CHECKLISTE

Korrekte Umsetzung der DSGVO in Vereinen

Achtung:
Diese Checkliste ersetzt nicht die Auseinandersetzung mit der DSGVO!

Hinweis: Definitionen der einzelnen unten angeführten Begriffe findet ihr hier:
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html

Am 25. Mai 2018 ist es so weit: Die Datenschutz-Grundverordnung 2016/679 (kurz DSGVO) tritt in allen EU-Mitgliedsstaaten und damit auch in Österreich in Kraft. Gegenüber der bisherigen Rechtslage im Bereich Datenschutz bringt die DSGVO wesentlich erhöhte Pflichten für all jene, die Daten von natürlichen Personen „verarbeiten" (ganz- oder teilautomatisiert bzw. nicht nichtautomatisiert und systematische Speicherung). Unter den weiten Begriff „Verarbeitung" fällt im Prinzip jede Form der Handhabung der Daten, etwa das Erheben, das Ordnen, die Speicherung, Veränderung, Übermittlung, Löschung, unabhängig von der gewählten Methode (also sowohl EDV gestützte Verarbeitung als auch manuelle Ablage sind davon betroffen) etc.

Führt euer Verein also solche Vorgänge regelmäßig durch, so bist du bzw. seid ihr als Verantwortliche verpflichtet, ein Verzeichnis über diese Tätigkeiten anzulegen und dieses laufend zu aktualisieren. Die DSGVO räumt den Personen, deren Daten dein Verein verarbeitet, außerdem eine Reihe von Rechten ein. Die Aufgabe des Vereinsverantwortlichen ist es, die Gewährung dieser Rechte sicherzustellen.

Die Erfüllung der datenschutzrechtlichen Verpflichtungen erscheint auf den ersten Blick kompliziert. Zwar kann die korrekte Durchführung der DSGVO-Bestimmungen tatsächlich einigen Aufwand in der Vorbereitung bedeuten – ist dein Verein jedoch erst einmal „datenschutzfit" aufgestellt, sind laufend nur geringe Anpassungen nötig. Die nachfolgende Checkliste soll dir als roter Faden in der Umsetzungsphase dienen und die Erfüllung der datenschutzrechtlichen Verpflichtungen deines Vereins auch in der Zukunft ermöglichen.

1. Phase – Organisation der Umsetzung:

- ☐ Festlegung einer im Verein für die Umsetzung der DSGVO-Bestimmungen zuständigen Person bzw. Personengruppe
- ☐ Vereinbarung eines Zeitplans – wann sind welche Schritte von wem zu setzen, um rechtzeitig bis 25. Mai einen DSGVO-konformen Zustand herzustellen?

2. Phase – Ermittlung des derzeitigen Zustandes (Ist-Analyse)

- ☐ Über welche personenbezogenen Daten verfügt der Verein?
  - WICHTIG! Personenbezogene Daten sind all jene Daten, die direkt oder indirekt Rückschlüsse auf die Identität einer natürlichen Person zulassen. Anonyme Daten (z.B. Daten aus einer anonymen Umfrageerhebung) oder Daten juristischer Personen (z.B. Lieferanten-GmbH, sofern diese nicht den Namen einer natürlichen Person trägt) sind daher für die Umsetzung der DSGVO-Bestimmungen nicht relevant.
  - Beispiele: Name, Adresse, Telefonnummer, E-Mail-Adresse, Sozialversicherungsnummer, Fotos der betroffenen Person, …
- ☐ Woher kommen bereits vorhandene Daten und auf welcher Grundlage wurden sie erhoben?
  - Beispiele:
    - es liegt ein Mitgliedsvertrag zwischen betroffener Person und dem Verein vor und die Datenverarbeitung wird vom Vertragszweck gedeckt.
    - die betroffene Person hat explizit in die Datenverarbeitung eingewilligt (z.B. mittels Double-Opt-In bei Newslettern an Nicht-Vereinsmitglieder. Unter Double-Opt-In wird verstanden, dass nach der Regis-trierung zur tatsächlichen Aufnahme in den Newsletter noch ein Bestätigungslink angeklickt werden muss).
    - die Datenverarbeitung liegt im berechtigten Interesse des Vereins und diesem Interesse stehen Grundrechte und -freiheiten der Betroffenen nicht entgegen.
- ☐ Wozu dienen diese personenbezogenen Daten bisher?
  - WICHTIG! Jede Datenverarbeitung (also auch die weitere Speicherung) muss einen Zweck erfüllen. Die grundlose Aufbewahrung von Daten auf unbestimmte Zeit ist daher unzulässig und nicht mehr gebrauchte Daten sind sofort zu löschen → Datenminimierung.
  - Beispiele:
    - Abwicklung eines Vertrages z.B. Mitgliedsvertrag
    - Information der Vereinsmitglieder
    - Newsletter-Versand an Mitglieder und Interessenten
- ☐ Werden die bestehenden Daten weitergegeben?
  - Wenn ja, wurden die Daten zur Auftragsverarbeitung weitergeleitet (z.B. Weitergabe der Arbeitnehmerdaten an eine Steuerberatungskanzlei zur Lohnverrechnung, Externe IT-Dienstleister die z.B. ein Cloud Service anbieten, Druckerei die Adresskarten druckt, etc.) oder
  - wurden die Daten an sonstige Empfänger weitergeleitet? Wenn ja, wurden die Betroffenen davon informiert?
- ☐ Werden auch sensible Daten verarbeitet?
  - Beispiele:
    - Gesundheitsdaten, Religionsbekenntnis, Gewerkschaftszugehörigkeit, politische Überzeugung, …
- ☐ Wie sind Beitrittsverträge, AGB, Website, Statuten in datenschutzrechtlicher Hinsicht ausgestaltet?
- ☐ Grundlegender Check der IT-Systeme um Datensicherheit zu gewährleisten (Backup-Prozesse, Kontrolle des Zugriffs, Log-Files, aber auch triviale Maßnahmen wie Passwortschutz, Virenschutz der Geräte, etc.). Siehe auch Allgemeine TOMs des Musterverzeichnisses.

3. Phase: Herstellung eines DSGVO-konformen Zustands

☐ Erstellung eines Datenverarbeitungsverzeichnisses (siehe z.B. Vorlage der SPORTUNION)

- WICHTIG! Ein Datenverarbeitungsverzeichnis ist bis auf wenige Ausnahmen von jedem Verein zu führen (kein Verzeichnis, wenn gar keine personenbezogenen Daten im Verein verarbeitet werden) Das Verzeichnis muss schriftlich geführt werden und kann z.B. in Word, Excel oder einer eigens dafür bestimmten Software gespeichert werden.
- Das Datenverarbeitungsverzeichnis hat zu enthalten:
  - die Kontaktdaten des Verantwortlichen (in diesem Fall also des Vereins), gegebenenfalls die Kontaktdaten eines Datenschutzbeauftragten
  - eine Beschreibung der Verarbeitungsvorgänge (und ggf. Verarbeitung durch Auftragsverarbeiter)
  - die Zwecke der Datenverarbeitungen
  - die Kategorien betroffener Personen (z.B. „Mitglieder")
  - die Kategorien verarbeiteter Daten (z.B. „Name und Adresse")
  - gegebenenfalls die Kategorien von Empfängern, an die die Daten weitergeleitet werden (z.B. „Partnervereine", „Inkassobüros" oder an den Dachverband bzw. Fachverbände)
  - wenn möglich, Löschfristen für die einzelnen Datenkategorien (z.B. 7 Jahre buchhalterische Aufbewahrungspflicht)
  - Klären ob Daten an Drittländer oder internationale Organisationen weitergegeben werden (v.a. im Leistungssport möglich)
  - Werden sensible Daten (darunter fallen auch Gesundheitsdaten) verarbeitet? Wenn ja, ist eventuell eine Datenschutzfolgeabschätzung sowie ein Datenschutzbeauftragter notwendig.
    - WICHTIG! Bist du dir diesbezüglich nicht sicher, empfiehlt sich die Konsultation eines Datenschutzexperten
- Das Datenverarbeitungsverzeichnis muss der Datenschutzbehörde jederzeit in aktueller Version zur Verfügung gestellt werden können! Es trifft den Verein also eine umfassende, laufende Dokumentationspflicht.

☐ Datenschutz-Update für Verträge und Vertragsgrundlagen

- Mitglieds-/Beitrittsverträge DSGVO-konform abfassen (Datenschutzerklärung, gesonderte Einwilligung für nicht vom Vertragszweck umfasste Verarbeitungen, z.B. Newsletter-Versand)
- schriftliche Verträge mit Auftragsverarbeitern
- Datenschutzerklärung in AGB / Statuten
- TIPP! Du greifst hier am besten auf DSGVO-konforme Vertragsschablonen zurück, wie sie z.B. die WKO auf Ihrer Website anbietet.
- Erfüllung der datenschutzrechtlichen Informationspflicht bei Erhebung der Daten

☐ Datenschutz-Update für sonstige Anwendungen

- Liegen Datenverarbeitungen vor, die von keiner vertraglichen Grundlage gedeckt sind bzw. für die der Verein keine berechtigten Interessen geltend machen kann?
  - Beispiel: Newsletter-Versand an Nichtmitglieder ist ohne nachweisbare Einwilligung der betroffenen Person nicht möglich!
- Ohne nachweisbare Einwilligung erhobene bzw. bestehende Daten sind zu löschen
- Erfüllung der datenschutzrechtlichen Informationspflicht bei Erhebung der Daten

☐ Sicherstellung der Geltendmachung von Betroffenenrechten
    - An wen im Verein können sich Betroffene, die ihre Rechte nach DSGVO ausüben möchten, wenden?
        - Recht auf Auskunft (Achtung Fristlauf Erteilung Auskunft 4 Wochen)
        - Recht auf Widerruf
        - Recht auf Löschung (Achtung Spannungsverhältnis gesetzliche Aufbewahrungspflicht)
        - Recht auf Information (im Zeitpunkt der Erhebung der Daten!)
        - Recht auf Datenübertragbarkeit
        - Recht auf Berichtigung und Einschränkung der Verarbeitung
    - Sind meine Systeme und Abläufe so konzipiert, dass die Rechte auch tatsächlich ausgeübt werden können?
        - Dies wäre z.B. dann nicht der Fall, wenn Mitarbeiter personenbezogene Daten jeweils auf ihren passwortgeschützten Accounts „zersplittert" speichern oder wenn personenbezogene Daten ohne entsprechende Garantien an Dritte weitergeleitet werden.

☐ Einführung technischer und organisatorischer Maßnahmen zum Datenschutz
    - technische Maßnahmen: Verschlüsselung, Back-Up-Strategien, Passwortschutz, Zugangskontrolle, Protokollierung von Zugriffen auf Datensätze, etc.
    - organisatorische Maßnahmen: Vier-Augen-Prinzip, „Datenschutz-Policies" im Verein (Bildschirme werden bei Verlassen des Raumes gesperrt, Dritte erhalten nur unter bestimmten Voraussetzungen Zugang zu den Räumlichkeiten, etc.)
    - WICHTIG! Bist du dir diesbezüglich nicht sicher, empfiehlt sich die Konsultation eines IT-Experten.

4. Phase: Nach Inkrafttreten der DSGVO

☐ Kontinuierliche Pflege und Berichtigung des Datenbestandes und des Datenverarbeitungsverzeichnisses
    - entsprechende Zuständigkeiten im Verein definieren

☐ Konzept zur Löschung nicht mehr gebrauchter Datensätze (in der einfachsten Umsetzung wird 1x jährlich ein Check mit dem Verzeichnis gemacht und so festgestellt welche Datensätze gelöscht / geschreddert gehören – z.B. alte Buchhaltung entsorgen. Weiters sollte ein Vorgang definiert werden, wie das Recht auf Löschung effizient umgesetzt werden kann, d.h. dass auch alle im Verein involvierten Personen davon erfahren und die Löschung vornehmen können. Achtung auf gesetzliche Aufbewahrungspflichten.

☐ Technische Maßnahmen müssen stets dem Letztstand der Technik entsprechen, laufend überprüfen und ggf. aktualisieren