Checklisten und Fragebögen zur Umsetzung des Datenschutzes im Sportverein

Bei der Umsetzung des Datenschutzes handelt es sich um einen fortlaufenden Prozess zur Verbesserung. Cybersicherheit und Datenschutzsensibilisierung sind niemals abgeschlossen, sondern ein Prozess, der ständig verbessert werden sollte.

Hinweis: Folgende Fragen und Checklisten geben dem Verein eine Orientierungshilfe ohne Anspruch auf Vollständigkeit.

Strukturierung und Verantwortlichkeit im Verein

- ✓ Ist dem Verein die kontinuierliche Umsetzung sowie Verbesserung des Datenschutzes und die Verantwortung bei den gesetzlichen Vertretern bewusst? ☐
  - Sind die Verantwortlichkeiten (am besten schriftlich) geregelt? ☐
  - Können Datenschutzrisiken bewusst gemacht werden? ☐
  - Können alle Verarbeitungstätigkeiten bzw. Prozesse, die personenbezogene Daten betreffen, beschrieben und in einem Verzeichnis dokumentiert werden? ☐
  - Können die Aufgaben zur Umsetzung des Datenschutzes strukturiert und in Teamarbeit umgesetzt werden? ☐
  - Gibt es ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DSGVO? ☐
  - Ist eine Datenschutzrichtlinie/ Datenschutzordnung des Vereins vorhanden? ☐
- ✓ Wurden die Voraussetzungen* zur verpflichtenden Bestellung eines Datenschutzbeauftragten geprüft? ☐

  Da die Voraussetzungen hierfür bei einem ehrenamtlich-gemeinnützigen Sportverein in der Regel nicht zutreffen, benötigt der Verein keinen Datenschutzbeauftragten.
  **Sind mehr als neun Personen ständig, also mehr als die Hälfte ihrer Tätigkeit (als Kerntätigkeit), mit der Verarbeitung von personenbezogenen Daten beschäftigt – (z.B. Mitgliederverwaltung/ Beitragsverwaltung/ Lohnabrechnung)?*
  - Hat der Verein sich über eine freiwillige Benennung eines Datenschutzbeauftragten Gedanken gemacht? ☐
  - Gibt es ein Mitglied, das den Verantwortlichen als Unterstützung rund um den Datenschutz im Verein beratend zur Seite stehen kann? ☐

Verarbeitungstätigkeiten

- ✓ Haben Sie ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DSGVO? ☐
- ✓ Gibt es für jede Verarbeitungstätigkeit Angaben, mit der Sie die Rechtmäßigkeit der Verarbeitung nachweisen können? (siehe auch Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung) ☐
- ✓ Liegen Einwilligungen zur Verarbeitung von personenbezogenen Daten vor, die nicht über eine rechtmäßige Verarbeitung gedeckt sind und kann dies nachgewiesen werden? ☐

(= Daten, die Vereine über die Erlaubnistatbestände der Erfüllung eines Vertrages oder eines berechtigten Interesses - wenn nicht die Interessen der betroffenen Person überwiegen - hinaus verarbeiten)

- ✓ Haben Sie geprüft, ob die Einwilligungen, auf die Sie eine Verarbeitung stützen, noch den Voraussetzungen der Art. 7 und/oder 8 DSGVO entsprechen? ☐
- ✓ Muss bei der Verwendung von Formularen zur Datenerhebung der Nutzer aktiv zustimmen, dass seine Informationen gespeichert werden? ☐
  Beispiel Kontaktformular: Einfügen einer Checkbox zur Einwilligung. Die Auswahl der Checkbox muss der Nutzer selbst aktiv durchführen.
- ✓ Haben Sie die Informations- und Zustimmungsverfahren dokumentiert und gespeichert? ☐
- ✓ Haben Sie eine Videoüberwachung und hierfür die entsprechenden Vorkehrungen getroffen? ☐

- ✓ Haben Sie Externe (Auftragsverarbeiter) zur Erledigung Ihrer Arbeiten (z.B. Mitgliederverwaltung) eingebunden? ☐
  - Wenn ja, haben Sie eine Übersicht über die Auftragsverarbeiter? ☐
  - Wenn ja, haben Sie mit allen Ihren Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DSGVO abgeschlossen? ☐
  - Wurden bestehende Verträge nach den Anforderungen der DSGVO überarbeitet? ☐
  - Ist gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können? ☐

Aufklärung und Schulung der ehren- und hauptamtlichen Mitarbeiter

- ✓ Sind alle Mitarbeiter, die mit personenbezogenen Daten Umgang haben bzgl. des Datenschutzes sensibilisiert (Aufklärung) und ggf. geschult (Schulungsmaßnahme zur konkreten Umsetzung des Datenschutzes im Verein)? ☐
  - Sind Teilnahmen an Schulungen mit Unterschrift der Teilnehmer dokumentiert? ☐
  - Haben alle Mitarbeiter, die mit personenbezogenen Daten Umgang eine Erklärung zum vertraulichen Umgang mit den ihnen anvertrauten personenbezogenen Daten unterzeichnet? ☐

Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte

- ✓ Haben Sie Ihre Datenschutzrichtlinien/ Datenschutzordnung im Verein zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 bzw. 14 DSGVO angepasst? ☐
  - Haben Sie die Datenschutzrichtlinien in die Beitrittserklärung integriert zur Erfüllung der Informationspflichten bei der Erhebung der Daten? ☐
  - Haben Sie eine Datenschutzerklärung auf der Webseite des Vereins integriert, um die Besucher über Ihre Verarbeitungsprozesse zu informieren? ☐
  - Ist die Datenschutzerklärung auf der Webseite auf der Landingpage jederzeit für die Besucher zu erreichen? ☐
  - Ist die Aufnahme einer Datenschutzklausel in der Vereinssatzung mit Verweis auf eine Datenschutzordnung im Verein geplant? ☐
- ✓ Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Auskunft zu den eigenen Daten nach Art. 15 DSGVO zeitnah und vollständig erfüllen zu können (Art. 12 Abs. 1 DSGVO)? ☐
- ✓ Haben Sie Verfahren eingerichtet, um Anträge auf Datenübertragbarkeit betroffener Personen erfüllen zu können (Art. 20 DS-GVO)? ☐
- ✓ Kann den Nutzern der Webseite Auskunft über die Verarbeitung und gespeicherten Datenkategorien gegeben werden? ☐

  Jedes Mitglied hat das Recht auf Auskunft und die Daten übertragen zu bekommen. Finden Sie einen Weg, wie Sie das Auskunftsrecht erfüllen können bzw. angeforderte Daten sicher und maschinenlesbar übertragen können.
- ✓ Haben Sie ein Konzept zum Umgang mit der Löschung von personenbezogenen Daten nach Zweckverfall bzw. Widerruf von Einwilligungen? ☐
  - Können Sie sicherstellen, dass zu löschende Daten (die keiner Aufbewahrungspflicht unterliegen) von ausgetretenen Mitgliedern auch auf allen EDV-Systemen im Verein, bei den zur Verarbeitung berechtigten Personen, bei Dienstleistern oder Verbänden gelöscht werden? ☐
  - Kann sichergestellt werden, dass bei Funktionärswechsel alle personenbezogenen Daten des Vereins herausgegeben bzw. bei den ehemaligen Funktionären gelöscht werden? ☐

Maßnahmen zur Datensicherheit

- ✓ Haben Sie Ihre bestehenden Prozesse zur Überprüfung der Sicherheit der Verarbeitung auf die neuen Anforderungen des Art. 32 DSGVO angepasst? ☐
- ✓ Wurden etablierte Standardmaßnahmen zum effektiven Schutz der Daten durchgeführt? ☐
  Dazu gehören u.a. aktuelle Betriebssysteme und Anwendungen, Passwortschutz, regelmäßige Backups, Virenscanner und Benutzerrechte.
- ✓ Gibt es ein geeignetes Managementsystem und Prozesse zur regelmäßigen Überprüfung, Bewertung und Verbesserung der Schutzmaßnahmen? ☐

- Sind alle Computer mit einer Virenschutz-Software ausgerüstet? Wird diese Virenschutz-Software regelmäßig aktualisiert? ☐
- Sind alle Computer mit einer Firewall ausgerüstet und wird diese regelmäßig aktualisiert? ☐
- Werden regelmäßig Backups durchgeführt? ☐
- Erstreckt sich das Datenschutz-Konzept auch auf mobile Datenträger, wie Smartphones? ☐
- Ist bei der Nutzung privater PCs sichergestellt, dass nur die berechtigte Person auf die Daten zugreifen kann und die Schutzmaßnahmen auch auf privaten PCs durchgeführt werden? ☐
- Wurden die Mitarbeiter hierzu informiert und ggf. geschult? ☐
- Ist Nicht-Berechtigten der Zutritt zu den Computern sowie mobilen Endgeräten, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt (Zutrittskontrolle)? ☐
- Wird die Nutzung dieser Computer sowie mobiler Endgeräte von Nicht-Berechtigten verhindert (Zugangskontrolle)? ☐
- Ist gewährleistet, dass die Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle)? ☐
- Ist gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können? ☐
- Ist gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind? ☐
- Sind Webseiten mit SSL-Zertifikaten (HTTPS) bei der Datenübertragung über Kontaktformulare geschützt? ☐

Datenschutzverletzungen

- ✓ Haben Sie gem. Art. 33 DSGVO sichergestellt, dass die Meldung von Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden an die Aufsichtsbehörde möglich ist? ☐
- ✓ Haben Sie insbesondere sichergestellt, dass Datenschutzverletzungen erkannt werden können? ☐
- ✓ Haben Sie einen Prozess aufgesetzt, wie mit potentiellen Verletzungen intern umzugehen ist? ☐
- ✓ Haben Sie festgelegt, wer, wann und wie mit der Datenschutzaufsichtsbehörde kommuniziert? ☐

Quelle: In Anlehnung an „Fragebogen zur Umsetzung der DS-GVO zum 25. Mai 2018" des Bayerisches Landesamts für Datenschutzaufsicht