# Datenschutz im Verein

## Einführung

Mit dem Inkrafttreten der europäischen Datenschutzgrundverordnung (DSGVO) 2018 hat sich für Unternehmen und Verein vieles geändert, die Anzahl der zu beachtenden Vorschriften hat sich vervielfacht. Viele Vereinsvorstände sind mit der Umsetzung der Vorgaben überfordert.

Wird jedoch der Datenschutz nicht ernst genommen, kann es teuer werden. Es drohen Abmahnungen und Bußgelder. Richtigen Datenschutz zu praktizieren ist eine komplexe Aufgabe.

Die folgenden Seiten sollen Ihnen einen (groben) Überblick verschaffen, was getan werden muss und auf was Sie unbedingt achten müssen. Doch Achtung: der „Teufel steckt im Detail“, wahrscheinlich kommen Sie ohne weitere Schulung bzw. externe Expertise nicht weiter.

**Um was es geht?**

Datenschutz ist der Schutz der personenbezogenen Daten vor unerlaubter Erhebung, Verarbeitung, Speicherung und Weitergabe. Ziel ist, das Persönlichkeitsrecht, die Grundrechte und Grundfreiheiten betroffener natürlichen Personen zu schützen.

Datenschutzgesetze legen fest, wie und in welchem Umfang Daten geschützt werden müssen. In Deutschland und der EU wird dies insbesondere durch die europäische Datenschutzgrundverordnung (DSGVO) und das deutsche Bundesdatenschutzgesetz (BDSG) geregelt.

Dem Datenschutz sind alle Institutionen verpflichtet, die personenbezogene Daten verarbeiten. Wichtig zu wissen: Vereine sind da keine Ausnahme und genießen keine Sonderrechte.

**Was genau ist mit Datenverarbeitung gemeint?**

In den Gesetzen einheitlich der Begriff Datenverarbeitung genannt. Dabei geht es im Einzelnen um das Erheben, Erfassen, Verwenden, Verbreiten, Abgleichen usw. Datenverarbeitung beinhaltet also alles, was mit den personenbezogenen Daten im Verein geschieht: Jede Form der Verwendung und Nutzung der Informationen, angefangen beim Erfassen neuer Mitglieder über das Ordnen, Speichern, Aktualisieren oder Löschen der Datensätze bis hin zur Verwendung z.B. für den Newsletter-Versand, die Vertragsgestaltung oder das Aufsetzen von Meldungen an Verbände und andere Organisationen. Dabei spielt es keine Rolle, ob die Daten digital oder analog verarbeitet werden.

**Was sind personenbezogene Daten?**

Das sind alle Informationen, die einen Menschen beschreiben und ihn identifizierbar machen.

Im Art. 4 Nr. 1 der DSGVO steht, dass alle Angaben, die Einblicke in die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität von natürlichen Personen ermöglichen, als personenbezogene Daten gelten. Dies gilt für Informationen jedweder Art, also für Schrift, Bild oder Tonaufnahmen.

Dann gibt es noch die einige sensible Daten, die besonders schützenswert sind: Daten über Herkunft, politische und religiöse Überzeugung, sexuelle Orientierung oder die Gesundheit. Deren Verarbeitung ist ohne Einwilligung grundsätzlich untersagt.

Die Liste der personenbezogenen Daten ist umfangreicher als viele vermuten. Das verdeutlicht die folgende Liste:

| | | | |
|---|---|---|---|
| Name, Adresse | Haar-/Augenfarbe | Einkommen | Sexuelle Orientierung |
| Alter, Geburtsdatum | Größe/Gewicht | Steuerdaten | Konfession |
| Familienstand | Interessen | Vertragsverhältnis | E-Mail-Adresse |
| Staatsangehörigkeit | Schuh-Kleidergr. | Besitzverhältnisse | IP-Adresse |
| Beruf | Beitrittsdatum | Bankdaten | Überzeugungen |
| Mitgliedschaften | sportl. Leistungen | Identifikationsnummer | KFZ-Kennzeichen |
| Trainingszeiten | Platzierungen | Sozialversicherungsnummer | Krankheiten/Verletzungen |
| Kurspläne | Auszeichnungen | Personalausweisnummer | Zeugnisse |

## Auf was es bei der Datenverarbeitung ankommt

### 1. Rechtsgrundlage zur Verarbeitung von Mitgliederdaten

Personenbezogene Daten dürfen nur dann verarbeitet - erhoben, gespeichert, verwendet und weitergegeben - werden, wenn es dafür eine gesetzliche Grundlage gibt. Die gesetzliche Grundlage kann sich aus der DSGVO oder anderen Gesetzen ergeben. Ebenso dürfen personenbezogenen Daten verarbeitet werden, wenn eine Einwilligung des betroffenen Mitglieds vorliegt. Anderslautende Regelungen in der Vereinssatzung sind rechtswidrig und haben keine Wirkung.

Generell ist die Datenverarbeitung im Verein zulässig, wenn sie Mitglieder- und Vereinsverwaltung betrifft und zur Erfüllung der Vereinszwecke erforderlich ist. Aber Vorsicht, wichtig ist auch was in der Satzung steht: Sieht die Satzung etwa keinen Bankeinzug für die Mitgliedsbeiträge vor, dürfen von den Mitgliedern auch keine Kontodaten erhoben werden, es sei denn, es liegt eine freiwillige Einwilligung vor.

Für Fehler beim Datenschutz haften immer Verein und Vorstand – der Vorstand sogar mit dem Privatvermögen. Das gilt grundsätzlich auch, wenn ein Datenschutzbeauftragter bestellt ist. Dieser haftet nur dann, wenn er falsch beraten bzw. den Vorstand nicht auf ihm bekannte Fehler und Mängel in Sachen Datenschutz hingewiesen hat.

## 2. Erhebung und Speicherung von personenbezogenen Daten

Prinzipiell sollten nur Daten erhoben, gespeichert und verarbeitet werden, die auch wirklich für den jeweiligen Zweck, erforderlich sind. Überlegen Sie also genau, welche Daten Sie z. B. mit dem Beitrittsformular erheben.

Gespeichert werden die Daten nur so lange, wie sie auch benötigt werden – unter Berücksichtigung der gesetzlichen Aufbewahrungsfristen.

## 3. Datenspeicherung und -sicherheit

Die DSGVO unterscheidet nicht zwischen analoger und digitaler Datenverarbeitung. Es ist unerheblich, ob Daten mittels herkömmlicher Karteien und Register oder automatisiert auf einem Computer oder Server gespeichert und verarbeitet werden. In allen Fällen muss die Sicherung der Daten den datenschutzrechtlichen Anforderungen genügen.

**Der Verein hat alle praktischen Sicherheitsmaßnahmen ergriffen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten.**

In diesem Zusammenhang sprechen wir von technischen und organisatorischen Maßnahmen (TOM). Dazu zählen zum Beispiel die Verschlüsselung von Daten, die Belastbarkeit und Vertraulichkeit von Systemen aber auch der Zugang zu EDV-Räumen, die Vergabe und Geheimhaltung von Zugangsdaten, eine sichere Kommunikation, regelmäßige Updates etc.

Ob Sie in Bezug auf die Datensicherheit alles richtig machen, können Sie mit der Beantwortung folgender Fragen überprüfen:

1. Benutzen Sie bei der Datenverarbeitung eine Software, die auf dem Stand der Technik und stets up-to-date ist?
2. Haben Sie klare Regeln zum DSGVO-konformen Umgang mit Daten an die Vereinsmitarbeiter kommuniziert?
3. Werden vertrauliche Daten, z.B. Gesundheitsdaten, besonders geschützt und ist der Zugriff durch Dritte ausgeschlossen?
4. Haben Sie dafür gesorgt, dass Daten unveränderbar und korrekt gespeichert werden und nicht verloren gehen können?

5. Ist die Website des Vereins sicher und entspricht sie den gesetzlichen Vorschriften? (Verschlüsselung, Cookie-Hinweis, Impressum, Datenschutzerklärung, Bilderrechte usw.).
6. Führen Sie regelmäßige Datensicherheitskontrollen im Verein durch?

## 4. Datenschutzbeauftragter

Ein Datenschutzbeauftragter (DSB) ist zu bestellen, wenn mindestens 20 Personen im Verein regelmäßig mit der automatisierten (digitalen) Verarbeitung personenbezogener Daten beschäftigt sind. Als DSB kann eine externe Person oder ein Vereinsmitglied benannt werden, Letzteres darf aber weder dem Vorstand angehören noch mit der regelmäßigen Datenverarbeitung im Verein betraut sein.

Der DSB hat primär eine beratende Funktion und soll den Verein bei der Umsetzung einer rechtskonformen Vereinsarbeit unterstützen. Er kann nicht für eine mangelnde Umsetzung von empfohlenen Datenschutzmaßnahmen verantwortlich gemacht werden.

Umgekehrt ist ein DSB darauf angewiesen, dass der Verein und ein benannter Ansprechpartner ihn bei seiner Arbeit unterstützt und ihn über alle datenschutzrechtlichen Belange auf dem Laufenden hält.

## 5. Verzeichnis über Verarbeitungstätigkeiten

Alle Vereine mit Mitgliederverwaltung und Beitragsabrechnung müssen ein Verzeichnis ihrer Verarbeitungstätigkeiten führen. Dieses gibt einen Überblick über die vereinsinterne Datenverarbeitung. In diesem Verzeichnis steht, wer für welchen Verarbeitungsbereich zuständig ist und wer Zugang zu welchen Daten hat. Ebenso wird der Zweck der Datenverarbeitung aufgeführt welche Software eingesetzt wird und welche Technischen und Organisatorischen Maßnahmen (TOM) für die Datensicherheit ergriffen werden.

Dieses Verzeichnis dient auch als Nachweis gegenüber den Aufsichtsbehörden, dass der Verein die datenschutzrechtlichen Vorgaben beachtet und umsetzt.

## 6. Information der Mitglieder zur Datenverarbeitung

Neue Mitglieder sollen schon bei der Aufnahme schriftlich über die Datenverarbeitung im Verein informiert werden. Es empfiehlt sich, schon auf dem Beitrittsformular auf wichtige Datenschutzregelungen hinzuweisen und notwendige Einwilligungen einzuholen.

Bestandsmitglieder können über ein gesondertes Schreiben über Änderungen im Datenschutz informiert werden. Diese Information muss nicht von den Mitgliedern unterschrieben werden

und dient als rechtliche Absicherung des Vereins. Einwilligungen hingegen sollten immer dokumentiert werden.

## 7. Verpflichtung auf datenschutzkonformen Umgang mit Daten nach DSGVO

Alle Personen des Vereins, die mit personenbezogenen Daten umgehen, müssen vom Verein informiert und schriftlich verpflichtet werden, dass die Verarbeitung der personenbezogenen Daten nach den Grundsätzen der DSGVO erfolgt.

Die Verpflichtung muss vor Aufnahme der Tätigkeit erfolgen, bevor die verpflichtete Person mit personenbezogenen Daten in Kontakt kommt.

Bereits im Verein beschäftigte Personen, z.B. Übungsleiter, Vorstandsmitglieder oder Personen in der Mitgliederverwaltung, können die Verpflichtung auch nachträglich im Rahmen der Umsetzung der DSGVO unterzeichnen.

Die DSGVO schreibt keine bestimmte Form der Verpflichtung vor. Aus Gründen der Nachweisbarkeit sollte jedoch ein entsprechendes Dokument verwendet werden Auf diesem sollten neben dem eigentlichen Inhalt der Verpflichtung auch Ort, Datum und die Unterschriften des Vereinsverantwortlichen und der zu Verpflichtenden festgehalten werden.

## 8. Auftragsverarbeitungsverträge mit Drittdienstleistern

Fast jeder Verein lässt personenbezogene Daten von Dritten verarbeiten. Das können z. B. sein:

- Website-Provider
- Anbieter für Cloud-Lösungen
- Buchhaltungs-/Finanzdienstleister

Das nennt man Auftragsverarbeitung (AV). Mit Drittanbietern ist zwingend ein Vertrag (AV-Vertrag) abzuschließen, in dem Datenschutz- und Vertraulichkeitsregelungen vereinbart werden. Der Verein hat die Pflicht, die Datenschutzmaßnahmen des Auftragsverarbeiters kontrollieren.

Es ist wichtig zu wissen, dass ohne einen solchen Vertrag der Verein für Datenschutzverletzungen haftet, selbst wenn diese bei dem jeweiligen Drittanbieter vorkommen.

## 9. Benachrichtigungspflicht des Vereins bei Datenpannen

Bei einer Gefährdung der Datensicherheit (Datenschutzverletzung) müssen betroffene Mitglieder benachrichtigt werden, wenn eine Gefahr für die Persönlichkeitsrechte besteht.

Meldepflichtige Datenschutzverletzungen sind schnell passiert. Stellen Sie sich vor, ein Übungsleiter verliert unterwegs auf dem Weg zur Trainingshalle einen Zettel mit den Kontaktinformationen seiner Trainingsgruppe. Schon ist es geschehen. In diesem Fall muss der Verein die betroffenen Mitglieder informieren und innerhalb von 72 Std auch die die Aufsichtsbehörde benachrichtigen. Das Nichtbefolgen dieser Vorschrift kann empfindliche Geldbußen nach sich ziehen.

Der Verein muss entsprechende Prozesse einrichten, um Probleme in der Datensicherheit sofort zu erkennen und richtig zu reagieren.

## 10. Risiko der Datenverarbeitung

Bestimmte Maßnahmen bergen ein besonders hohes Risiko aus Sicht des Datenschutzes. Ein Beispiel dafür ist zum Beispiel die Installation einer Videoüberwachung. Wie hoch ist dieses Risiko tatsächlich ist, gilt es im Rahmen einer Datenschutz-Folgeabschätzung abzuschätzen, um in der Folge geeignete Maßnahmen zur Risikominimierung zu ergreifen.

## 11. Veröffentlichung von Bildern und anderen personenbezogenen Daten

Die Veröffentlichung personenbezogener Daten in Internet, Presse und Aushängen durch den Verein ist grundsätzlich nur mit ausdrücklicher Einwilligung des Mitglieds zulässig, die der Verein nach den Vorgaben der DSGVO auch entsprechend dokumentieren muss. Das Thema ist komplex und birgt viele Stolperfallen. Besondere Vorsicht ist bei Bildern von Kindern geboten.