  |  |  |
| Daten werden in regelmäßigen Abständen gesichert – Automatisches Backup |  |  |  |
| Datenträger mit Sicherung wird außerhalb des Vereinsbüros aufbewahrt (USB-Stick/externe Festplatte/Cloud) |  |  |  |
| Datenwiederherstellung wird in regelmäßigen Abständen getestet |  |  |  |
| *Mitarbeiter werden bezüglich Viren Emails sensibilisiert* |  |  |  |
| *Sonstiges…* |  |  |  |

1. Datenträgerkontrolle

Die Datenträgerkontrolle soll verhindern, dass Unbefugte Datenträger lesen, kopieren, verändern oder löschen können.

|  |  |  |  |
| --- | --- | --- | --- |
| **Umsetzung** | **Ja** | **Nein** | **NR** |
| Datenträger werden sicher aufbewahrt (Vereinsbüro, Schrank usw.) |  |  |  |
| Notebooks, Handys- bzw. Tablets sind mit Passwort bzw. PIN verschlüsselt. |  |  |  |
| Ordnungsgemäße Vernichtung von Datenträgern (Physische Zerstörung von USB-Sticks, Schreddern von Dokumenten) |  |  |  |
| USB-Sticks sind versperrt bzw. verschlüsselt. |  |  |  |
| *Sonstiges…* |  |  |  |

1. Transportkontrolle und Übertragungskontrolle

Die Transport- und Übertragungskontrolle soll gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

|  |  |  |  |
| --- | --- | --- | --- |
| **Umsetzung** | **Ja** | **Nein** | **NR** |
| Verschlüsselungs-Technologien der Homepage (SSL-Verschlüsselung) |  |  |  |
| Einrichtung von Standleitungen (VPN) beim Fernzugriff auf den Vereinscomputer |  |  |  |
| Bei Weitergabe von USB-Sticks mit Dateien, die persönliche Daten enthalten, sind diese verschlüsselt |  |  |  |
| Anonymisierungsfunktion bei der Onlinedatenbank zur Mitgliederverwaltung (durch Softwarehersteller) |  |  |  |

1. Homework&Office

Hier gelten grundsätzlich dieselben technisch-organisatorischen Maßnahmen wie bereits oben erwähnt. Nachfolgend eine kurze Checkliste

|  |  |  |  |
| --- | --- | --- | --- |
| **Umsetzung** | **Ja** | **Nein** | **NR** |
| Computer Passwortgeschützt |  |  |  |
| Antivirenprogramm installiert |  |  |  |
| Antivirenprogramm aktuell |  |  |  |
| Datensicherung |  |  |  |
| Unterlagen vor Unbefugten geschützt (abgeschlossener Schrank, usw.) |  |  |  |
| Gesichertes W-LAN |  |  |  |
| *Sonstiges* |  |  |  |

Datum: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Unterschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_