

DSGVO-Checkliste 2025 – Sportvereine

(Praktischer Leitfaden zur Einhaltung der Vorschriften und zum Schutz der Mitgliederdaten)

1. Governance und Verantwortlichkeit

- Einen DSGVO-Beauftragten oder Datenschutzbeauftragten (DPO) benennen
- Ein Verzeichnis der Datenverarbeitungen führen (Mitglieder, Ehrenamtliche, Sponsoren usw.)
- Dienstleister und Anbieter identifizieren, die Daten im Auftrag des Vereins verarbeiten (z. B. ERP-System, Hosting, Bank)

2. Datenerhebung

- Klare Anmeldeformulare mit sichtbaren DSGVO-Hinweisen verwenden
- Nur notwendige Daten erheben (Grundsatz der Datenminimierung)
- Ausdrückliche Einwilligung einholen für:
 - Veröffentlichung von Fotos und Videos
 - Weitergabe an Partner (z. B. Sponsoren)
- Einen Link zur Datenschutzrichtlinie des Vereins einfügen

3. Verwaltung und Speicherung

- Daten zentral in einem sicheren Tool speichern (z. B. DSGVO-konformes ERP-System)
- Datenzugriffe entsprechend der Rollen beschränken (Trainer, Kassenwart, Vorstand)
- Sensible Dokumente (ärztliche Atteste, Verträge) in einem verschlüsselten und passwortgeschützten Bereich speichern

4. IT-Sicherheit

- Zwei-Faktor-Authentifizierung für sensible Nutzerkonten aktivieren
- Regelmäßige Datensicherungen durchführen
- Komplexe und regelmäßig erneuerte Passwörter verwenden
- Nutzung unsicherer Medien verbieten (z. B. unverschlüsselte USB-Sticks, öffentlich geteilte Ordner)

5. Aufbewahrung und Löschung

- Für jede Datenart eine Aufbewahrungsfrist festlegen
- Daten ehemaliger Mitglieder nach Ablauf gesetzlicher Fristen löschen oder anonymisieren
- Ein Löschprotokoll führen, um die Einhaltung nachzuweisen

6. Rechte der Betroffenen

- Ein einfaches Verfahren zur Ausübung der Rechte einrichten:
 - Auskunftsrecht
 - Recht auf Berichtigung
 - Recht auf Löschung
 - Recht auf Datenübertragbarkeit
- Auf jede Anfrage innerhalb von maximal 30 Tagen reagieren

7. Kommunikation und Sensibilisierung

- Vorstand, Trainer und Ehrenamtliche in DSGVO-Best Practices schulen
- Datenschutzrichtlinie im Vereinsheim und auf der Website veröffentlichen
- Mitglieder über wichtige Änderungen bei der Datenverarbeitung informieren

8. Im Falle eines Vorfalls

- Eine interne Notfallprozedur bei Datenverlust oder Datenleck vorhalten
- Gegebenenfalls innerhalb von 72 Stunden die Datenschutzaufsichtsbehörde informieren
- Betroffene Personen benachrichtigen, wenn ein Risiko für ihre Rechte und Freiheiten besteht