EU-Datenschutz-Grundverordnung (DSGVO)

1. Allgemeines

Die DSGVO gilt auch für Vereine und Verbände. Bei Verstößen drohen empfindliche Strafen.

Datenverarbeitung ist grundsätzlich nur erlaubt, wenn es eine gesetzliche Grundlage dafür gibt oder sie zur Wahrung der berechtigten Interessen des Vereins oder eines Dritten erforderlich ist (Art. 6 Absatz 1 Satz 1 f DSGVO).

Es gelten zwei Grundsätze:
- Grundsatz des Verbots mit Erlaubnisvorbehalt
  (Die Datenverarbeitung ist generell verboten, so lange sie nicht durch ein Gesetz oder Vertrag ausdrücklich erlaubt ist oder der Betroffene in die Verarbeitung eingewilligt hat)
- Grundsatz der Datensparsamkeit
  (Es sollten nicht mehr Daten erhoben werden, als erforderlich)

2. Rechte der Betroffenen / Mitglieder

- Auskunftsrecht
- Zugriffsrecht
- Recht auf Berichtigung falscher Daten
- Recht auf Einschränkung der Datennutzung
- Einspruchsrecht
- Widerspruchsrecht zur Datenerhebung
- Recht auf Löschung / Vergessenwerden

3. Datenschutzverletzung/Datenpanne

Im Falle einer Datenschutzverletzung sind die betroffenen Personen innerhalb von 72 Stunden zu informieren, wenn diese Panne mit einem "hohen Risiko" verbunden ist. Das ist der Fall, wenn es:
- unbeabsichtigt oder unrechtmäßig zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von persönlichen Daten kommt
- es unbefugten Zugang zu personenbezogenen Daten gegeben hat

4. Technische und organisatorische Maßnahmen (TOM)

Der Verein muss darstellen, welche Maßnahmen zur Datensicherung er unternimmt. Das sind:
- Regelmäßige Updates zu Betriebssystemen und genutzten Programmen
- Passwortgeschützte Datensysteme
- Regelmäßige Backups
- Aktuelle Virenscanner und Firewalls
- Vergabe von Benutzerrechten

5. Strafen

Bei Verletzung des Datenschutzes drohen hohe Bußgelder.

6. Umkehr der Beweislast

Nach der DSGVO muss der Verein beweisen, dass keine Datenschutzverletzung vorliegt.

7. Datengeheimnis

Die Personen, die mit der Datenverarbeitung befasst sind, müssen auf das Datengeheimnis verpflichtet werden. Dazu sollte der Verein ein entsprechendes Merkblatt vorbereiten und per Unterschrift bestätigen lassen.

8. Weitergabe von Daten

Sollte der Verein, über den internen Gebrauch hinaus, auch Daten weitergeben (müssen), ist das an bestimmte Bedingungen geknüpft:

- Weitergabe an andere Mitglieder: Nur bei einem Minderheitenbegehren nach § 37 BGB
- Weitergabe an Verbände: Ist zulässig, wenn sich das aus der Vereinstätigkeit ergibt.
- Veröffentlichung von Daten: Die Veröffentlichung (Vereinszeitung, Mitteilungsblatt, Schwarzes Brett usw.) ist zulässig, wenn eine entsprechende Einwilligung vorliegt oder sie zwingend für die Verwirklichung des Vereinszwecks erforderlich ist.
- Veröffentlichung im Internet: Ist grundsätzlich unzulässig, wenn sich der Betroffene nicht ausdrücklich damit einverstanden erklärt hat.
- Die Weitergabe zu Werbezwecken darf nur mit Zustimmung des jeweiligen Mitglieds erfolgen.

9. Informationspflicht in Formularen

Der Verein muss in jedem Formular, das er zu Erhebung personenbezogener Daten nutzt (z.B. Aufnahmeantrag), folgende Angaben machen:

- Name und Kontaktdaten des Vereins und des Vorstands.
- Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden).
- Konkreter Zweck der Datenverarbeitung.
- Rechtsgrundlage der Datenverarbeitung (z.B. Betreuung des Mitgliedschaftsverhältnisses).
- Ggf. berechtigte Interessen im Sinne des Art. 6 Abs. 1 f DSGVO, wenn diese Rechtsgrundlage für die Datenverarbeitung ist.
- Empfänger oder Kategorien von Empfängern bei der geplanten Weitergabe (z.B. an einen Dachverband)
- Hinweis auf geplante Übermittlungen in ein Drittland, ggf. mit Hinweis auf das Fehlen von Garantien zur Datensicherheit.
- Speicherdauer der personenbezogenen Daten (wenn möglich).
- Belehrung über Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht).
- Hinweis auf jederzeitiges Widerrufsrecht einer gegebenen Einwilligung.
- Hinweis auf Beschwerderecht beim Landesdatenschutzbeauftragten.

10. Verzeichnis der Verarbeitungstätigkeiten

Artikel 30 DSGVO fordert, dass die Verantwortlichen ein Verzeichnis über alle Verarbeitungstätigkeiten führen, die in ihrer Organisation durchgeführt werden. Es muss genau dokumentiert werden, in welchem Zusammenhang wie mit personenbezogenen Daten gearbeitet wird.
Es muss mindestens folgende Daten enthalten:

- Namen und Kontaktdaten des Vereins
- Namen und Kontaktdaten des Verantwortlichen
- Name des Datenschutzbeauftragten (falls vorhanden)
- Zweck der Verarbeitung (z. B. Mitgliederverwaltung)
- Beschreibung der Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt werden (müssen), z.B. Verbände, Kommune, Sponsoren, Presse usw.
- Eine Beschreibung der technischen und organisatorischen Maßnahmen für die Datensicherheit
- Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien,

Typische Verarbeitungstätigkeiten in einem Verein sind:

- Mitgliederverwaltung,
- Verwaltung der Mitgliedsbeiträge,

- Lohn- und Gehaltsabrechnung von Beschäftigten,
- Betrieb der Webseite des Vereins (auch wenn das Hosting über einen Dienstleister erfolgt),
- Veröffentlichung von Fotos der Mitglieder auf der Webseite oder in der Vereinszeitung,
- Meldung von Mitgliedern zu Veranstaltungen und Wettkämpfen,
- Organisation von Kursen und anderen Vereinsveranstaltungen.

11. Auftragsverarbeitung

Die Pflicht zum Abschluss von Auftragsverarbeitungsverträgen besteht nach Art. 28 DSGVO, wenn externe Dienstleister vom Verein beauftragt werden. Das sind dann "Auftragsverarbeiter".

Hier sind folgende Punkte zu beachten:
- eine sorgfältige Auswahl des Auftragsverarbeiters
- **vertragliche Vereinbarung** mit Datenschutzregelung (Art. 28 DSGVO)
- Darstellung der Datenschutzmaßnahmen im Vertrag
- Konsequenzen bei Vertragsende
- Unteraufträge nur mit Erlaubnis des Vereins

12. Der Datenschutzbeauftragte

Sind im Verein mindestens zehn Personen regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, muss ein Datenschutzbeauftragter bestellt werden (§ 38 BDSG). **Dabei spielt es keine Rolle, ob diese Personen hauptamtlich oder ehrenamtlich tätig sind.**
Der Vorstand im Sinne des § 26 BGB darf die Funktion des Datenschutzbeauftragten nicht übernehmen. Der Datenschutzbeauftragte muss der zuständigen Aufsichtsbehörde gemeldet werden (Art. 37 Abs. 8 DSGVO).

Auch unter 10 Personen kann ein Datenschutzbeauftragter zur Pflicht werden, wenn es z.B. um besonders schutzwürdige personenbezogene Daten geht (z.B. Gesundheitsdaten) und die Verarbeitung dieser Daten eine **Kerntätigkeit** des Vereins ist.

13. Einwilligungserklärung

Bereits erteilte Einwilligungserklärungen gelten weiter, wenn sie mit den Anforderungen aus Artikel 7 DSGVO übereinstimmen. Diese Einwilligungserklärung ist nicht erforderlich, wenn die Verarbeitung von Daten für die Erfüllung eines Vertrags erforderlich ist.

Mitgliederdaten, die der Verein benötigt, um die Erfüllung eines Vertrags sicherzustellen (dazu zählt auch der Mitgliedsvertrag), dürfen ohne ausdrückliche Einwilligung des Vertragspartners verarbeitet werden (Art. 6 Abs. 1 Satz 1b DSGVO).

Wichtig:
Damit sind aber nur die Daten gemeint, die zur Bearbeitung des Mitgliedschaftsverhältnisses unbedingt **erforderlich** sind. Für Daten darüber hinaus muss eine Einwilligung vorliegen.

Außerdem ist auch keine Einwilligung erforderlich, wenn es sich um Daten handelt, die zur Erfüllung einer rechtlichen Verpflichtung erforderlich sind (z.B. gesetzliche Aufbewahrungspflichten von steuerrelevanten Unterlagen).

Bei der Einwilligungserklärung muss jeder einzelne Zweck der Datenverarbeitung aufgeführt werden.
Die Einwilligung muss eindeutig und aktiv erklärt werden. Eine stillschweigende Zustimmung reicht nicht aus. Sie muss freiwillig und in informierter Weise erfolgen. Den Betroffenen muss also klar sein, welche ihrer Daten zu welchem konkreten Zweck wie genutzt werden:

Die Einwilligungserklärung kann nicht durch eine Satzungsregelung oder einen Mitgliederbeschluss ersetzt werden. Auch Sammellisten sind nicht zulässig.

14. Erforderliche Aufgaben für den Vorstand

Folgende Maßnahmen und Aufgaben müssen erfüllt werden (die Reihenfolge ist nicht entscheidend):

1. Analyse, mit welchen personenbezogenen Daten von Mitgliedern, Interessenten und Mitarbeitern umgegangen wird.
2. Wie werden diese erhoben, gespeichert und verarbeitet?
3. Wer darf darauf zugreifen, und wie ist der Zugriff geschützt?
4. Liegen gesetzliche oder vertragliche Voraussetzungen für die Datenerfassung vor?
5. Welche Daten sind danach wirklich erforderlich?
6. Welche Daten können (sollten) demnach gelöscht werden? "Karteileichen" bzw. überflüssige Daten darf es nicht mehr geben.
7. Bestellung eines Datenschutzbeauftragten (wenn erforderlich).
8. Erstellung eines Verarbeitungsverzeichnisses.
9. Abschluss von Verträgen zur Auftragsdatenverarbeitung mit externen Dritten.
10. Entwicklung von Sicherungssystemen, um unberechtigte Zugriffe und Datenverlust zu verhindern.
11. Prüfung und Sicherstellung der TOMs (= technischen und organisatorischen Maßnahmen).
12. Sicherstellung der Betroffenenrechte.
13. Einwilligungserklärungen verfassen und von allen Mitgliedern (auch Altmitgliedern). unterschreiben lassen
14. Datenschutzerklärungen (z.B. auf der Homepage) aktualisieren.

Fazit:
Der Datenschutz sollte nicht auf die leichte Schulter genommen werden. Auch, wenn manch einer diese ganzen Maßnahmen als übertrieben und überzogen betrachten sollte, es kann sich kein Verein dieser EU-Datenschutzgrundverordnung und dem Bundesdatenschutzgesetz entziehen.