

Das VereinsServiceBüro informiert

Technische und organisatorische Schutzmaßnahmen

Laut Artikel 32 und Erwägungsgrund 83 der Datenschutzgrundverordnung müssen Verantwortliche geeignete technische und organisatorische Maßnahmen festlegen, um Daten effektiv zu schützen. Hierzu schreibt die Datenschutzgrundverordnung keine bestimmten Maßnahmen vor. Sie hängen vom Schutzbedarf und weiteren Faktoren ab, wie z.B. dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang sowie den Umständen und Zwecken der Verarbeitung. Auch die Eintrittswahrscheinlichkeit und Schwere des Risikos für Rechte und Freiheiten der betroffenen Person spielen in dieser Abwägung eine Rolle. Für jeden Vorgang der Datenverarbeitung sollte der Verantwortliche im Verein eine Risikobeurteilung vornehmen und erforderliche Vorkehrungen ableiten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten.

Beispiele für technische und organisatorische Schutzmaßnahmen liefert der § 64 BDSG. Er behandelt Anforderungen an die Sicherheit der Datenverarbeitung, welche als Anhaltspunkte genutzt werden können:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste
- Wiederherstellung von und Zugang zu Daten bei einem physischen oder technischen Zwischenfall
- Gewährung der Sicherheit der Verarbeitung durch regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Im Falle einer automatisierten Verarbeitung sind nach Risikobewertung diverse Maßnahmen zu ergreifen, aus den Bereichen Zugangs-, Datenträger-, Speicher-, Benutzer-, Zugriffs-, Übertragungs-, Eingabe- und Transportkontrolle sowie Wiederherstellbarkeit, Zuverlässigkeit, Datenintegrität, Auftrags-, Verfügbarkeitskontrolle sowie Trennbarkeit. Folgende Maßnahmen können Beispiele zu dieser umfangreichen Liste sein – es ist natürlich für Vereine auch auf eine gewisse Verhältnismäßigkeit und die Möglichkeit der Umsetzung zu achten:

1) Zutrittskontrolle

- Schlüsselregelung/Schließsysteme
- Sorgfalt bei Auswahl Reinigungsdienste
- ...

2) Zugangskontrolle

- Eigener Login mit Benutzername + Passwort für jede Person (keine Gruppenbenutzung)
- Richtlinie „Sicheres Passwort“
- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen (eigene E-Mail-Adressen, wie z.B. max.muster@verein.de, die beim Ausscheiden auch wieder deaktiviert werden)
- Automatische Desktopsperre bei Abwesenheit
- ...

3) Zugriffskontrolle

- Aktenshredder
- Minimale Anzahl von Administratoren/Benutzern
- Nur Zugriff auf die unbedingt erforderlichen Daten
- Wegschließen von Papierunterlagen vor Unbefugten

4) Datenträger

- Datensicherung durch externe Datenträger
- Nur Weitergabe der zwingend erforderlichen Daten (Datenminimierung/Datensparsamkeit)

5) Weitergabekontrolle

- Bereitstellung über verschlüsselte Verbindungen (https)
- ...

6) IT-Sicherheitsmanagement

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Virens Scanner und regelmäßige Aktualisierung

7) Notfallmanagement

- Backup von Daten
- Notfallplan: Wer muss verständigt werden? (Datenschutzpannen müssen gegebenenfalls der Aufsichtsbehörde gemeldet werden).

Bei dieser Aufzählung handelt sich lediglich um eine unvollständige Liste möglicher Maßnahmen, welche als Mindestvoraussetzungen zum technischen und organisatorischen Schutz der personenbezogenen Daten zu sehen sind. Weitere Maßnahmen finden Sie [hier](#).

Im World Wide Web sind nicht nur Firmen, Medien und Privatpersonen global vernetzt. Auch Sportvereinen bietet die Digitalisierung von Daten große Vorteile. Damit steigt jedoch nicht nur die Effizienz, sondern auch das Risiko eines Online-Angriffs auf die eingesetzten IT-Systeme.

Bei Bedarf einer zusätzlichen Absicherung bietet die ARAG Sportversicherung ein Angebot zum CyberSchutz. Die neue ARAG CyberSchutz für Sportvereine bewahrt die Handlungsfähigkeit und schützt vor finanziellen Folgen. Weitere Informationen finden Sie [hier](#).

Dies ist jedoch keine Alternative zu den technischen und organisatorischen Schutzmaßnahmen, sondern eine Ergänzung derselben.

Quelle: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Elke Liebrich, Zertifizierte Datenschutzbeauftragte

<https://www.bdsge-externer-datenschutzbeauftragter.de>

Hinweis:

Bitte beachten Sie, dass keinerlei Haftung für die korrekte Anwendung im Einzelfall und Aktualität der Informationen zum Zeitpunkt der Verwendung übernommen werden kann. Die Informationen können insoweit nur Anregungen liefern und sind stets an die individuellen Bedürfnisse **im Einzelfall anzupassen**. Wir empfehlen Ihnen im Einzelfall ergänzend rechtlichen und steuerlichen Rat im Vorfeld einzuholen.

Württembergischer Landessportbund e.V.
VereinsServiceBüro
Fritz-Walter-Weg 19
70372 Stuttgart
Tel. 0711/28077-125
E-Mail: info@wlsb.de
Internet: www.wlsb.de



Stand: 30.01.2019