Datenschutz im Sportverein

Vorwort

Datenschutz ist längst zu einem festen Bestandteil der Vereinsarbeit geworden. Spätestens seit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) stehen auch Vereine vor der Aufgabe, den Umgang mit personenbezogenen Daten sorgfältig zu regeln und transparent zu dokumentieren. Die Anforderungen sind deutlich gestiegen und betreffen nahezu alle Bereiche des Vereinslebens – von der Mitgliederverwaltung über die Öffentlichkeitsarbeit bis hin zum Umgang mit digitalen Kommunikationsmitteln.

Um Vereine bei dieser Herausforderung praxisnah zu unterstützen, wurde in enger Zusammenarbeit mit erfahrenen Fachleuten aus dem Medien- und Datenschutzrecht ein Konzept entwickelt, das speziell auf die Bedürfnisse kleiner und mittlerer Vereine zugeschnitten ist. Das Ergebnis ist dieser Leitfaden, der nicht nur wichtige Muster für eine datenschutzkonforme Dokumentation enthält, sondern auch leicht verständliche Erläuterungen zu häufigen Fragen aus dem Vereinsalltag bietet.

Ziel ist es, Verantwortlichen in Vereinen eine verlässliche Orientierungshilfe an die Hand zu geben und damit einen sicheren und zugleich praktikablen Umgang mit dem Thema Datenschutz zu ermöglichen.

Der Sportbund Rheinland arbeitet seit Jahren eng mit Herrn Rechtsanwalt Alexander Brittner, LL.M. zusammen, der den Verband mit der ADLEX GmbH medien- und datenschutzrechtlich unterstützt.

Ergebnis dieser Zusammenarbeit ist dieser Leitfaden, der neben wichtigen Mustern für eine datenschutzkonforme Dokumentation auch hilfreiche Erläuterungen zu Alltagsfragen liefert.

Inhaltsverzeichnis

1 Einführung

1.1 Was bedeutet Datenschutz im Verein?

Datenschutz bezeichnet den Schutz personenbezogener Daten natürlicher Personen vor unbefugter Erhebung, Verarbeitung, Speicherung und Weitergabe. Ziel ist es, die Privatsphäre und das Persönlichkeitsrecht der betroffenen Personen – insbesondere Ihrer Mitglieder – zu schützen.

Personenbezogene Daten umfassen z. B. Name, Adresse, Geburtsdatum, Telefonnummer, E-Mail-Adresse, Bankverbindung oder sportliche Leistungen. Besonders sensible Daten, etwa zur Gesundheit oder politischen Überzeugung, unterliegen einem erhöhten Schutz.

NACH OBEN

1.2 Wann ist eine Datenverarbeitung erlaubt?

Nach Art. 6 DSGVO ist die Verarbeitung personenbezogener Daten grundsätzlich nur dann zulässig, wenn:

- eine gesetzliche Grundlage besteht (z. B. zur Erfüllung des Vereinszwecks),
- eine ausdrückliche Einwilligung der betroffenen Person vorliegt oder
- ein berechtigtes Interesse des Vereins überwiegt, ohne die Rechte der Betroffenen zu verletzen.

Beispiel: Die Verarbeitung der Kontodaten für den Mitgliedsbeitrag ist nur dann zulässig, wenn die Satzung dies ausdrücklich vorsieht oder eine Einwilligung vorliegt.

Datenverarbeitungsvorgänge müssen nachvollziehbar, dokumentiert und für befugte Personen verständlich sein. Jede Datenverarbeitung bedarf einer schriftlichen oder elektronischen Erfassung, etwa im Verzeichnis von Verarbeitungstätigkeiten.

Es ist sicherzustellen, dass die verarbeiteten personenbezogenen Daten sachlich richtig, vollständig und – soweit erforderlich – aktuell sind. Unrichtige Daten sind zu berichtigen oder zu löschen.

NACH OBEN

1.3 Pflichten des Vereins

Als Verantwortlicher im Sinne der DSGVO trifft Ihren Verein eine Vielzahl an Pflichten:

- Informationspflichten nach Art. 13 DSGVO (z. B. im Mitgliedsantrag),
- technische und organisatorische Maßnahmen zur Datensicherheit (z. B. Passwortschutz, Zugriffsbeschränkungen),
- Verzeichnis von Verarbeitungstätigkeiten,
- Benennung eines Datenschutzbeauftragten, wenn regelmäßig mindestens 20 Personen mit Datenverarbeitung betraut sind,
- Vertragskontrolle bei Auftragsverarbeitern (z. B. IT-Dienstleister, Buchhaltungsbüro),
- Löschung personenbezogener Daten, sobald sie nicht mehr benötigt werden.

NACH OBEN

1.4 Veröffentlichung und Weitergabe von Daten

Die Weitergabe personenbezogener Daten – auch innerhalb des Vereins oder an Dachverbände – ist nur unter bestimmten Voraussetzungen erlaubt. Eine Veröffentlichung (z. B. auf der Website, in sozialen Medien oder im Vereinsblatt) bedarf in der Regel einer vorherigen, informierten Einwilligung.

Achtung: Auch Fotos von Vereinsveranstaltungen oder Turnieren fallen unter personenbezogene Daten und dürfen ohne Einwilligung nicht veröffentlicht werden.

NACH OBEN

1.5 Datensicherheit im Verein

Die DSGVO verpflichtet Vereine zu geeigneten Schutzmaßnahmen, um personenbezogene Daten vor unbefugtem Zugriff, Verlust oder Veränderung zu schützen. Hierzu zählen unter anderem:

- Einsatz sicherer Software und regelmäßiger Updates,
- Zugriffskontrollen und Passwortschutz,
- sichere Datenübertragung (z. B. SSL-Verschlüsselung auf der Website),
- regelmäßige Schulungen und Dokumentation der Maßnahmen.

NACH OBEN

2 Datenschutz-Gesetze

Seit dem 25. Mai 2018 ist die Datenschutzgrundverordnung (DSGVO) europaweit in Kraft. In Deutschland wird sie durch das neue Bundesdatenschutzgesetz (BDSG n. F.) ergänzt. Diese Regelwerke bilden die zentrale rechtliche Grundlage für den Schutz personenbezogener Daten. Während ursprünglich vor allem Unternehmen im Fokus der Umsetzung standen, ist heute klar, dass auch Vereine in vollem Umfang von der DSGVO betroffen sind. Unabhängig davon, ob ein Verein wirtschaftlich tätig ist oder nicht, ob er klein oder groß ist, ob er lokal oder bundesweit aktiv ist – sobald personenbezogene Daten verarbeitet werden, greifen die Vorschriften.

Für Vereine bedeutet dies, dass sie ihre Prozesse zur Erhebung, Speicherung, Nutzung und Weitergabe personenbezogener Daten auf rechtliche Zulässigkeit überprüfen und dokumentieren müssen. Verantwortlich dafür ist grundsätzlich der Vereinsvorstand. Dieser trägt die datenschutzrechtliche Verantwortung für alle im Verein verarbeiteten personenbezogenen Daten.

Insbesondere bei Mitgliedsdaten, Kommunikationsdaten, Gesundheitsdaten (z. B. im Sportbereich) oder auch Fotos von Veranstaltungen handelt es sich regelmäßig um personenbezogene Daten. Entsprechend ist auch bei der Arbeit von Ehrenamtlichen oder beim Versand von Vereinsinformationen stets zu prüfen, ob und wie der Datenschutz gewahrt bleibt.

Ein Grundverständnis der DSGVO sowie der damit verbundenen organisatorischen Pflichten sollte daher zur Grundausstattung jedes Vereinsvorstands gehören. In vielen Fällen empfiehlt es sich zudem, eine fachkundige Person mit der Umsetzung zu betrauen – sei es als externer Datenschutzbeauftragter oder als datenschutzverantwortliches Vorstandsmitglied.

NACH OBEN

3 Begriffe

3.1 Personenbezogene Daten

Der Begriff der personenbezogenen Daten ist zentral im Datenschutzrecht. Nach Art. 4 Nr. 1 DSGVO sowie § 46 BDSG n. F. handelt es sich um alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Identifizierbar ist eine Person bereits dann, wenn sie direkt oder indirekt, etwa über eine Mitgliedsnummer, eine Telefonnummer oder eine E-Mail-Adresse erkannt werden kann.

In der Vereinsarbeit begegnen solche Daten häufig. Schon bei der Erhebung von Mitgliedsdaten – sei es über ein Formular auf Papier oder ein Online-Anmeldeformular – werden personenbezogene Daten verarbeitet. Dazu zählen Namen, Geburtsdaten, Adressen, Telefonnummern, Bankverbindungen, aber auch etwa Fotos oder Gesundheitsdaten, etwa bei der Teilnahme an Wettkämpfen oder Veranstaltungen mit medizinischem Risiko.

Besondere Kategorien personenbezogener Daten unterliegen einem noch höheren Schutz. Hierzu zählen insbesondere Daten über die religiöse oder weltanschauliche Überzeugung, politische Meinungen, die sexuelle Orientierung oder Gesundheitsinformationen. Werden solche Daten verarbeitet, gelten erhöhte Anforderungen hinsichtlich Einwilligung, Zweckbindung und Schutzmaßnahmen.

NACH OBEN

3.2 Verarbeitung von Daten

Unter Verarbeitung versteht die DSGVO jeden Vorgang im Zusammenhang mit personenbezogenen Daten. Dies beginnt bei der Erhebung und reicht über die Speicherung, Veränderung, Übermittlung bis hin zur Löschung der Daten. Auch die Nutzung einfacher technischer Hilfsmittel wie einer Excel-Tabelle auf dem Vereinscomputer oder das Speichern von Daten in einer Cloud ist bereits eine Verarbeitung im Sinne des Datenschutzrechts.

Wichtig ist, dass die Verantwortlichen im Verein ein vollständiges Bild davon haben, wo, wie und zu welchem Zweck personenbezogene Daten verarbeitet werden. Nur dann lassen sich datenschutzrechtliche Risiken vermeiden. Auch die Weitergabe von Daten an Dritte – etwa an Dachverbände, Versicherungsträger oder IT-Dienstleister – fällt unter die Verarbeitung und muss entsprechend geprüft und dokumentiert werden

NACH OBEN

3.3 Einwilligung

Die Verarbeitung personenbezogener Daten ist grundsätzlich nur erlaubt, wenn dafür eine gesetzliche Grundlage besteht. Eine zentrale Rechtsgrundlage bildet die freiwillige, informierte und eindeutige Einwilligung der betroffenen Person. Insbesondere für Fotos bei Veranstaltungen, für den Versand von Newslettern oder für die Veröffentlichung von Daten auf der Vereinswebsite ist in der Regel eine Einwilligung erforderlich.

Die Einwilligung muss freiwillig und für einen bestimmten Zweck erteilt werden. Sie darf nicht an andere Leistungen gekoppelt werden, wenn diese nicht zwingend mit der Datenverarbeitung zusammenhängen. Ein Beispiel hierfür ist die Anmeldung zu einem Sportkurs, bei der zugleich eine Zustimmung zur Veröffentlichung von Fotos eingeholt wird – dies ist nur dann zulässig, wenn die Einwilligung gesondert eingeholt wird.

Auch Minderjährige können in der Regel erst ab einem Alter von 16 Jahren wirksam einwilligen. Bei jüngeren Personen ist die Zustimmung der Erziehungsberechtigten erforderlich. Dies betrifft viele Jugendabteilungen in Sport-, Musik- oder Kulturvereinen.

Vereine sollten Einwilligungen immer schriftlich oder digital dokumentieren. Die Nachweispflicht liegt beim Verein. Ein einfaches Formular, das bei der Aufnahme ausgefüllt wird, kann hier bereits ausreichend sein. Wichtig ist, dass Betroffene jederzeit das Recht haben, ihre Einwilligung zu widerrufen.

Dabei sind für eine wirksame Einwilligung folgende Informationen relevant:

- Betroffene müssen über den Umfang der verarbeiteten Daten und den Zweck der Verarbeitung informiert werden.
- Die Einwilligungserklärung muss leicht zugänglich und in leicht verständlicher Form verfasst sein.
- Der Verarbeitende muss die betroffene Person darauf hinweisen, dass diese ihre Einwilligung jederzeit widerrufen kann.
- Die Einwilligung darf nicht durch Zwang eingeholt werden und ist stets aus freiem Willen zu erteilen.
- Es besteht ein „Kopplungsverbot": Ein Vertragsschluss oder eine sonstige Teilnahme darf nicht von der Einwilligung in die Verarbeitung von personenbezogenen Daten, die für die Durchführung des Vertrags nicht erforderlich sind, abhängig gemacht werden (z.B. Mitgliedschaft nur bei Newslettereinwilligung oder Teilnahme an Sommerfest nur bei Foto-Zustimmung).
- Der Betroffene muss selbst **aktiv** werden: beim Ankreuzen, Setzen von Häkchen oder Anklicken von Kästchen muss die Person dies selbst tun. Wurden entsprechende Kreuze oder Häkchen schon vom Verantwortlichen gesetzt, führt dies zur Unwirksamkeit der Einwilligung („Privacy by Default").
- **Minderjährige**, die nicht das 16. Lebensjahr vollendet haben, können nach Art. 8 DSGVO erst wirksam einwilligen, wenn sie eine Zustimmung der gesetzlichen Vertreter haben (hiervon abweichende Regelungen sind durch die EU-Mitgliedstaaten möglich).

- Ein **Formerfordernis** für Einwilligung besteht nicht (Art. 7 DSGVO). Demnach muss die Einwilligung nicht in Schriftform erteilt werden. Allerdings sollten Sie aus Beweisgründen eine erteilte Einwilligung dokumentieren, da die Beweislast beim Verarbeiter liegt. Zudem muss der Betroffene genau erkennen können, in was er einwilligt.
- Anders ist es im **Beschäftigungsverhältnis.** Dort bedarf die Einwilligung grundsätzlich der Textform (vgl. § 26 Abs. 2 BDSG).

NACH OBEN

3.4 Verantwortlichkeit und Ansprechpartner

Neben den allgemeinen datenschutzrechtlichen Pflichten ist es für Vereine besonders wichtig, klare Zuständigkeiten zu definieren. Die Datenschutz-Grundverordnung sieht ausdrücklich vor, dass Verantwortliche benannt werden müssen, die auf die Einhaltung der Vorgaben hinwirken. Der Verein sollte daher eine konkrete Person als Datenschutzbeauftragten benennen, sofern die gesetzlichen Voraussetzungen erfüllt sind oder eine freiwillige Bestellung aus Gründen der Transparenz und Professionalität sinnvoll erscheint. Diese Person überwacht die Einhaltung der datenschutzrechtlichen Vorgaben, berät den Vorstand und steht den Mitgliedern als Ansprechpartner zur Verfügung. Im Verein kann es zudem zweckmäßig sein, ein kleines Datenschutz-Organisationsteam einzurichten, das aus mehreren Funktionsträgern besteht und die Vertretung im Falle von Urlaub oder Krankheit sicherstellt. Durch klare Kommunikationswege und die Veröffentlichung einer zentralen Kontaktadresse (z. B. eine allgemeine Datenschutz-E-Mailadresse des Vereins) wird sichergestellt, dass Fragen oder Meldungen von Betroffenen jederzeit an der richtigen Stelle eingehen.

Sollte Ihr Verein einen Datenschutzbeauftragten benötigen oder freiwillig benennen wollen, steht das Team der ADLEX GmbH auch kostengünstig als Datenschutzbeauftragter zur Verfügung. Bei Interesse senden Sie uns bitte eine E-Mail an Barbara.Berg@Sportbund-Rheinland.de

Hier geht´s zum Angebot Datenschutz-Komplettpakete.

NACH OBEN

4 Betroffene Personen

4.1 Personenkreise

Der Datenschutz im Vereinsalltag betrifft eine Vielzahl konkreter Tätigkeiten und organisatorischer Prozesse. Daher ist es wichtig, dass die Umsetzung der gesetzlichen Vorgaben praxisnah erfolgt und sich gut in die bestehenden Abläufe integrieren lässt. Die folgenden Abschnitte geben einen Überblick über typische datenschutzrechtlich relevante Situationen und zeigen auf, wie Vereine damit verantwortungsvoll umgehen können.

➢ Relevante Personengruppen

Vereine verarbeiten personenbezogene Daten zahlreicher Personengruppen. Neben den regulären Mitgliedern gehören dazu beispielsweise auch:

- Ehrenamtlich Engagierte, Trainer*innen und Betreuer*innen,
- Teilnehmende an Veranstaltungen (z. B. Workshops, Turnieren, Konzerten),
- Spenderinnen und Spender,
- Fördermitglieder,
- Eltern minderjähriger Mitglieder,
- Interessierte und ehemalige Mitglieder.

Für jede dieser Gruppen sind eigene Datenverarbeitungsvorgänge denkbar – etwa bei der Anmeldung, bei Zahlungsabwicklungen, bei der Kommunikation oder bei der Nutzung von Fotos. Daher ist es empfehlenswert, im Verein eine Übersicht aller relevanten Personengruppen zu erstellen und die jeweils verarbeiteten Datenarten sowie Zwecke systematisch zu dokumentieren.

NACH OBEN

4.2 Rechte als Betroffener

Nach der DSGVO haben alle Personen, deren Daten verarbeitet werden, umfassende Rechte. Diese gelten uneingeschränkt auch für Vereine. Die wichtigsten Rechte sind:

- **Das Recht auf Information:** Die betroffene Person muss darüber informiert werden, welche Daten zu welchem Zweck verarbeitet werden, wer die verantwortliche Stelle ist und wie lange die Speicherung erfolgt.
- **Das Recht auf Auskunft:** Auf Anfrage müssen Vereine mitteilen, welche personenbezogenen Daten gespeichert sind, woher diese stammen, an wen sie weitergegeben wurden und wofür sie verwendet werden.
- **Das Recht auf Berichtigung:** Falsche oder unvollständige Daten müssen auf Wunsch berichtigt werden.
- **Das Recht auf Löschung:** Personen können unter bestimmten Voraussetzungen verlangen, dass ihre Daten gelöscht werden (Recht auf Vergessenwerden).
- **Das Recht auf Einschränkung der Verarbeitung:** Wenn die Richtigkeit der Daten bestritten wird oder ein Löschanspruch noch geprüft wird.
- **Das Widerspruchsrecht:** Daten dürfen nicht mehr verarbeitet werden, wenn ein berechtigter Widerspruch vorliegt.

Vereine müssen sicherstellen, dass sie in der Lage sind, diese Rechte fristgerecht zu erfüllen. Das bedeutet, dass entsprechende organisatorische und technische Prozesse geschaffen werden müssen, z.B. für die Prüfung von Auskunftsanträgen oder die fristgerechte Umsetzung von Löschbegehren.

In der Praxis problematisch ist insbesondere die Datenschutzauskunft nach Art. 15 DSGVO. Dieses kann auch mit dem Recht auf (kostenlose) Kopie verbunden werden.

➢ Auskunftsrecht gemäß Art. 15 DSGVO

Mitglieder, ehemalige Mitglieder oder sonstige Betroffene können vom Verein insbesondere folgende Informationen verlangen:

- Welche personenbezogenen Daten über sie gespeichert sind (z. B. Name, Anschrift, Kontaktdaten, Mitgliedsnummer, Bankverbindung, Teilnahme an Vereinsveranstaltungen),
- zu welchen Zwecken diese Daten verarbeitet werden,
- an welche Empfänger oder Kategorien von Empfängern die Daten übermittelt wurden oder werden (z. B. Dachverbände, Steuerberater, IT-Dienstleister),
- wie lange die Daten gespeichert werden bzw. nach welchen Kriterien sich die Speicherdauer richtet,
- welche Rechte den Betroffenen im Hinblick auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch zustehen,
- ob eine automatisierte Entscheidungsfindung einschließlich Profiling stattfindet (in der Regel bei Vereinen: nein).

➢ Recht auf Kopie der Daten

Nach Art. 15 Abs. 3 DSGVO haben betroffene Personen außerdem Anspruch auf eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind. Diese Kopie soll es der betroffenen Person ermöglichen, sich ein vollständiges Bild davon zu machen, welche Daten der Verein über sie verarbeitet.

Die Kopie ist in einem gängigen elektronischen Format oder auf Papier zur Verfügung zu stellen – je nach Art der Anfrage. Bei elektronischen Anträgen wird die Auskunft in der Regel auch elektronisch erteilt, sofern nichts anderes gewünscht wird.

Der Anspruch auf eine erste Kopie ist kostenlos. Für weitere Kopien kann der Verein ein angemessenes Entgelt auf Grundlage der Verwaltungskosten verlangen.

➢ Verfahren zur Auskunftserteilung

Ein Antrag auf Auskunft kann formfrei gestellt werden, sollte jedoch zur erleichterten Bearbeitung schriftlich oder per E-Mail erfolgen. Der Verein muss die Auskunft in der Regel innerhalb eines Monats erteilen. In Ausnahmefällen kann diese Frist um zwei weitere Monate verlängert werden, wenn der Antrag besonders komplex ist oder eine Vielzahl von Anträgen vorliegt. In diesem Fall ist der Antragsteller rechtzeitig zu informieren.

➢ Identitätsprüfung

Zum Schutz der Daten ist der Verein berechtigt, Nachweise zur Identität der anfragenden Person anzufordern – insbesondere dann, wenn Zweifel an der Berechtigung bestehen oder sensible Daten betroffen sind.

➢ Kosten

Die Auskunft ist grundsätzlich kostenlos. Nur bei offenkundig unbegründeten oder exzessiven Anträgen (z. B. wiederholte Auskünfte ohne sachlichen Grund) kann der Verein ein angemessenes Entgelt verlangen oder die Bearbeitung ablehnen.

NACH OBEN

4.3 Betroffeneninformation

Im Rahmen der Umsetzung der Datenschutz-Grundverordnung (DSGVO) trifft auch Vereine die Pflicht, betroffene Personen über die Erhebung und Verwendung ihrer personenbezogenen Daten zu informieren. Diese Pflicht besteht nicht nur im Zusammenhang mit einer Vereinswebsite, sondern auch bei allen Offline-Vorgängen, in denen personenbezogene Daten erstmals erhoben oder deren Verarbeitung geändert wird.

Möglicherweise haben Sie einen Teil Ihrer Pflichten hierzu bereits erfüllt, indem Sie die Maßnahmen nach Ziffer I. umgesetzt haben und Mitglieder bereits im Rahmen der Aufnahme des Mitgliedsverhältnisses über einige Datenverarbeitungen informiert haben.

Ziel ist es jedoch stets, Transparenz zu schaffen und den betroffenen Personen – also insbesondere Mitgliedern, Interessierten, Teilnehmenden oder Spendern – verständlich darzulegen, wie ihre Daten verarbeitet werden, auf welcher Rechtsgrundlage dies geschieht und welche Rechte ihnen zustehen.

➢ Relevante Anwendungsfälle

Die Informationspflicht gemäß Art. 13 DSGVO gilt bei jeder erstmaligen Datenerhebung, etwa bei folgenden Vorgängen:

- Aufnahme neuer Mitglieder,
- Anmeldung zu Veranstaltungen (inkl. Teilnehmerlisten),
- Entgegennahme von Spenden oder Anfragen,
- Durchführung von Öffentlichkeitsarbeit (z. B. bei Fotoveröffentlichungen),
- Gewinnung und Verarbeitung von Kontaktdaten für die Vereinskommunikation.

➢ Form und Inhalt der Information

Die Datenschutzinformation muss verständlich, transparent und leicht zugänglich sein. Sie muss insbesondere folgende Angaben enthalten:

- Zweck und Rechtsgrundlage der Datenverarbeitung,
- Name und Kontaktdaten des Vereins (Verantwortlicher),
- ggf. Kontaktdaten eines Datenschutzbeauftragten,
- Kategorien von Empfängern (z. B. Dachverbände, Dienstleister),
- Dauer der Speicherung,
- Rechte der betroffenen Person (Auskunft, Berichtigung, Löschung etc.),
- Hinweis auf das Beschwerderecht bei einer Datenschutzaufsichtsbehörde.

Ein ausreichendes Muster für eine Datenschutzinformation stellen wir im Anhang zu diesem Teil zur Verfügung. Es kann ohne Zustimmung der betroffenen Person übermittelt werden, sollte jedoch individuell angepasst werden – insbesondere an die konkreten Verarbeitungstätigkeiten Ihres Vereins.

➢ Umsetzung in der Vereinspraxis

Die Erfüllung der Informationspflicht muss nicht kompliziert sein. Ziel ist eine praktikable Lösung, die rechtlich sicher ist, aber den Verwaltungsaufwand so gering wie möglich hält.

Empfohlene Vorgehensweise:

- Online-Veröffentlichung:
  Stellen Sie das Informationsdokument auf Ihrer Vereinswebsite bereit und erzeugen Sie einen eindeutigen Link (z. B. „www.beispielverein.de/datenschutzinfo“).
- Verlinkung in der E-Mail-Signatur:
  Verwenden Sie einen Hinweis wie: „Informationen zur Datenverarbeitung im Verein“ finden Sie hier: [Link]“
- Beilegen bei schriftlicher Korrespondenz:
  Legen Sie die Datenschutzinformation der ersten postalischen Korrespondenz bei – etwa bei der Aufnahme neuer Mitglieder oder Veranstaltungsanmeldungen.

Alternativen:

- Versand als PDF-Anhang bei E-Mails,
- Abdruck einer Kurzinformation auf der Rückseite von Formularen oder Vereinsanschreiben,
- Auslage gedruckter Exemplare bei Veranstaltungen oder in Vereinsräumen.

➢ Dokumentation

Die erstmalige Information der betroffenen Person muss nicht durch eine Unterschrift bestätigt werden. Es genügt, die Übersendung zu dokumentieren, z. B. durch:

- Eintrag im Postausgangsverzeichnis,
- E-Mail-Archivierung mit Anhang,
- Vermerk auf dem Aufnahmeformular.

➢ Unterstützung durch Muster

Hier geht’s zum Mustertext zur Erfüllung der Informationspflicht gemäß Art. 13 DSGVO

NACH OBEN

5 Fotos und Veröffentlichungen bei Veranstaltungen

5.1 Hintergrund

Fotos von Vereinsmitgliedern, Sportlerinnen und Sportlern oder Besucherinnen und Besuchern von Vereinsveranstaltungen sind ein wichtiger Bestandteil der Öffentlichkeitsarbeit vieler Vereine. Sie illustrieren das Vereinsleben auf Websites, in sozialen Medien, im Vereinsheft oder in Presseberichten. Auch intern werden Fotos oft dokumentiert oder archiviert.

Wichtig: Die Veröffentlichung solcher Fotos ist datenschutzrechtlich relevant. Sie stellt eine Verarbeitung personenbezogener Daten dar – sowohl nach der Datenschutz-Grundverordnung (DSGVO) als auch nach dem Kunsturhebergesetz (KunstUrhG).

NACH OBEN

5.2 Rechtliche Anforderungen

Nach Art. 6 Abs. 1 DSGVO ist für die Veröffentlichung von Fotos in aller Regel die Einwilligung der betroffenen Person erforderlich.

Zusätzlich regelt § 22 KunstUrhG, dass „Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden“ dürfen.

Die Einwilligung muss informiert, freiwillig, eindeutig und widerruflich erfolgen.

NACH OBEN

5.3 Empfehlung: Schriftliche Einwilligung

Um rechtliche Risiken zu vermeiden – insbesondere Schadensersatzansprüche oder Bußgelder – empfiehlt sich der Einsatz einer schriftlichen Einwilligungserklärung.
Aus Praktikabilitätsgründen muss das konkrete Foto nicht benannt werden. Eine Eingrenzung auf einen konkreten Anlass (z. B. „Einwilligung zur Fotoverwendung im Rahmen des Sommerfests am 20.07.2025“) bietet eine praktikable und rechtssichere Alternative.

NACH OBEN

5.4 Zusätzlicher Hinweis bei Veranstaltungen

Vereine sollten Gäste und Teilnehmer bereits bei Veranstaltungen darauf hinweisen, dass Foto- und Videoaufnahmen gemacht werden – etwa durch Aushänge, Einladungen oder Hinweise auf der Website. Eine empfohlene Formulierung lautet:

Hinweis zu Foto- und Videoaufnahmen:
Im Rahmen dieser Vereinsveranstaltung werden Foto- und Videoaufnahmen gemacht, die im Rahmen unserer Öffentlichkeitsarbeit verwendet werden können. Dies betrifft insbesondere Veröffentlichungen auf unserer Vereinswebsite, in sozialen Medien, in Vereinszeitschriften oder in der regionalen Presse. Weitere Informationen entnehmen Sie bitte unserer Datenschutzerklärung unter: [LINK ZUR VEREINSWEBSITE].

NACH OBEN

5.5 Aufbewahrung und Widerruf

Die unterzeichnete Einwilligung sollte sicher dokumentiert und archiviert werden (z. B. digital oder in einem Datenschutzordner). Im Falle eines Widerrufs ist sicherzustellen, dass das entsprechende Foto nicht weiterverwendet und ggf. gelöscht wird.

NACH OBEN

5.6 Praxistipps

- Verwenden Sie das Muster angepasst an die jeweilige Veranstaltung.
- Kombinieren Sie die Einwilligung mit anderen Formularen (z. B. Teilnahmeformular).
- Weisen Sie Verantwortliche (z. B. Fotografen, Übungsleiter) auf das Einholen und den Umgang mit Einwilligungen hin.
- Denken Sie bei Minderjährigen immer an die Unterschrift der Erziehungsberechtigten.

Hier geht's zum Muster „Einwilligung zur Veröffentlichung von Foto- und Videoaufnahmen sowie personenbezogenen Daten."

NACH OBEN

6 Verzeichnis der Verarbeitungstätigkeiten

Ein zentrales Element der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO ist das sogenannte Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO. Auch Vereine sind verpflichtet, ein solches Verzeichnis zu führen – unabhängig von ihrer Größe, sofern die Datenverarbeitung nicht nur gelegentlich erfolgt.

Das Verzeichnis enthält für jede relevante Datenverarbeitung folgende Angaben:

- Zweck der Verarbeitung (z. B. Mitgliederverwaltung, Beitragsabrechnung),
- Beschreibung der betroffenen Personengruppen (z. B. Mitglieder, Ehrenamtliche),
- Art der verarbeiteten Daten (z. B. Name, Anschrift, Bankverbindung),
- Kategorien von Empfängern (z. B. Bank, Versicherung, Verband),
- geplante Fristen für die Löschung,
- Beschreibung der eingesetzten technischen und organisatorischen Maßnahmen.

Das Verzeichnis kann formlos erstellt werden, sollte jedoch stets aktuell gehalten werden. Es dient nicht nur der internen Organisation, sondern muss im Fall einer Datenschutzprüfung der Aufsichtsbehörde vorgelegt werden können.

NACH OBEN

6.1 Verarbeitungsverzeichnisse für Vereine

Einer der wichtigsten Bausteine im Rahmen Ihres Datenschutzmanagements sind Verarbeitungsverzeichnisse.

Sie sind nach Art. 30 DSGVO verpflichtet, alle Verarbeitungstätigkeiten innerhalb Ihres Vereins in einem Verzeichnis abzubilden. Hier besteht also eine Dokumentationspflicht.

Das Verzeichnis dient als zentrales Nachweis- und Steuerungsinstrument und ist der Aufsichtsbehörde auf Verlangen vorzulegen. Es hilft Ihnen, jederzeit einen Überblick über Ihre Datenverarbeitungen, deren Zwecke, Empfänger und Speicherfristen zu behalten.

Die in Art. 30 Abs. 5 DSGVO vorgesehene Ausnahme für kleine Organisationen greift bei Vereinen in der Praxis selten, weil Vereinsverarbeitungen wie Mitgliederverwaltung, Beitragseinzug, E-Mail-Kommunikation und der Betrieb einer Website nicht nur gelegentlich erfolgen und oft besondere Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) betreffen.

Fazit: Vereine sollten grundsätzlich ein Verarbeitungsverzeichnis führen.

NACH OBEN

6.2 Pflichtinhalte nach Art. 30 DSGVO

Für jede Verarbeitungstätigkeit müssen Sie mindestens dokumentieren:

- Bezeichnung des Verarbeitungsvorgangs,
- Verarbeitungszweck,
- Kategorien betroffener Personen,
- Kategorien verarbeiteter Daten,
- Kategorien der Empfänger,
- Datenübermittlung in Drittländer (ja/nein; ggf. wohin, auf welcher Rechtsgrundlage),
- Aufbewahrungsfrist.

Empfehlenswert ist zudem, im Kopf des Verzeichnisses den Verein als Verantwortlichen mit Kontaktangaben sowie ggf. den Datenschutzbeauftragten zu benennen.

NACH OBEN

6.3 Muster-Verzeichnis

Wir haben ein solches Verzeichnis – von denen Vereine sicher 20 bis 30 anlegen müssen – für Sie vorbereitet.

Hier geht's zum Muster Verzeichnis der Verarbeitungstätigkeiten

NACH OBEN

6.4 Beispiele für typische Verarbeitungsverzeichnisse im Verein

In Vereinen zeigen sich häufig wiederkehrend folgende Verarbeitungsmaßnahmen, für die Sie ein Verarbeitungsverzeichnis anlegen sollten:

- Mitgliederverwaltung (CRM),
- Aufnahmeverfahren (Mitgliedsantrag),
- Beitragsverwaltung & SEPA-Lastschriften,
- Spendenverwaltung & Zuwendungsbestätigungen,
- Mahnwesen,
- Ehrenamts-/Übungsleiterverwaltung,
- Bewerbungsverfahren (haupt- oder nebenamtliche Stellen),
- Personalakte (angestellte Mitarbeitende),
- Einsatzplan,
- Kontaktdatenbank (Vereinskontakte),
- Terminverwaltung (Kalender),
- Schlüssel-/Zutrittsverwaltung,
- Veranstaltungsanmeldungen (Kurse, Turniere, Fahrten),
- Foto-/Videoaufnahmen bei Vereinsveranstaltungen,
- Website & Social Media.

Legen Sie Ihre Verarbeitungsverzeichnisse also sorgfältig an, indem Sie alle relevanten Verarbeitungsvorgänge vollständig dokumentieren, diese mit den zuständigen Abteilungen in Ihrem Verein abstimmen und klare Verantwortlichkeiten festlegen.

Achten Sie auf eine einheitliche Struktur, aktualisieren Sie die Verzeichnisse regelmäßig und prüfen Sie neue Verarbeitungsvorgänge zeitnah.

Ziehen Sie bei Bedarf für die Erstellung und Verwaltung fachkundige Unterstützung hinzu, um Fehler zu vermeiden und die Anforderungen der DSGVO rechtssicher umzusetzen. Denn eine unvollständige oder fehlerhafte Dokumentation kann nicht nur zu organisatorischen Problemen führen, sondern auch empfindliche Bußgelder nach sich ziehen.

NACH OBEN

7 Datenschutzrichtlinie und Vereinssatzung

Die Datenschutz-Grundverordnung (DSGVO) verpflichtet Vereine auch zum verantwortungsvollen Umgang mit personenbezogenen Daten. Dabei empfiehlt es sich aus praktischen und rechtlichen Gründen, den Datenschutz im Verein strukturiert zu regeln – entweder durch eine eigene Datenschutzrichtlinie oder durch entsprechende Klauseln in der Vereinssatzung.

Die Vereinssatzung kann – insbesondere zur Transparenz gegenüber Mitgliedern – grundlegende Aussagen zum Datenschutz enthalten, etwa:

- Hinweis auf die Verarbeitung personenbezogener Daten im Rahmen der Mitgliedschaft,
- Verweis auf eine ergänzende Datenschutzrichtlinie,
- Information der Mitglieder zur Datenverarbeitung im Rahmen satzungsgemäßer Zwecke,

Die Satzung sollte keine Detailregelungen zur Datenverarbeitung enthalten, da Satzungsänderungen formalen Anforderungen unterliegen und mit größerem Aufwand verbunden sind. Vorzugswürdig ist daher eine flexibel anpassbare Datenschutzrichtlinie statt der Niederlegung von Hinweisen in der Satzung.

Die Datenschutzrichtlinie ist hingegen ein internes Dokument, das die praktische Umsetzung der DSGVO im Verein beschreibt. Sie kann z. B. folgende Punkte enthalten:

- Welche Daten zu welchen Zwecken erhoben werden (z. B. Mitgliederdaten, Teilnehmerlisten, Bankverbindungen),
- wer Zugriff auf welche Daten hat (z. B. Vorstand, Kassenwart, Übungsleiter),
- wie lange Daten gespeichert werden,
- technische und organisatorische Maßnahmen zum Schutz der Daten,
- Hinweise zur Veröffentlichung von Fotos und Berichten,
- Umgang mit Auskunftsverlangen, Löschungsanträgen und Datenschutzverletzungen.

Diese Richtlinie sollte allen Funktionsträgern bekannt sein und regelmäßig überprüft sowie bei Bedarf aktualisiert werden. Für Mitglieder sollte sie auf Anfrage oder im Mitgliederbereich zugänglich gemacht werden.

Hier geht's zum Muster für eine Datenschutzklausel in der Satzung

NACH OBEN

8 Aufbewahrungs- und Löschfristen

Die Pflicht zur Löschung personenbezogener Daten ist in Art. 17 DSGVO geregelt. Danach sind Daten unverzüglich zu löschen, sobald der Zweck der Speicherung entfällt oder keine gesetzliche Aufbewahrungspflicht mehr besteht. Für Vereine bedeutet dies, dass sie die Erforderlichkeit jeder gespeicherten Information regelmäßig überprüfen und dokumentieren müssen, wie lange und zu welchem Zweck sie bestimmte Daten speichern.

Ein häufiger Anwendungsfall ist das Ausscheiden von Mitgliedern: Hier dürfen personenbezogene Daten grundsätzlich nicht unbegrenzt gespeichert werden. Hat ein Mitglied den Verein verlassen, so sind dessen personenbezogene Daten zu löschen, sobald etwaige gesetzliche oder satzungsmäßige Verpflichtungen erfüllt und Fristen abgelaufen sind. Dies betrifft z. B. Abrechnungen, Versicherungsschutz, Nachweispflichten gegenüber dem Finanzamt oder dem Dachverband.

Für bestimmte Daten gelten gesetzlich geregelte Aufbewahrungsfristen, die auch Vereine beachten müssen. Beispielsweise:

- Buchhaltungsunterlagen und Rechnungen müssen 10 Jahre aufbewahrt werden (§ 147 AO).
- Geschäftsbriefe und sonstige relevante Korrespondenz 6 Jahre (§ 257 HGB).
- Zuwendungsbestätigungen (Spendenquittungen) mindestens 10 Jahre (§ 147 AO).

Die DSGVO verlangt zudem ein systematisches Löschkonzept. Dieses sollte aufzeigen, welche Datenarten zu welchem Zeitpunkt gelöscht oder archiviert werden. Eine sinnvolle Einteilung kann nach folgenden Kategorien erfolgen:

- Mitgliedsdaten,
- Veranstaltungsdokumentation (z. B. Fotos, Teilnehmerlisten),
- Spender- und Sponsoreninformationen,
- Daten aus Bewerbungsverfahren (z. B. für Ehrenämter).

Wichtig ist, dass die Löschung nicht nur technisch, sondern auch organisatorisch sichergestellt ist. Das bedeutet, dass neben elektronischen Daten auch analoge Akten rechtzeitig vernichtet werden müssen – idealerweise mit einem Aktenvernichter nach DIN 66399.

Ein weiterer Aspekt ist der Widerruf einer Einwilligung. Hat ein Mitglied oder eine andere betroffene Person ihre Zustimmung zur Datenverarbeitung widerrufen, so ist der Verein verpflichtet, die betreffenden Daten zu löschen, sofern keine vorrangigen gesetzlichen Gründe dagegensprechen.

Handlungsempfehlung:

- Erstellen Sie ein schriftliches Löschkonzept für alle relevanten Datenkategorien.
- Weisen Sie alle mit der Datenverarbeitung betrauten Personen auf ihre Pflichten hin.
- Überprüfen Sie regelmäßig die gespeicherten Datenbestände auf ihre Erforderlichkeit.
- Dokumentieren Sie jede Löschung nachvollziehbar – dies kann im Rahmen einer einfachen Löschprotokollvorlage erfolgen.

Ein gut gepflegtes Lösch- und Archivierungskonzept erhöht nicht nur die Rechtssicherheit, sondern schützt auch die personenbezogenen Daten Ihrer Mitglieder wirksam vor unberechtigtem Zugriff oder Missbrauch.

NACH OBEN

9 Mitgliedsantrag

Die Aufnahme neuer Mitglieder gehört zu den zentralen administrativen Abläufen in jedem Verein. Dabei werden regelmäßig personenbezogene Daten erhoben und verarbeitet – etwa Name, Kontaktdaten oder Bankverbindung. Diese Vorgänge unterliegen den Anforderungen der Datenschutz-Grundverordnung (DSGVO).

In diesem Teil erhalten Sie praxisorientierte Hinweise zur datenschutzkonformen Gestaltung Ihres Mitgliedsantrags. Ziel ist es, rechtliche Risiken zu vermeiden und gleichzeitig ein praktikables Verfahren für die Vereinsverwaltung zu schaffen.

NACH OBEN

9.1 Datensparsamkeit und Zweckbindung

Nach dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) dürfen nur solche Daten erhoben werden, die für die Begründung und Durchführung der Mitgliedschaft erforderlich sind. Dazu zählen in der Regel:

- Name, Adresse, Geburtsdatum,
- Kontaktdaten (E-Mail, Telefonnummer),
- Bankverbindung für den Beitragseinzug.

Nicht erforderlich sind z. B. Angaben zur beruflichen Tätigkeit oder familiären Situation – es sei denn, hierfür besteht ein sachlich begründeter Zweck, etwa zur Berechnung von Familienbeiträgen. Hier finden Sie ein Muster für die notwendigen Datenschutzregelungen auf dem Mitgliedsantrag.

NACH OBEN

9.2 Newsletter & zusätzliche Kommunikation

Der Vereinszweck allein deckt nicht automatisch die regelmäßige Zusendung eines Newsletters oder sonstiger Informations-E-Mails ab. Möchte der Verein seine Mitglieder zusätzlich zum Vereinsleben informieren, ist hierfür eine gesonderte Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO erforderlich.

Empfehlung: Integrieren Sie im Mitgliedsantrag eine freiwillig ankreuzbare Einwilligung mit folgendem Wortlaut:

[ ] Ich möchte den Vereins-Newsletter mit Neuigkeiten zum Vereinsleben per E-Mail erhalten. Ich kann diese Einwilligung jederzeit widerrufen.

Damit wird die Freiwilligkeit und Nachweisbarkeit der Einwilligung gewahrt – ein zentrales Kriterium der DSGVO.

NACH OBEN

9.3 Einwilligung in die Veröffentlichung von Fotos

Viele Mitgliedsanträge enthalten Passagen zur Einwilligung in die Veröffentlichung von Fotos, etwa auf der Vereinswebsite oder in Presseberichten. In der Praxis sind diese Klauseln jedoch oft zu allgemein gefasst und damit nicht wirksam.

Eine wirksame Einwilligung muss klar, verständlich, freiwillig und für einen konkreten Zweck formuliert sein. Idealerweise sollte sie kontextbezogen (z. B. „im Rahmen von Vereinsveranstaltungen“) sein und freiwillig durch Ankreuzen erteilt werden.

Empfehlung:

[ ] Ich bin damit einverstanden, dass Fotos von meiner Person, die im Rahmen von Vereinsveranstaltungen entstehen, auf der Website und in Printmedien des Vereins veröffentlicht werden dürfen. Diese Einwilligung kann ich jederzeit mit Wirkung für die Zukunft widerrufen.

Auch wenn eine solche Einwilligung nicht alle denkbaren Risiken abdeckt, stellt sie eine praxistaugliche Lösung dar. Wichtig ist: Löschungsaufforderungen müssen jederzeit umgesetzt werden.

NACH OBEN

9.4 Datenschutzinformation nach Art. 13 DSGVO

Neben dem eigentlichen Antrag ist der Verein verpflichtet, jede betroffene Person transparent über die Datenverarbeitung zu informieren. Diese sogenannte Datenschutzinformation muss unter anderem enthalten:

- Welche Daten verarbeitet werden und zu welchem Zweck,
- auf welcher Rechtsgrundlage dies geschieht,
- wer Zugriff auf die Daten hat (z. B. Vorstand, Abteilungen),
- wie lange die Daten gespeichert werden,
- welche Rechte die betroffene Person hat (Auskunft, Berichtigung, Löschung etc.),
- Kontaktdaten des Vereins und ggf. des Datenschutzbeauftragten.

Empfehlung: Fügen Sie die Datenschutzinformation als separate Seite dem Mitgliedsantrag bei und ergänzen Sie diesen durch einen Hinweis wie:

„Ich habe die anliegenden Datenschutzhinweise zur Kenntnis genommen."

Hinweis: Auch Bestandsmitglieder haben Anspruch auf diese Information. Bei nächster Gelegenheit (z. B. per Rundschreiben oder Mitgliederbrief) sollte die Datenschutzinformation auch ihnen zur Verfügung gestellt werden.

NACH OBEN

9.5 Zusammenfassung: Ihre To-do-Liste

- Nur notwendige Daten abfragen (Datenminimierung),
- gesonderte Einwilligung für Newsletter oder Fotos einholen,
- Datenschutzinformation beifügen,
- Einwilligungen dokumentieren (schriftlich oder elektronisch),
- Bestandsmitglieder nachträglich informieren.

Hier geht‘ s zum Muster „Mitgliedsantrag nebst Datenschutzinformation“.

NACH OBEN

10 Datenschutzerklärung Website

Die Bereitstellung einer Datenschutzerklärung auf der Vereinswebsite gehört zu den grundlegenden Pflichten im Rahmen der DSGVO. Jeder Verein, der eine Website betreibt, auf der personenbezogene Daten verarbeitet werden – z. B. über Kontaktformulare, eingebettete Inhalte oder Analyse-Tools – ist verpflichtet, Websitebesucher über Art, Umfang und Zweck der Datenverarbeitung zu informieren.

Ziel dieses Teils ist es, Vereinsverantwortlichen zu erklären, wie eine rechtssichere Datenschutzerklärung aufgebaut ist, welche Bestandteile erforderlich sind – und wie diese an die individuelle technische Konfiguration des Vereins angepasst werden müssen.

NACH OBEN

10.1 Rechtsgrundlage

Die Informationspflicht ergibt sich insbesondere aus:

- Art. 12–14 DSGVO (Informationspflichten bei Datenerhebung),
- Art. 5 Abs. 1 lit. a DSGVO (Transparenz),
- § 25 TDDDG (früher TTDSG, zur Verwendung von Cookies und Tracking-Tools).

Die Datenschutzerklärung muss leicht auffindbar und dauerhaft verfügbar sein, z. B. über einen deutlich sichtbaren Link im Footer der Website.

NACH OBEN

10.2 Ausgangspunkt: Musterdatenschutzerklärung

Dem „Startpaket Datenschutz“ liegt ein Muster für eine umfassende Datenschutzerklärung bei. Dieses deckt die meisten datenschutzrechtlich relevanten Themen für Vereinswebsites ab, darunter:

- Allgemeine Informationen zum Verantwortlichen,
- Rechtsgrundlagen der Datenverarbeitung,
- Erhebung technischer Zugriffsdaten beim Websitenbesuch,
- Verwendung von Cookies und Tracking-Technologien,
- Einsatz externer Dienste (z. B. Google Maps, Social Plugins, WordPress-Plugins),
- Hinweise auf Rechte der betroffenen Personen.

NACH OBEN

10.3 Anpassungsbedarf: Warum das Muster nicht automatisch ausreicht

Da viele Vereinswebsites individuell gestaltet und technisch unterschiedlich ausgestattet sind, muss die Datenschutzerklärung stets konkret auf die eingesetzten Tools, Plugins und externen Dienste angepasst werden.

Typische Ergänzungen oder Prüfbereiche sind:

Technische Funktion / Plugin	Anpassung erforderlich?
Google Maps / YouTube-Einbindung	ja – Datenschutzhinweis zu Google-Diensten erforderlich
WordPress-Plugins (z. B. Kontaktformular)	ja – je nach Plugintyp
FUSSBALL.DE Widget	ja – IP-Übermittlung an DFB, Einwilligung erforderlich
Social Media Links / 2-Klick-Lösungen	ja – Hinweis auf externe Datenübermittlung
Analyse-Tools (z. B. Matomo, Google Analytics)	ja – Cookie-Hinweis und Einwilligung notwendig
Newsletter-Tools / Formulare	ja – Zweck, Anbieter, Opt-In-Verfahren erläutern

Empfehlung: Führen Sie eine kurze Funktionsprüfung Ihrer Website durch (ggf. gemeinsam mit Ihrer Webagentur) und notieren Sie, welche Services aktiv eingebunden sind. Ergänzen oder löschen Sie dann im Muster gezielt einzelne Textbausteine.

NACH OBEN

10.4 Cookie-Einwilligung: Rechtssicher gestalten

Sobald auf Ihrer Website nicht-funktionale Cookies eingesetzt werden (z. B. für Analyse, Werbung oder Social Media), muss vor deren Aktivierung eine aktive Einwilligung der Nutzer erfolgen. Dies erfolgt über ein Cookie-Banner mit Auswahlmöglichkeit (Consent Manager).

Die Datenschutzerklärung muss dazu klarstellen:

- welche Cookies gesetzt werden,
- zu welchem Zweck,
- durch welche Anbieter,
- wie lange sie aktiv bleiben,
- wie die Einwilligung widerrufen werden kann.

NACH OBEN

10.5 Mindestanforderungen an die Darstellung

Die Datenschutzerklärung sollte:

- als eigenständige Seite oder Abschnitt mit direktem Link erreichbar sein,
- in klarer und verständlicher Sprache verfasst sein,
- alle Pflichtangaben nach Art. 13 und 14 DSGVO enthalten,
- ggf. in mehreren Sprachen angeboten werden (z. B. bei internationalen Turnieren).

NACH OBEN

10.6 Hinweise zur Pflege und Aktualisierung

Da sich datenschutzrechtliche Anforderungen und technische Systeme laufend ändern, sollte die Datenschutzerklärung mindestens jährlich überprüft und bei technischen Änderungen (neues Plugin, Newslettertool etc.) sofort angepasst werden.

NACH OBEN

10.7 Zusammenfassung: Ihre To-do-Liste

- Musterdatenschutzerklärung als Ausgangspunkt verwenden,
- eingesetzte Dienste und Plugins auf der Website erfassen,
- Inhalte individuell anpassen (z. B. Google Maps, FUSSBALL.de etc.),
- Cookie-Banner prüfen und mit der Erklärung abstimmen,
- Datenschutzerklärung auf der Website gut sichtbar verlinken,
- Bei Änderungen aktualisieren, Datum anpassen.

Hier geht's zum Muster „Datenschutzerklärung Website".

NACH OBEN

11 Technisch-organisatorische Maßnahmen

Die Datenschutzgrundverordnung verpflichtet alle Verantwortlichen, geeignete technische und organisatorische Maßnahmen (TOMs) zu treffen, um ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten (Art. 32 DSGVO). Diese Maßnahmen sind nicht optional, sondern verpflichtend – auch für Vereine. Dabei ist nicht entscheidend, ob ein Verein über eine professionelle IT-Infrastruktur verfügt. Vielmehr kommt es auf die konkrete Verarbeitungssituation und die möglichen Risiken für die Rechte und Freiheiten der betroffenen Personen an.

Die im „Startpaket Datenschutz“ beschriebenen technisch-organisatorischen Maßnahmen lassen sich um weitere Aspekte aus der Praxis ergänzen. Von zentraler Bedeutung ist die Passwortsicherheit. Der Verein sollte verbindliche Vorgaben für die Erstellung und Verwendung von Passwörtern aufstellen. Dazu gehört, dass Passwörter nicht weitergegeben, regelmäßig erneuert und nicht mehrfach für unterschiedliche Anwendungen genutzt werden dürfen. Auch triviale Passwörter wie „12345“ oder einfache Wörter sind strikt zu vermeiden.

Darüber hinaus spielt die Gerätesicherheit eine Rolle. Jeder Computer oder jedes mobile Endgerät, das für Vereinszwecke verwendet wird, muss beim Start mit einem Passwort geschützt sein und sollte bei Abwesenheit des Nutzers unverzüglich gesperrt werden. Eine automatische Bildschirmsperre nach wenigen Minuten Inaktivität ist eine einfache und wirksame Maßnahme. Besonders bei mobilen Geräten wie Laptops oder Smartphones ist zudem eine vollständige Verschlüsselung der Festplatte zu empfehlen.

Da viele Vereinsmitglieder auch unterwegs an Vereinsangelegenheiten arbeiten, sollte auf die Verwendung öffentlicher Hotspots verzichtet werden. Um die Vertraulichkeit auch in öffentlichen Räumen zu wahren, kann der Einsatz von Sichtschutzfolien auf Bildschirmen sinnvoll sein. Ebenso ist darauf zu achten, dass vertrauliche Gespräche nicht in der Öffentlichkeit geführt werden, wo Dritte mithören könnten.

Ein weiterer Bereich betrifft die Abwehr von sogenannten Phishing- und Spoofing-Angriffen. Vereinsverantwortliche sollten regelmäßig für die Gefahr sensibilisiert werden, dass Betrüger per E-Mail oder Telefon versuchen, an vertrauliche Informationen zu gelangen. Ein gesundes Misstrauen gegenüber unerwarteten Datenanfragen ist hier geboten.

Schließlich sollten auch Maßnahmen wie die Pseudonymisierung und die strikte Trennung von Datenquellen beachtet werden. Werden personenbezogene Daten durch Codes ersetzt, sodass ein Rückschluss auf die betroffene Person nur mit Zusatzinformationen möglich ist, erhöht dies den Schutz bei internen Auswertungen. Ebenso ist darauf zu achten, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, nicht ohne rechtliche Grundlage zusammengeführt werden dürfen. Eine klare organisatorische Trennung von Mitglieder-, Spender- oder Mitarbeiterdaten kann hier Missbrauch verhindern.

Darüber hinaus sind Kontrollen der Datenweitergabe einzurichten. Personenbezogene Daten dürfen nur über sichere Kanäle übermittelt werden. Der Versand per E-Mail sollte nach Möglichkeit verschlüsselt erfolgen; bei Sammel-E-Mails an mehrere Empfänger ist die Verwendung der Blindkopie-Funktion („bcc“) zwingend notwendig, um unbefugte Einblicke in die Adressen anderer Mitglieder zu verhindern. Ebenso wichtig ist eine Eingabekontrolle: Es muss dokumentiert werden können, welche Person wann welche Daten in Systeme eingegeben oder verändert hat.

Ein Verein, der ausschließlich mit Papierlisten arbeitet, hat andere Anforderungen als ein Verein, der seine Mitgliederdaten digital verwaltet, online kommuniziert oder mit Cloud-Diensten arbeitet. Dennoch gelten die Grundprinzipien der Datensicherheit für alle gleichermaßen.

NACH OBEN

11.1 Zutrittskontrolle

Ziel ist es, Unbefugten den physischen Zugang zu den Bereichen zu verwehren, in denen personenbezogene Daten verarbeitet werden. Das betrifft etwa Vereinsbüros, Lagerräume mit Akten oder auch Serverräume, soweit vorhanden.

Empfehlungen:

- Nutzung abschließbarer Schränke oder Räume für personenbezogene Unterlagen.
- Zugang nur für autorisierte Personen (z. B. Vorstand, Mitgliederverwaltung).
- Bei Veranstaltungen: Sichere Aufbewahrung von Listen oder Dokumenten.

NACH OBEN

11.2 Zugriffskontrolle

Diese Maßnahme soll verhindern, dass unbefugte Personen auf IT-Systeme oder Akten zugreifen. Dazu gehört insbesondere der Schutz von Computern, E-Mail-Konten und Online-Portalen.

Empfehlungen:

- Passwörter für Benutzerkonten einrichten und regelmäßig ändern.
- Keine gemeinsame Nutzung von Benutzerkonten.
- Zugang zu Software nur für berechtigte Personen.
- Regelmäßige Sperrung von nicht mehr benötigten Nutzerkonten (z. B. nach Vorstandswechsel)

NACH OBEN

11.3 Zugriffsbeschränkungen innerhalb des Vereins

Nicht jede Person im Verein braucht Zugriff auf alle Daten. Eine rollenbasierte Rechtevergabe stellt sicher, dass nur diejenigen Zugang zu personenbezogenen Daten erhalten, die diese für ihre Aufgaben benötigen.

Beispiele:

- Kassierer*innen dürfen auf Bankverbindungen zugreifen, nicht aber auf Gesundheitsdaten.
- Trainer*innen erhalten nur die für den Trainingsbetrieb notwendigen Daten

NACH OBEN

11.4 Verschlüsselung und sichere Übertragung

Personenbezogene Daten, die per E-Mail oder über Online-Formulare übermittelt werden, sollten verschlüsselt übertragen werden. Insbesondere bei sensiblen Daten (z. B. Krankmeldungen, Minderjährigen) ist dies unerlässlich.

Empfehlungen:

- Nutzung von TLS-verschlüsselten E-Mail-Diensten.
- Vermeidung der Versendung sensibler Daten per ungesicherter E-Mail.
- Cloud-Dienste mit Ende-zu-Ende-Verschlüsselung bevorzugen.

NACH OBEN

11.5 Schutz mobiler Geräte

Viele Vereinsverantwortliche nutzen private oder mobile Endgeräte (z. B. Laptops, Tablets oder Smartphones) für die Vereinsarbeit. Auch hier gelten die Anforderungen der DSGVO.

Empfehlungen:

- Nutzung sicherer Geräte mit Passwortschutz.
- Bei Verlust: Möglichkeit zur Fernlöschung.
- Keine dauerhafte Speicherung sensibler Daten auf privaten Geräten.

NACH OBEN

11.6 Datensicherung und Wiederherstellung

Verluste durch Systemabstürze, Schadsoftware oder Fehlbedienung können auch in Vereinen schnell erhebliche Schäden anrichten. Daher sind regelmäßige Backups erforderlich.

Empfehlungen:

- Regelmäßige Sicherung von Datenbeständen (z. B. Mitgliederdatenbank).
- Backups an getrenntem Ort oder auf externem Datenträger.
- Protokollierung von Sicherungen und Wiederherstellungstests.

NACH OBEN

11.7 Schutz vor Einsichtnahme und Mithören

Auch der Schutz vor zufälligem Mitlesen oder Mithören gehört zu den organisatorischen Grundpflichten. Dies betrifft z. B. Gespräche über Mitgliedsdaten in öffentlichen Räumen oder offen herumliegende Listen.

Empfehlungen:

- Sichtschutzfilter auf mobilen Geräten in öffentlicher Umgebung.
- Sensibilisierung für Datenschutz bei Telefonaten.
- Keine öffentlichen Aushänge mit personenbezogenen Daten (z. B. vollständige Teilnehmerlisten).

NACH OBEN

11.8 Aktenvernichtung

Nicht mehr benötigte Dokumente mit personenbezogenen Daten dürfen nicht einfach im Papierkorb entsorgt werden.

Empfehlungen:

- Vernichtung mit Aktenvernichtern gemäß DIN 66399.
- Bei externer Entsorgung: Vertrauenswürdige Dienstleister wählen.
- Dokumentation von Vernichtungsvorgängen bei sensiblen Daten.

NACH OBEN

11.9 Datenschutz bei Veranstaltungen

Bei Vereinsfesten, Turnieren oder öffentlichen Auftritten entstehen häufig Foto- oder Videoaufnahmen. Diese fallen unter den Datenschutz, sobald Personen darauf eindeutig erkennbar sind.

Empfehlungen:

- Vorab Einwilligung zur Nutzung von Bildern einholen (insbesondere bei Minderjährigen).
- Teilnehmer im Vorfeld transparent informieren (z. B. Aushänge, Anmeldung).
- Bei Veröffentlichung in sozialen Netzwerken: gesonderte Freigabe einholen.

NACH OBEN

11.10Vertraulichkeit, Sensibilisierung und Schulung

Technische Maßnahmen sind nur wirksam, wenn auch das Bewusstsein für Datenschutz vorhanden ist. Daher ist es wichtig, alle mit Datenverarbeitung betrauten Personen regelmäßig zu schulen und für Risiken zu sensibilisieren.

Empfehlungen:

- Kurze Infoblätter oder Leitfäden für Vorstandsmitglieder.
- Einführungsschulungen für neue Verantwortliche.
- Hinweise auf aktuelle Gefahren (Phishing, Datendiebstahl).

Hierbei kann sich auch als sinnvoll erweisen, den Vorstand zur Vertraulichkeit zu verpflichten. Bereits aus ihrer treuepflichtigen Stellung ergibt sich für Vorstandsmitglieder zwar eine gesetzliche Verschwiegenheitspflicht. Diese Pflicht betrifft sowohl vereinsinterne Belange als auch personenbezogene Daten nach Art. 5 ff. DSGVO. Eine ausdrückliche Vertraulichkeitsverpflichtung ist jedoch sinnvoll, um Klarheit zu schaffen und zur Sensibilisierung beizutragen. Eine solche Erklärung könnte beinhalten:

„Ich verpflichte mich, alle mir im Rahmen meiner Vorstandstätigkeit bekannt gewordenen personenbezogenen Daten sowie sonstige vertrauliche Informationen über den Verein, seine Mitglieder und Partnerorganisationen streng vertraulich zu behandeln. Diese Verpflichtung gilt über die Dauer meines Amtes hinaus."

Nach Art. 32 DSGVO sind Vereine in der Konsequenz verpflichtet, geeignete technische und organisatorische Maßnahmen (TOM) zu treffen, die die Sicherheit der verarbeiteten personenbezogenen Daten gewährleisten. Das betrifft sämtliche Verarbeitungsvorgänge – von der Mitgliederverwaltung bis hin zur Veranstaltungsorganisation oder Öffentlichkeitsarbeit.

Die TOM dienen dazu, ein dem Risiko angemessenes Schutzniveau zu erreichen. Berücksichtigt werden müssen dabei insbesondere:

- Stand der Technik,
- Kosten der Implementierung,
- Art, Umfang, Umstände und Zwecke der Verarbeitung,
- Eintrittswahrscheinlichkeit und Schwere möglicher Risiken für die Rechte und Freiheiten der Betroffenen.

Für Vereine bedeutet dies: Der Schutzbedarf ist oft niedriger als bei Großunternehmen, aber auch Vereine verarbeiten sensible Daten (z. B. Gesundheitsdaten im Sportbereich, Fotos, Bankdaten). Ein TOM-Verzeichnis ist deshalb Pflicht. Es dokumentiert vorhandene Schutzmaßnahmen, dient als Nachweis gegenüber Aufsichtsbehörden und unterstützt die interne Organisation.

Hierzu kann das Muster verwendet werden, wobei die technisch-organisatorischen Maßnahmen im Verein ergänzt werden sollten.

Hier geht's zum Muster „Verzeichnis Technisch-Organisatorische Maßnahmen".

NACH OBEN

12 Auftragsverarbeitung

Viele Vereine greifen bei der Erfüllung ihrer Aufgaben auf externe Dienstleister zurück – etwa für die Verwaltung von Mitgliedsdaten über Vereinssoftware, das Hosting der Vereinswebsite, die Nutzung von Cloud-Diensten, Buchhaltungsdienstleistungen oder den Versand von Newslettern. In all diesen Fällen kann es vorkommen, dass Dritte im Auftrag des Vereins personenbezogene Daten verarbeiten. Solche Konstellationen fallen unter den Begriff der Auftragsverarbeitung im Sinne von Art. 28 DSGVO.

Eine Auftragsverarbeitung liegt vor, wenn ein externer Dienstleister weisungsgebunden im Auftrag des Vereins personenbezogene Daten verarbeitet, ohne dabei selbst für die Verarbeitung verantwortlich zu sein. Wichtig ist, dass der Verein in diesen Fällen weiterhin als datenschutzrechtlich „Verantwortlicher" gilt – er bleibt also für die Einhaltung der gesetzlichen Vorgaben vollumfänglich zuständig.

Typische Beispiele für Auftragsverarbeiter:

- Anbieter von Vereinsverwaltungssoftware (z. B. cloudbasierte Mitgliederverwaltung),
- IT-Dienstleister, die Server betreiben oder Wartung durchführen,
- Online-Bezahldienste, die Spenden oder Mitgliedsbeiträge abwickeln,
- E-Mail-Versanddienste für Vereinskommunikation (z. B. Mailchimp, CleverReach),
- Dienstleister für Druck und Versand von Mitgliederzeitschriften.

In allen Fällen muss mit dem jeweiligen Dienstleister ein Vertrag über die Auftragsverarbeitung (AV-Vertrag) abgeschlossen werden. Dieser Vertrag regelt unter anderem:

- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Datenverarbeitung,
- Art der personenbezogenen Daten und Kategorien betroffener Personen,
- Pflichten und Rechte des Verantwortlichen (Verein),
- technische und organisatorische Maßnahmen beim Auftragsverarbeiter,
- Unterauftragsverhältnisse,
- Rückgabe oder Löschung der Daten nach Auftragsende.

Der Vertrag muss in schriftlicher oder elektronischer Form vorliegen und spätestens bei Aufnahme der Datenverarbeitung abgeschlossen werden. Ein Verstoß gegen diese Pflicht stellt eine Ordnungswidrigkeit dar und kann mit einem Bußgeld belegt werden.

Wichtig ist außerdem, dass der Verein sich vor Vertragsabschluss davon überzeugt, dass der Dienstleister geeignete technische und organisatorische Maßnahmen zum Schutz der Daten getroffen hat. Eine entsprechende Dokumentation dieser Prüfung sollte aufbewahrt werden.

Werden Daten an Anbieter außerhalb der EU oder des Europäischen Wirtschaftsraums (EWR) übermittelt, gelten besondere Voraussetzungen. In solchen Fällen ist zusätzlich zu prüfen, ob im Zielland ein angemessenes Datenschutzniveau besteht. Liegt kein Angemessenheitsbeschluss der EU-Kommission vor, können sogenannte Standardvertragsklauseln erforderlich sein. Für US-Anbieter ist das aktuelle Datenschutzabkommen „EU-U.S. Data Privacy Framework" relevant, sofern der Dienstleister daran teilnimmt.

Handlungsempfehlungen für Vereine:

- Erfassen Sie alle Dienstleister, die in Ihrem Auftrag personenbezogene Daten verarbeiten.
- Schließen Sie mit diesen AV-Verträge nach Art. 28 DSGVO ab – ggf. unter Nutzung von Mustern.
- Dokumentieren Sie die Prüfung der datenschutzrechtlichen Eignung des Dienstleisters.
- Bevorzugen Sie nach Möglichkeit europäische Anbieter.
- Achten Sie bei der Auswahl auf Transparenz, technische Sicherheitsstandards und Seriosität.

NACH OBEN

12.1 Was ist Auftragsverarbeitung?

Die Auftragsverarbeitung ist in Art. 28 DSGVO geregelt. Sie liegt immer dann vor, wenn der Verein sich eines externen Dienstleisters bedient, der personenbezogene Daten im Auftrag und auf Weisung des Vereins verarbeitet, ohne die Daten für eigene Zwecke zu verwenden.

Typische Fälle im Vereinskontext:

- Vernichtung alter Mitgliederlisten durch einen Aktenvernichter-Dienst,
- Pflege oder Wartung der Vereinssoftware durch einen IT-Dienstleister,
- Hosting der Vereinswebsite durch einen Webprovider,
- Durchführung der Lohn- oder Mitgliedsbeitragsabrechnung durch eine externe Buchhaltung,
- Betrieb eines E-Mail-Newsletters durch einen externen Dienst.

Wichtig: Für diese Art der Datenverarbeitung ist zwingend ein Auftragsverarbeitungsvertrag abzuschließen, da der Dienstleister nicht selbst für die Daten verantwortlich ist, sondern ausschließlich im Auftrag des Vereins handelt.

NACH OBEN

12.2 Wann liegt keine Auftragsverarbeitung vor?

Keine Auftragsverarbeitung liegt vor, wenn der externe Dritte die personenbezogenen Daten nicht im Auftrag, sondern für eigene Zwecke verarbeitet – etwa zur Erfüllung eigener rechtlicher oder vertraglicher Pflichten gegenüber der betroffenen Person. In diesen Fällen spricht man von einer Funktionsübertragung, die eine andere rechtliche Grundlage erfordert, aber keinen AVV.

Beispiele:

- Postdienstleister (z. B. Versand von Einladungen oder Mitgliederzeitschriften),
- Steuerberater, Rechtsanwälte, Notare,
- Inkassounternehmen,
- Personalvermittler,
- Finanz- oder Versicherungsberater.

Hier agiert der Dienstleister als eigenständig Verantwortlicher. Statt eines AV-Vertrags ist eine Rechtsgrundlage für die Weitergabe erforderlich – etwa:

- Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung),
- Art. 6 Abs. 1 lit. a DSGVO (Einwilligung),
- oder ein berechtigtes Interesse gem. Art. 6 Abs. 1 lit. f DSGVO.

NACH OBEN

12.3 Sonderfall: Keine Weitergabe im datenschutzrechtlichen Sinne

Es gibt auch Fälle, in denen weder eine Auftragsverarbeitung noch eine Weitergabe personenbezogener Daten vorliegt – etwa weil keine personenbezogenen Daten verarbeitet werden oder diese Personen nicht bestimmbar sind. In diesen Fällen ist weder ein AV-Vertrag noch eine Einwilligung erforderlich, ggf. aber eine Vertraulichkeitsvereinbarung.

Beispiele:

- Reinigungs- und Hausmeisterdienste,
- Raumausstatter,
- Reparaturdienstleister,
- sonstige Helfer ohne Datenzugang.

Dennoch sollten technisch-organisatorische Maßnahmen (z. B. Verschluss von Akten, Zugriffsbeschränkungen) vorgesehen werden, um ungewollte Datenzugriffe zu verhindern.

NACH OBEN

12.4 Vertragsmuster und Umsetzung

Ein Muster für einen Auftragsverarbeitungsvertrag stellen wir Ihnen im Anhang dieses Teils zur Verfügung. Dieses ist für all jene Dienstleister zu verwenden, die im Auftrag des Vereins personenbezogene Daten verarbeiten, ohne sie selbst weiter zu nutzen.

Empfehlung:

- Verwenden Sie nach Möglichkeit das bereitgestellte Muster.
- Achten Sie darauf, dass keine nachteiligen Haftungsregelungen zulasten des Vereins aufgenommen sind.
- Prüfen Sie im Zweifel vorab, ob wirklich eine Auftragsverarbeitung vorliegt – wir unterstützen Sie gerne dabei.

Wichtig: Viele Dienstleister bieten eigene AV-Verträge an. Diese sollten sorgfältig geprüft werden. Haftungsausschlüsse zu Ungunsten des Vereins oder unvollständige Regelungen sollten nicht ohne rechtliche Prüfung akzeptiert werden.

NACH OBEN

12.5 Zusammenfassung: Ihre To-do-Liste

- Erfassen Sie alle externen Dienstleister mit Datenzugriff.
- Prüfen Sie, ob Daten im Auftrag oder für eigene Zwecke verarbeitet werden.
- Schließen Sie bei Auftragsverarbeitung einen AV-Vertrag ab.
- Verwenden Sie möglichst das bereitgestellte Muster.
- Achten Sie auf unfaire Haftungsregelungen in Fremdverträgen.
- Dokumentieren Sie alle abgeschlossenen AV-Verträge systematisch (z. B. in einem Datenschutzordner).
- Verwenden Sie ein **Muster** wie das anliegende.

Hier geht's zum Mustervertrag „Auftragsverarbeitung personenbezogener Daten".

NACH OBEN

13 Internationale Bezüge und Nutzung externer Dienste

Auch wenn viele Vereine lokal agieren, nutzen sie doch häufig digitale Dienste, die in datenschutzrechtlicher Hinsicht eine internationale Komponente haben – etwa Cloud-Dienste, Messenger oder Newsletter-Plattformen. Wenn personenbezogene Daten in sogenannte Drittländer übermittelt werden (z. B. in die USA), ist zu prüfen, ob dort ein angemessenes Datenschutzniveau besteht. Die DSGVO nennt hierfür klare Bedingungen in den Artikeln 44 bis 49.

So kann eine Übermittlung zulässig sein, wenn:

- ein Angemessenheitsbeschluss der EU-Kommission für das betreffende Land vorliegt,
- Standarddatenschutzklauseln mit dem Anbieter abgeschlossen wurden,
- die betroffene Person ausdrücklich eingewilligt hat.

Im Zweifel sollte auf europäische Anbieter zurückgegriffen werden, um die Einhaltung der DSGVO einfacher und sicherer zu gestalten.

Handlungsempfehlung:

- Prüfen Sie eingesetzte Softwarelösungen auf DSGVO-Konformität.
- Nutzen Sie möglichst europäische Anbieter mit Serverstandorten in der EU.
- Dokumentieren Sie alle datenschutzrechtlich relevanten Entscheidungen.

Die praktische Umsetzung des Datenschutzes im Verein erfordert also keine Perfektion, wohl aber ein systematisches und verantwortungsvolles Vorgehen. Mit Transparenz, Dokumentation und der Bereitschaft zur kontinuierlichen Verbesserung lassen sich die Anforderungen der DSGVO gut in den Vereinsalltag integrieren.

NACH OBEN

14 Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) ist ein zentrales Instrument der DSGVO, um Risiken für die Rechte und Freiheiten betroffener Personen frühzeitig zu erkennen und angemessen zu steuern. Vereine müssen in bestimmten Fällen vor Einführung einer Datenverarbeitung prüfen, ob eine DSFA erforderlich ist – insbesondere bei technischen Maßnahmen mit hohem Risiko, wie z. B. bei der Einrichtung einer Videoüberwachung.

NACH OBEN

14.1 Wann ist eine DSFA durchzuführen?

Gemäß Art. 35 DSGVO ist eine DSFA durchzuführen, wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat – insbesondere wenn:

- eine systematische Überwachung öffentlicher Bereiche erfolgt,
- sensible oder besonders schutzwürdige Daten verarbeitet werden (z. B. Gesundheitsdaten),
- eine umfassende Bewertung des Verhaltens oder der Persönlichkeit stattfindet,
- automatisierte Entscheidungen mit Rechtswirkung getroffen werden.

Beispiel: Videoüberwachung in Vereinsräumen oder -geländen

Die Einrichtung von Kameras, etwa zur Überwachung von Eingangsbereichen, Vereinsheimen oder Sportanlagen, erfasst regelmäßig personenbezogene Daten und kann einen Überwachungsdruck erzeugen. Daher ist hier regelmäßig eine DSFA erforderlich, es sei denn, es liegt ein Ausnahmefall mit minimalem Risiko vor (z. B. reine Attrappen oder ausschließlich privater Bereich).

NACH OBEN

14.2 Ablauf der Datenschutz-Folgenabschätzung

Eine DSFA muss vor Beginn der Verarbeitung durchgeführt werden und mindestens folgende Punkte umfassen:

- **Beschreibung der geplanten Verarbeitung**

Was soll verarbeitet werden? Wer ist verantwortlich? Welche Technik wird eingesetzt?

Beispiel: 3 fest installierte Kameras im Eingangsbereich des Vereinsheims, Aufzeichnung auf lokalem Rekorder, Zugriff nur durch Vorstand.

- **Bewertung der Notwendigkeit und Verhältnismäßigkeit**

Gibt es eine rechtliche Grundlage? Ist die Maßnahme geeignet, erforderlich und angemessen?

Beispiel: Schutz vor Einbruch und Vandalismus – keine milderen Mittel (z. B. Beleuchtung, Zugangskontrolle) vorhanden.

- **Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen**

Mögliche Risiken: unbeobachtete Überwachung, falscher Eindruck von Überwachung im Privatbereich, Datenmissbrauch bei Zugriff.

- **Maßnahmen zur Risikominderung**
  - Klare Beschilderung der Videoüberwachung,
  - Zugriffsbeschränkung durch Passwortschutz,
  - automatische Löschung der Aufnahmen nach 48 Stunden,
  - keine Überwachung von Umkleiden oder privaten Bereichen.

NACH OBEN

14.3 Beteiligung des Datenschutzbeauftragten / externe Beratung

Falls ein Datenschutzbeauftragter im Verein benannt ist oder beratende externe Fachkräfte hinzugezogen werden, muss dieser bei der DSFA verpflichtend eingebunden werden.

Wenn trotz technischer und organisatorischer Maßnahmen ein hohes Risiko für Betroffene verbleibt, ist die Aufsichtsbehörde zu konsultieren, bevor die Verarbeitung begonnen werden darf.

NACH OBEN

14.4 Weitere denkbare Anwendungsfälle für eine DSFA im Verein

Neben den bereits dargestellten Situationen gibt es eine Reihe weiterer Konstellationen, in denen für Vereine die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) in Betracht kommt:

- **Einsatz automatisierter Bewertungsverfahren:**

Werden Tools verwendet, um Mitglieder nach bestimmten Kriterien – etwa im Rahmen von Förderprogrammen oder internen Auswahlprozessen – automatisiert zu bewerten oder einzuordnen, kann dies erhebliche Auswirkungen auf die Rechte der Betroffenen haben und eine DSFA erforderlich machen.

- **Einführung digitaler Zutrittssysteme:**

Der Betrieb eines zentralen elektronischen Zutrittskontrollsystems, das sämtliche Zutritte erfasst und protokolliert, birgt ein erhöhtes Risiko der umfassenden Überwachung und verlangt daher eine besonders sorgfältige datenschutzrechtliche Bewertung.

- **Verarbeitung besonderer Kategorien personenbezogener Daten:**

Im Bereich des Reha- oder Behindertensports werden regelmäßig Gesundheitsdaten verarbeitet. Aufgrund ihrer besonderen Sensibilität ist hier stets zu prüfen, ob eine DSFA notwendig ist, um die Risiken für die Betroffenen angemessen zu erfassen und abzumildern.

- **Veröffentlichung umfangreicher Mitgliederdaten:**

Werden große Datenmengen über Vereinsmitglieder – etwa Teilnehmerlisten, Ergebnisse oder Profile – online zugänglich gemacht, erhöht sich das Risiko einer ungewollten Weiterverbreitung oder missbräuchlichen Nutzung, sodass eine DSFA angezeigt sein kann.

NACH OBEN

14.5 Dokumentation und Nachweis

Eine durchgeführte DSFA muss schriftlich dokumentiert und archiviert werden – auch wenn sie zum Ergebnis kommt, dass kein hohes Risiko besteht. Dies ist wichtig zur Wahrung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO.

Eine Dokumentation sollte eine abschließende Bewertung anhand einer Auswertung wie der nachfolgenden enthalten:

Schutzbedarf sehr hoch	☐	☐	☐
Schutzbedarf hoch	☐	☐	☐
Schutzbedarf gering	☐	☐	☐
	Eintrittswahrscheinlich-keit für Schäden gering	Eintrittswahrscheinlich-keit für Schäden mittel	Eintrittswahrscheinlich-keit für Schäden hoch

NACH OBEN

15 Datenschutzverstöße

Auch in Vereinen kann es zu Datenschutzverstößen kommen – sei es versehentlich oder infolge mangelnder organisatorischer oder technischer Vorkehrungen. Ein Datenschutzverstoß im Sinne der DSGVO liegt dann vor, wenn es zu einer Verletzung der Sicherheit personenbezogener Daten kommt, durch die unbefugt auf Daten zugegriffen, Daten verändert, gelöscht oder verloren werden oder wenn sie unbefugt übermittelt werden.

Typische Beispiele im Vereinskontext:

- Eine Mitgliederliste wird versehentlich an den falschen E-Mail-Verteiler geschickt.
- Ein Vereinslaptop mit sensiblen Daten wird gestohlen und war nicht verschlüsselt.
- Ausdrucke mit personenbezogenen Daten landen im Papiermüll statt im Aktenvernichter.
- Ein E-Mail-Konto des Vorstands wird gehackt und vertrauliche Nachrichten gelangen nach außen.

Sobald ein solcher Vorfall festgestellt wird, besteht nach Art. 33 DSGVO eine Meldepflicht gegenüber der zuständigen Datenschutzaufsichtsbehörde, sofern ein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Diese Meldung muss unverzüglich erfolgen – möglichst binnen 72 Stunden nach Bekanntwerden.

Die Meldung muss mindestens folgende Angaben enthalten:

- Beschreibung der Art des Verstoßes (z. B. unbefugte Offenlegung, Verlust von Daten),
- Art und Anzahl der betroffenen Personen und Datensätze,
- Name und Kontaktdaten der Ansprechperson im Verein (i. d. R. der Vorstand oder die datenschutzverantwortliche Person),
- Beschreibung der wahrscheinlichen Folgen des Verstoßes,
- Maßnahmen, die bereits ergriffen wurden oder geplant sind, um den Schaden zu begrenzen.

Darüber hinaus ist unter bestimmten Voraussetzungen auch die betroffene Person über den Vorfall zu informieren (Art. 34 DSGVO). Dies ist insbesondere dann erforderlich, wenn ein hohes Risiko für ihre Rechte und Freiheiten besteht – etwa bei dem Verlust besonders sensibler Daten oder Zugangsinformationen.

Im Verein sollte daher ein klares Verfahren zur Bearbeitung von Datenschutzverstößen festgelegt werden. Dabei ist nicht nur die technische Schadensbegrenzung von Bedeutung, sondern auch die lückenlose Dokumentation des Vorfalls. Dies dient zum einen der Rechenschaftspflicht, zum anderen hilft es dem Verein, aus Fehlern zu lernen und die Prozesse entsprechend zu verbessern.

Empfehlungen für den Umgang mit Datenschutzverstößen:

- Richten Sie eine interne Meldekette ein (z. B. Vorstand → Datenschutzbeauftragte*r → Aufsichtsbehörde).
- Erfassen und dokumentieren Sie alle Datenschutzpannen, auch wenn keine Meldepflicht besteht.
- Legen Sie Zuständigkeiten im Verein fest – insbesondere bei Abwesenheit oder Wechsel im Vorstand.

- Schulen Sie regelmäßig alle mit Datenverarbeitung betrauten Personen im Umgang mit solchen Vorfällen.

Je schneller und transparenter ein Verein auf Datenschutzverstöße reagiert, desto geringer ist in der Regel das rechtliche und reputative Risiko. Eine gute Vorbereitung, insbesondere in Form eines Datenschutz-Notfallplans, hilft, im Ernstfall strukturiert und rechtskonform zu handeln.

Vorstandsmitglieder können bei grob fahrlässigem oder vorsätzlichem Handeln persönlich haftbar gemacht werden. Dies verdeutlicht, dass ein gewissenhafter und verantwortungsvoller Umgang mit personenbezogenen Daten im Interesse des gesamten Vereins liegt. Durch präventive Maßnahmen, transparente Prozesse und eine offene Fehlerkultur lassen sich die Risiken eines Datenschutzverstoßes jedoch erheblich reduzieren.

NACH OBEN

16 Rechtsfolge von Verstößen gegen Datenschutzrecht

Die Nichteinhaltung datenschutzrechtlicher Vorgaben kann für Vereine empfindliche rechtliche, finanzielle und auch imagebezogene Konsequenzen nach sich ziehen. Die Datenschutzgrundverordnung sieht bei Verstößen erhebliche Sanktionsmöglichkeiten vor – unabhängig davon, ob der Verstoß vorsätzlich oder fahrlässig geschieht.

Vereine unterliegen denselben Vorschriften wie Unternehmen, wenn sie personenbezogene Daten verarbeiten. Daher gelten auch die in Art. 83 DSGVO genannten Bußgeldrahmen. Diese reichen bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes – wobei in der Praxis bei Vereinen meist niedrigere Beträge verhängt werden. Dennoch können auch kleinere Bußgelder (im unteren fünfstelligen Bereich) für einen gemeinnützigen Verein erhebliche Auswirkungen haben.

Mögliche Konsequenzen bei Datenschutzverstößen:

- Verwaltungsrechtliche Bußgelder durch die Datenschutzaufsichtsbehörde,
- Untersagung bestimmter Datenverarbeitungen oder deren Rückabwicklung,
- Verpflichtung zur nachträglichen Umsetzung technischer oder organisatorischer Maßnahmen,
- zivilrechtliche Schadensersatzforderungen durch betroffene Personen,
- Reputationsschäden in der Öffentlichkeit, insbesondere bei gemeinnützigen oder öffentlichkeitswirksamen Vereinen.

Neben dem Verein als juristische Person kann auch eine persönliche Haftung von Vorstandsmitgliedern oder datenschutzverantwortlichen Personen in Betracht kommen, wenn diese grob fahrlässig oder vorsätzlich gegen ihre Pflichten verstoßen haben. Nach
§ 26 BGB haften Vorstände gegenüber dem Verein grundsätzlich nur bei Vorsatz und grober Fahrlässigkeit – in der Praxis bedeutet dies jedoch, dass bei schweren Versäumnissen (z. B. keine Absicherung sensibler Daten trotz Kenntnis von Risiken) eine Haftung denkbar ist.

Ein besonders sensibles Thema ist die Veröffentlichung von Fotos oder personenbezogenen Daten auf der Vereinswebsite oder in sozialen Netzwerken ohne gültige Einwilligung. Solche Verstöße werden von Betroffenen zunehmend zur Anzeige gebracht oder mit Unterlassungsforderungen und Schadenersatzansprüchen verbunden.

Was Vereine tun sollten, um sich abzusichern:

- Die datenschutzrechtlichen Vorgaben ernst nehmen und kontinuierlich umsetzen.
- Verantwortung und Zuständigkeiten klar regeln (z. B. durch Beschluss des Vorstands).
- Risiken identifizieren, bewerten und geeignete Maßnahmen ergreifen.
- Schulungen und Informationsangebote für alle Beteiligten anbieten.
- Vorab rechtlichen Rat einholen, insbesondere bei neuen oder sensiblen Projekten (z. B. Online-Wettbewerbe, Fotoaktionen).

Ein transparenter und sorgfältiger Umgang mit personenbezogenen Daten stärkt nicht nur das Vertrauen von Mitgliedern, Förderern und der Öffentlichkeit in den Verein, sondern reduziert auch ganz konkret das Risiko rechtlicher und finanzieller Folgen. Bei Unsicherheiten empfiehlt sich die Rücksprache mit den zuständigen Aufsichtsbehörden oder fachkundigen Berater*innen.

NACH OBEN

17 Wo erhalte ich Unterstützung?

Allgemeine Fragen zum Datenschutz können Sie gerne an den Sportbund Rheinland richten:

Barbara Berg, Tel.: (02 61) 135-145
Barbara.Berg@Sportbund-Rheinland.de

Über unsere Partner, die ADLEX GmbH und die Kanzlei Schneiders & Behrendt bieten wir Ihnen eine Analyse Ihrer aktuellen Datenschutzsituation im Verein an. Bestandteile sind hierbei insbesondere:

- Rechtsanwaltliche Bewertung der Maßnahmen des Datenschutzes über Abfragebogen, E-Mail und Telefon
- Ausführlicher Bericht mit Handlungsempfehlungen zu erforderlichen Maßnahmen
- Klärung der Haftung sowie der Risiken von Bußgeldern und Schadensersatzansprüchen

Die Kosten für die Analyse Ihrer Datenschutzsituation betragen einmalig 90,00 Euro.

Anmelden für die Datenschutzanalyse können Sie sich unter Barbara.Berg@Sportbund-Rheinland.de

NACH OBEN

18 Impressum

Herausgeber:

Sportbund Rheinland e. V.

Rheinau 11

56075 Koblenz

Tel.: (02 61) 1 35 – 0

E-Mail: info@sportbund-rheinland.de

Internet: www.sportbund-rheinland.de

V.i.S.d.P.:

Monika Sauer (Präsidentin)

Martin Weinitschke (Geschäftsführer)

Autoren: Alexander Brittner (ADLEX GmbH / Kanzlei Schneiders & Behrendt)

Redaktion: Barbara Berg, Melanie Hohn

Layout: Melanie Hohn

NACH OBEN