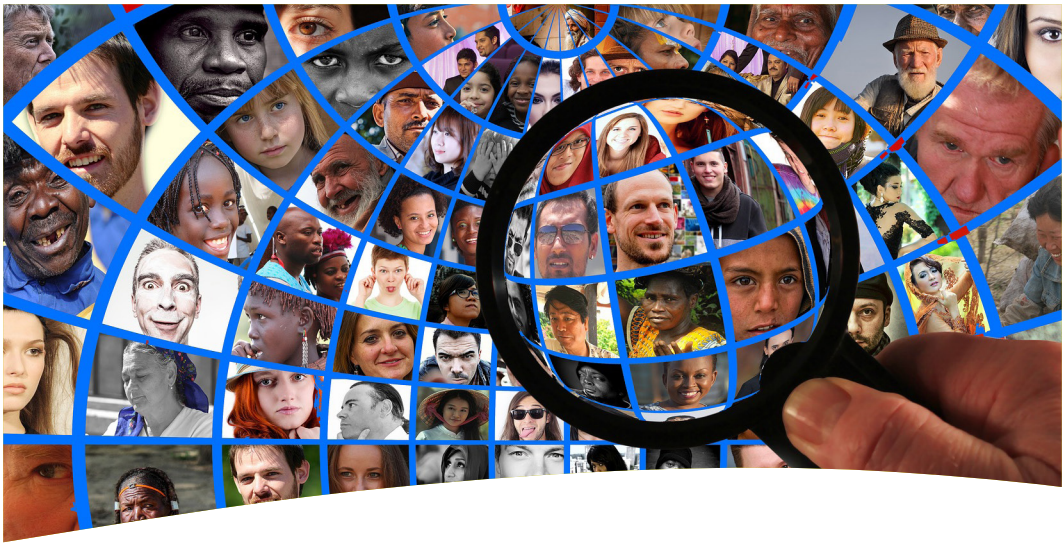


Leitfaden

Datenschutz – Orientierungshilfe für Vereine in Mecklenburg-Vorpommern

Stand: 09. Oktober 2018

Der Landesbeauftragte für Datenschutz
und Informationsfreiheit Mecklenburg-Vorpommern

Stiftung für Ehrenamt und
bürgerschaftliches Engagement
in Mecklenburg-Vorpommern

IMPRESSUM

Leitfaden | Datenschutz – Orientierungshilfe für Vereine in Mecklenburg-Vorpommern
1. Auflage
Ausgabe für Mecklenburg-Vorpommern

Herausgeber:
Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
Werderstraße 74a
19055 Schwerin
Tel: 0385 59494 0
Mail: info@datenschutz-mv.de
Web: www.datenschutz-mv.de; www.informationsfreiheit-mv.de

Stiftung für Ehrenamt und bürgerschaftliches Engagement in Mecklenburg-Vorpommern
Burgstraße 9
18273 Güstrow
Tel: 03843 77499 0
Mail: kontakt@ehrenamtsstiftung-mv.de
Web: www.ehrenamtsstiftung-mv.de

Lektorat:
Susann Plant

Satz und Layout:
Thomas Massow, progress4

Druck:
Stadtdruckerei Weidner

Bildnachweis:
David Außerhofer, Seite 3 rechts
www.pixabay.com

Leitfaden

Datenschutz – Orientierungshilfe für Vereine in Mecklenburg-Vorpommern

Stand: 09. Oktober 2018

Der Landesbeauftragte für Datenschutz
und Informationsfreiheit Mecklenburg-Vorpommern

Stiftung für Ehrenamt und
bürgerschaftliches Engagement
in Mecklenburg-Vorpommern

Dieser Leitfaden umfasst zwei jeweils eigenständige Teile:

Teil I „DS-GVO light“
– ein Praxisratgeber für die schnelle Orientierung mit häufig gestellten Fragen, Checkliste und Mustern

Teil II „DS-GVO Vertiefung“
– ausführliche Orientierungshilfe zu Einzelfragen

Der Text dieses Leitfadens basiert zu großen Teilen auf der Orientierungshilfe „Datenschutz im Verein nach der Datenschutzgrundverordnung (DS-GVO)“ und dem „Praxisratgeber Datenschutz im Verein nach der DS-GVO“ des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg.

An dieser Stelle ein großer Dank an die Kolleginnen und Kollegen aus Baden-Württemberg dafür, dass wir ihr Material nutzen durften.

Inhalt

3 Vorworte

4 Datenschutz – Kein Thema? Sollte es aber …

5 **Teil I** | „DS-GVO light“ – ein Praxisratgeber für die schnelle Orientierung

6 1. Fragen und Antworten

1.1 Basics

7 1.2 Einwilligung

8 1.3 Informationspflichten – (K)ein Blatt für alle Fälle

9 1.4 Benennung eines Datenschutzbeauftragten

11 1.5 Verzeichnis von Verarbeitungstätigkeiten

12 1.6 Kommunikation – nach innen und außen

13 1.7 Auftragsverarbeitung

14 1.8 Datensicherung

15 2. Checkliste – 11 Schritte für den Datenschutz

17 3. Muster

33 **Teil II** | DS-GVO-Vertiefung – Ausführliche Orientierungshilfe zu Einzelfragen

34 4. Rechtsgrundlagen für den Umgang mit personenbezogenen Daten von Mitgliedern und sonstigen Personen

4.1 Datenschutzgrundverordnung und Bundesdatenschutzgesetz – neu als Rechtsgrundlage

35 4.2 Begriffsbestimmungen – Personenbezogene Daten sind …

4.3 Rechtmäßigkeit der Verarbeitung

42 5. Erhebung personenbezogener Daten durch den Verein

5.1 Erhebung nur von erforderlichen Daten der Vereinsmitglieder

43 5.2 Erhebung von Daten Dritter

5.3 Erhebung von Personaldaten der Beschäftigten des Vereins

44 6. Datenverarbeitung mit Hilfe von Dienstleistern

6.1 Datenverarbeitung im Auftrag
46 6.2 Cloud-Mitgliederverwaltungsdienste
47 7. Nutzung von personenbezogenen Daten
7.1 Nutzung von Mitgliederdaten
7.2 Nutzung von Daten Dritter
48 7.3 Nutzung der Daten des Vereins für Spendenaufrufe und Werbung
49 8. Verarbeitung personenbezogener Daten durch den Verein, insbesondere Übermittlung an Dritte
8.1 Datenübermittlung an Vereinsmitglieder
50 8.2 Bekanntgabe zur Wahrnehmung satzungsmäßiger Mitgliederrechte
51 8.3 Mitteilungen in Aushängen und Vereinspublikationen
52 8.4 Datenübermittlung an Dachverbände und andere Vereine
53 8.5 Datenübermittlung an Sponsoren und Firmen zu Werbezwecken, insbesondere Versicherungen
55 8.6 Veröffentlichungen im Internet
56 8.7 Veröffentlichungen im Intranet
8.8 Personenbezogene Auskünfte an die Presse und sonstige Massenmedien
57 8.9 Übermittlung für Zwecke der Wahlwerbung
8.10 Übermittlung von Mitgliederdaten an die Gemeindeverwaltung
59 9. Recht auf Löschung und Einschränkung personenbezogener Daten
61 10. Technische und organisatorische Maßnahmen
10.1. Gewährleistungsziele
65 10.2 Benennung eines Datenschutzbeauftragten
66 10.3 Verzeichnis von Verarbeitungstätigkeiten
67 10.4 Datenschutz-Folgeabschätzung

Vorworte

Liebe Leserin, lieber Leser,
seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DS-GVO) in Deutschland und in allen anderen Mitgliedstaaten der Europäischen Union geltendes Recht. Gerade kleine Vereine sind sehr verunsichert, welche Neuerungen anstehen bzw. welche neuen Anforderungen an sie gestellt werden. Noch schwieriger ist die Frage, wie diese Anforderungen konkret umzusetzen sind. Informationen zur DS-GVO gibt es zwar zwischenzeitlich zu Genüge, jedoch sind diese Informationen oft sehr theoretisch gehalten und somit für eine Umsetzung in die Praxis nicht immer hilfreich.
Wir hoffen sehr, dass dieser Leitfaden Ihnen dabei hilft, die eigentlich überschaubaren Anforderungen zu erfüllen, damit Sie Ihre Kraft wieder auf das verwenden können, was Sie wirklich antreibt – Ihr Engagement im Verein.
Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern und die Stiftung für Ehrenamt und bürgerschaftliches Engagement in Mecklenburg-Vorpommern werden den Vereinen auch in Zukunft unterstützend zur Seite stehen.

Heinz Müller
Landesbeauftragter für Datenschutz
und Informationsfreiheit
Mecklenburg-Vorpommern

Hannelore Kohl
Vorsitzende des Vorstands
Stiftung für Ehrenamt und bürgerschaftliches
Engagement in Mecklenburg-Vorpommern

Datenschutz – kein Thema? sollte es aber …

Die Digitalisierung lässt keinen Lebensbereich mehr aus. Vom sanften Weckruf der Smart Watch mit Schlaftracking-Funktion, über den ersten Nachrichtencheck des Tages am Smart Phone, der navigationsgestützten Autofahrt zur Arbeit, der Organisation des Vereinstreffens über den Messenger Dienst bis zum Livebild aus dem Kühlschrank zur Erinnerung an den Einkauf auf dem Heimweg – unser Alltag ist digital durchgestaltet. Google, Facebook, Twitter, Instagram und Co laden ein, den eigenen Status quo non Stopp in die Welt hinaus zu senden. Mit jedem Klick, jedem gesendeten Foto, jedem Kommentar hinterlassen wir digitale Fingerabdrücke, die vermeintlich Aussagen darüber zulassen, was wir wollen und wer wir sind. Unternehmen und Institutionen benutzen diese Daten, um Profile über uns zu erstellen und Nachrichten und Werbung darauf abzustimmen.

Wir müssen lernen sensibler und bewusster mit unseren und den Daten anderer umzugehen. Das Datenschutzrecht reglementiert uns dabei nicht nur, es stärkt uns auch den Rücken. Es gibt uns als Einzelnem die Möglichkeit, auf diese Prozesse Einfluss zu nehmen und selbst zu bestimmen, was mit unseren Daten geschieht.

Für Institutionen und Organisationen, die mit personenbezogenen Daten anderer umgehen, gelten mit der seit dem 25. Mai 2018 in Kraft getretenen EU-Datenschutz-Grundverordnung (DS-GVO) nun strengere Regeln. Sie gilt nicht nur für Unternehmen und Behörden, sondern auch für gemeinnützige Organisationen wie Vereine. Doch was genau müssen Vereine denn jetzt beachten in Sachen Datenschutz?

Dieser Leitfaden führt Sie Schritt für Schritt durch die wesentlichen Aufgaben.
Teil I – der Praxisratgeber beantwortet kurz zusammengefasst häufig gestellte Fragen und gibt Ihnen Mustervorlagen an die Hand.
In Teil II – der Orientierungshilfe zur Vertiefung werden die gesetzlichen Regelungen ausführlicher erläutert.

Teil I

„DS-GVO Light“ – Ein Praxisratgeber für die schnelle Orientierung

1. Fragen und Antworten

1.1 Basics

Gilt die DS-GVO überhaupt für unseren kleinen Verein?
Ja, die DS-GVO gilt für alle Vereine.

Wer muss das alles umsetzen, was in der DS-GVO steht?
Nach der DS-GVO muss das der Verantwortliche tun. Der Verantwortliche muss nach der DS-GVO allerdings nicht unbedingt eine natürliche Person sein. Verantwortlich ist der Verein, die DS-GVO umsetzen, muss aber der Vorstand.

Was sind personenbezogene Daten?
Kurz gesagt, alle Informationen oder Merkmale, die man selbst oder auch Dritte eindeutig einer natürlichen Person zuordnen können. Die Person müssen Sie dabei nicht unbedingt namentlich kennen. Zu den personenbezogenen Daten gehören u.a. auch Adress- und Kontoverbindungsdaten, Fotos oder IP-Adressen.

Gibt es besonders sensible Daten?
Ja. Nicht alle Daten sind gleich schutzbedürftig. Personenbezogene Daten von Kindern sind z.B. schutzbedürftiger als E-Mailadressen von Erwachsenen, deren Kontodaten müssen besser geschützt werden als deren Handynummern. Das muss grundsätzlich beachtet werden.
Außerdem gibt es besondere Kategorien („sensibler“) personenbezogener Daten (Art. 9 DS-GVO), insbesondere Gesundheitsdaten, aber auch Daten zum Migrationshintergrund, zu politischen, religiösen und weltanschaulichen Überzeugungen, zur Gewerkschaftszugehörigkeit, zur sexuellen Orientierung sowie genetische und biometrische Daten. Für die Verarbeitung dieser Daten sind spezielle Vorschriften zu beachten.

Wann darf ein Verein überhaupt personenbezogene Daten verarbeiten?
Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Rechtsgrundlage dies erlaubt.
Viele Vereine sind daher der Ansicht, dass sie von jedem Mitglied für die Verarbeitung der personenbezogenen Daten der Mitglieder zwingend eine Einwilligungserklärung benötigen und dass ohne eine Einwilligung eine Datenverarbeitung unzulässig ist. Dies trifft jedoch nicht zu. Die Einwilligung ist nämlich nur eine von mehreren Rechtsgrundlagen.

Andere Rechtsgrundlagen sind zum Beispiel:
- die Erfüllung eines Vertrages (Art. 6 Abs. 1 lit. b DS-GVO) oder

- die „berechtigten Interessen“ des Vereins, die allerdings gegen die Interessen derer abgewogen werden müssen, deren Daten verarbeitet werden sollen (Art. 6 Abs. 1 lit. f DS-GVO).

Ein Verein darf daher – auch ohne Einwilligung personenbezogene Daten verarbeiten,

- wenn diese die für die Anbahnung, Begründung und Durchführung des zwischen Mitglied und Verein durch den Beitritt zustande kommenden Vertrages **erforderlich** sind oder
- wenn der Verein an der Datenverarbeitung ein **berechtigtes Interesse** hat und die Interessen der anderen Seite nicht überwiegen

Wann diese Rechtsgrundlagen greifen, können Sie ausführlicher im Teil II Kapitel 5 nachlesen.
Eine Einwilligung muss und sollte deshalb grundsätzlich nur dann eingeholt werden, wenn keine der genannten anderen Rechtsgrundlagen zur Verfügung steht.

WICHTIGE AUSNAHME:
Dies gilt nicht für besonders sensible Daten, wie zum Beispiel Gesundheitsdaten oder die Religionszugehörigkeit. Für die Verarbeitung dieser Daten muss in der Regel eine Einwilligung eingeholt werden (Art. 9 Abs. 2 lit. a DS-GVO).

Dürfen nur Vorstandsmitglieder Zugriff auf personenbezogene Daten haben?
Nein. Der Verein hat für bestimmte Verarbeitungen Zwecke festgelegt. Er darf mit den personenbezogenen Daten so arbeiten, dass er diese Zwecke erreichen kann. Soweit es in diesem Rahmen erforderlich ist, dürfen auch andere Personen Zugriff auf die Daten haben.

1.2 Einwilligung

Welche Form muss eine Einwilligung haben (wenn keine andere Rechtsgrundlage greift)?
Der Verein muss für den Fall, dass die Verarbeitung auf einer Einwilligung beruht, nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat (Art. 7 Abs. 1 DS-GVO). Aus diesem Grund ist es ratsam, Einwilligungen zum Zwecke des Nachweises schriftlich (d. h. mit eigenhändiger Unterschrift der betroffenen Person) einzuholen.

Muss der Verein nach dem 25. Mai 2018 von allen Mitgliedern, die bereits eine Einwilligung abgegeben haben, eine neue Einwilligung einholen?
Nein. Liegt seitens der bestehenden Mitglieder bereits eine korrekte (informierte und freiwillige) Einwilligung mit Hinweis auf das Widerrufsrecht vor, so gilt diese weiter und muss nicht erneut eingeholt werden.

Wenn jedoch die vorliegende „alte“ Einwilligung seinerzeit nicht korrekt (also nicht informiert und freiwillig) eingeholt worden war, ist eine neue Einwilligung notwendig. Außerdem ist eine neue Einwilligung notwendig, sobald weitere personenbezogene Daten erhoben oder sonst verarbeitet werden sollen (z.B. Adressänderungen, etc.).

Reicht ein allgemeiner Beschluss der Mitgliederversammlung zum Umgang mit persönlichen Daten der Mitglieder als Einwilligung?
Nein. Der Beschluss ist keine Einwilligung. (Er kann jedoch in Ergänzung zu den anderen genannten Rechtsgrundlagen bedeutsam sein, also beispielsweise berechtigte Interessen des Vereins oder Vereinszwecke konkretisieren).

1.3 Informationspflichten – (k)ein Blatt für alle Fälle

Jeder Verein hat aus Gründen der Transparenz umfassend darüber zu informieren, wer, wie und warum personenbezogene Daten der Mitglieder im Verein verarbeitet. Es empfiehlt sich hier, Infoblätter zu erstellen.

MUSTER: Entsprechende Muster zur Erfüllung der Informationspflichten nach Art. 13 DS-GVO finden Sie in Teil I / Kapitel 3. Muster.

Dabei lassen sich aber nicht alle Verarbeitungen über einen Kamm scheren. Veröffentlicht der Verein z.B. Fotos einer Veranstaltung mit Besuchern auf seiner Homepage, muss er die betroffenen Personen anders informieren, als wenn er nur die Namen von Mitgliedern verwaltet, um den Mitgliedsbeitrag einzuziehen.

Wann muss der Verein seinen Informationspflichten nachkommen?
Zum Zeitpunkt der Erhebung (z.B. im Mitgliedsantrag) müssen sämtliche Informationen nach dem Katalog in Art. 13 DS-GVO mitgeteilt werden.

Infoblätter – Was muss rein?

- Name und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten, falls es einen gibt
- Warum der Verein die Daten verarbeitet (Zweck) und nach welcher Rechtsgrundlage er das darf (z.B. für die Öffentlichkeitsarbeit aufgrund berechtigter Interessen gem. Art. 6 Abs. 1 lit. f DS-GVO, zur Erfüllung des Mitgliedvertrags aufgrund von Vertragserfüllung gem. Art. 6 Abs. 1 lit. b DS-GVO)
- Falls es eine Pflicht gibt, dass dem Verein personenbezogene Daten durch das Mitglied bereitgestellt werden (z.B. im Vertrag oder weil ein Gesetz das vorschreibt), muss über diese Pflicht informiert werden und darüber, was passiert,

wenn die betroffene Person die Daten nicht zur Verfügung stellen will
- Falls die Verarbeitung auf berechtigten Interessen (Art. 6 Abs. 1 lit. f DS-GVO) beruht, müssen diese konkret benannt werden (z.B. Öffentlichkeitsarbeit)
- Empfänger oder Kategorien von Empfängern, das sind alle, denen personenbezogene Daten offengelegt werden (z.B. externe Dienstleister, die Computer warten oder Dachverbände)
- Falls der Verein beabsichtigt, personenbezogene Daten an Empfänger außerhalb der europäischen Union zu übermitteln, muss er gesondert prüfen, ob das zulässig ist (Art. 44 ff. DS-GVO) und genau über diese zusätzlichen Voraussetzungen informieren
- Speicherdauer der personenbezogenen Daten
- Belehrung über die jeweils einschlägigen Betroffenenrechte (immer: Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung; Widerspruchsrecht gegen Verarbeitung nur bei berechtigten Interessen)
- Hinweis auf jederzeitiges Widerrufsrecht nur bei der Einwilligung
- Hinweis auf Beschwerderecht bei der zuständigen Datenschutz-Aufsichtsbehörde mit Nennung der Kontaktdaten (in M-V: der Landesbeauftragte für Datenschutz und Informationsfreiheit, Lennestraße 1, 19053 Schwerin)
- Wenn der Verein Profile über die Mitglieder anlegt, also bestimmte Merkmale digital sammelt, um allein aufgrund dieser Merkmale bestimmte Bewertungen vorzunehmen, müsste auch darüber informiert werden (Art. 4 Nr. 4 DS-GVO)

Ist es ausreichend, wenn der Verein die Datenschutzhinweise auf seine Webseite stellt und das Mitglied etwa bei Abschluss eines Mitgliedvertrages einfach darauf verweist?

Nein. Grundsätzlich sollte man der betroffenen Person die Information so anbieten, wie man gerade mit ihr kommuniziert. Wird das Beitrittsformular von Hand ausgefüllt, sollten dem Mitglied die Informationen nach Art. 13 DS-GVO auch in Papierform ausgehändigt werden.

Nimmt man Daten am Telefon auf, sollte man die Information zumindest mündlich anbieten. Spätestens für diese Konstellation ist es sinnvoll, wenn ergänzend auf ein Infoblatt auf der Homepage verwiesen werden kann und die betroffene Person die Gelegenheit erhält, sich dort zu informieren, bevor sie die Daten übermittelt. Zudem können so auch die Bestandsmitglieder des Vereins Kenntnis hiervon erlangen.

Auf der Homepage muss es zusätzlich immer ein Infoblatt für den rein informatorischen Besuch der Homepage geben, soweit dabei IP-Adressen gespeichert werden. Das ist in der Regel der Fall.

MUSTER: Ein Beispiel eines Informationsblatts für den rein informatorischen Besuch einer Vereins-Homepage finden Sie in Teil I / Kapitel 3. Muster.

Müssen die Informationspflichten des Art. 13 DS-GVO für bereits nach dem Bundesdatenschutzgesetz (BDSG) erfolgte Datenerhebungen nachgeholt werden?

Nein. Bei bereits erfolgten Datenerhebungen nach dem BDSG sind die Informations-

pflichten des Art. 13 DS-GVO nicht zu erfüllen bzw. nachzuholen. Sobald der Verein allerdings nach dem 25. Mai 2018 neue Daten von dem Bestandsmitglied erhebt (z.B. eine Telefonnummer berichtigt) sind die Informationspflichten zu erfüllen. Allerdings empfiehlt es sich, auch Bestandsmitgliedern bei der nächsten passenden Gelegenheit ein Informationsblatt zur Kenntnis zu geben.

1.4 Benennung eines Datenschutzbeauftragten

Wann muss der Verein einen Datenschutzbeauftragten (DSB) benennen?
Der Verein hat einen Datenschutzbeauftragen zu benennen, wenn

a) mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§ 38 BDSG-neu) oder
b) der Verein Verarbeitungen vornimmt, die einer Datenschutzfolgeabschätzung gemäß Art. 35 DS-GVO unterliegen (§ 38 BDSG-neu, Art. 35 DS-GVO), (z.B. umfangreiche Verarbeitung von Gesundheitsdaten, sowie bei umfangreicher Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten und bei umfangreicher Verarbeitung von personenbezogenen Daten per Videoüberwachung z.B. in Stadien) oder
c) die Kerntätigkeit des Verantwortlichen eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (Art. 37 DS-GVO) – siehe Teil II / Kapitel 10.

Was bedeutet „ständig“, wer zählt zu diesen 10 Personen?
Nach dem Gesetzeswortlaut zählen nur solche Personen mit, die regelmäßig mit der automatisierten Verarbeitung personenbezogene Daten „beschäftigt“ sind. Das sind nur Personen, bei denen der Schwerpunkt der Tätigkeit im Verein überwiegend darin besteht, personenbezogene Daten zu verarbeiten.
Im Verein können daher auch mehr als 10 Personen regelmäßig Zugriff auf die Datenbestände der Vereinsmitglieder haben (beispielsweise zur Organisation von wöchentlichen Proben, Trainingseinheiten, Spielen oder Veranstaltungen), ohne dass deshalb ein Datenschutzbeauftragter bestellt werden müsste, da hier zwar eine wiederkehrende und häufige, aber keine ständige Datenverarbeitung vorliegt. Nicht mitzuzählen sind also z. B. die Empfänger einer digitalen Teilnehmerliste (etwa Trainer). Zwar speichert auch ein Trainer die Liste ab, jedoch besteht der Schwerpunkt seiner Tätigkeit nicht in der Datenverarbeitung, sondern im Training.
Irrelevant ist hingegen, ob die Person beim Verein beschäftigt oder ehrenamtlich tätig ist. Auch ehrenamtlich Tätige sind gemeint.

Und wann muss der Verein eine Datenschutz-Folgenabschätzung machen und deshalb einen Datenschutzbeauftragten benennen?

Entweder weil die Verarbeitung besondere Risiken birgt, etwa weil neue Technologien zum Einsatz kommen. Besonders risikoreich kann eine Verarbeitung auch sein, wenn sensible Daten außerhalb der EU verarbeitet werden sollen, also zum Beispiel auf Servern außerhalb der EU gespeichert werden sollen.
Oder aber, wenn umfangreich besondere Kategorien personenbezogener Daten verarbeitet werden. Was umfangreich ist, ist nicht eindeutig definiert. Aber die Datenschutzbeauftragten des Bundes und der Länder haben sich darauf verständigt, dass beispielsweise ein Arzt mit weniger als 9 Mitarbeitern, die Daten verarbeiten (also insgesamt weniger als 10), in der Regel noch nicht umfangreich Gesundheitsdaten verarbeitet. Bei einem Verein werden wir hier keine strengeren Maßstäbe ansetzen. Bei weniger als 10 Personen, die besondere Kategorien personenbezogener Daten verarbeiten, liegt also noch keine umfangreiche Verarbeitung vor.

Wann macht die Kerntätigkeit des Verantwortlichen eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich?
Gemeint sind hier eher Unternehmen, die z.B. mit GPS-Trackern, Biometriesystemen oder weiträumigen Videoüberwachungssystemen arbeiten. Bei „klassischen“ Vereinen erfolgt demgegenüber eine Verarbeitung personenbezogener Daten ohnehin sehr häufig lediglich als notwendig anfallende Nebentätigkeit (Mitgliederverwaltung, Verarbeitung von Daten von Beschäftigten etc.). Vereine, deren Kerntätigkeit in Verarbeitungsprozessen liegt, die noch dazu eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person erforderlich machen, sind sehr selten. Allein das Aufhängen einer Videokamera gehört ebenso wenig dazu wie die Dokumentation von Trainingsfortschritten.

Muss der Verein den Datenschutzbeauftragten öffentlich machen?
Der Verein hat die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen. Hierbei ist es ausreichend, wenn die E-Mail-Adresse des Datenschutzbeauftragten auf der Vereinshomepage frei zugänglich genannt wird. Der Datenschutzbeauftragte ist zudem bei der zuständigen Aufsichtsbehörde zu melden. Eine Meldung ist beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Mecklenburg-Vorpommern ist über folgendes Online-Formular möglich:

MUSTER: Vorlage für die Mitteilung von Datenschutzbeauftragten: www.datenschutz-mv.de/kontakt/Mitteilung-von-Datenschutzbeauftragten/

Was muss der Datenschutzbeauftragte können?
Er muss fachlich versiert sein. Entscheidend ist aber nicht, wie die Leute ihre Sachkunde bekommen haben, sondern dass sie sie besitzen. So gehen wir bei Anwälten davon aus, dass sie sachkundig sind. Oder dass die Person eine Ausbildung – eine drei- bis fünftägige Schulung – hinter sich hat und sich weiter im Datenschutz fortbildet.

Haftet der (ehrenamtliche) Datenschutzbeauftragte persönlich für Datenschutzverstöße des Vereins?
Nein, für den Verein (nach außen) haftet der Vorstand. Nur im sogenannten Innenverhältnis – also vereinsintern – kann es ggf. zu Ansprüchen des Vereins gegen den Datenschutzbeauftragten kommen.

1.5 Verzeichnis von Verarbeitungstätigkeiten

Braucht mein Verein ein Verzeichnis von Verarbeitungstätigkeiten?
Ja, da in jedem Verein die Verarbeitung personenbezogener Daten nicht nur gelegentlich, sondern regelmäßig stattfindend erfolgt (z.B. Aktualisierung der Mitgliederliste, Versand von Nachrichten an Mitglieder, Einzug von Mitgliedsbeiträgen, Anmeldung zu Wettkämpfen etc.), ist auch bei Vereinen mit z.B. 3 Mitarbeitern ein Verzeichnis von Verarbeitungstätigkeiten zu führen.
WEITERE INFORMATIONEN zu diesem Thema finden Sie in Teil II / Kapitel 10.3.

Was muss ins Verarbeitungsverzeichnis?
Eine Vorlage für die Erstellung eines Verarbeitungsverzeichnisses finden Sie in Teil I / Kapitel 3. Muster. Auf der Homepage des Landesbeauftragten für Datenschutz und Informationsfreiheit M-V finden Sie dazu eine digitale Vorlage.

MUSTER: Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher und Ausfüllhinweise zu finden unter www.datenschutz-mv.de/datenschutz/DS-GVO/Hilfsmittel-zur-Umsetzung/

Beim Ausfüllen ist darauf zu achten, dass **pro Verarbeitungstätigkeit** die Blätter hinter dem Deckblatt jeweils gesondert auszufüllen sind. Hinter die erste Seite als Deckblatt kommen dann also nummeriert die Angaben zu den einzelnen Verarbeitungsvorgängen. Klassische Verarbeitungstätigkeiten im Verein sind zum Beispiel Mitgliederdatenverwaltung, Öffentlichkeitsarbeit, Sponsoring und Lohnabrechnung. Keine Verarbeitungsvorgänge in diesem Sinn sind eingesetzte Produkte oder Software.

1.6 Kommunikation – nach Innen und Außen

Benötigt unsere Vereinswebsite ein Sicherheitszertifikat zur Verschlüsselung?
Ja. Das ist Stand der Technik.

Welche persönlichen Daten (z.B. Name, Alter, Wettkampfergebnisse) der Mitglieder darf der Verein auf der Vereins-Website veröffentlichen?
Das hängt davon ab, welche Rechtsgrundlage vorliegt. Bei berechtigten Interessen (Art. 6 Abs. 1 lit. f DS-GVO) muss sehr genau abgewogen werden, was wirklich wichtig für die Öffentlichkeitsarbeit ist oder ob hier nicht das Interesse des Mitglieds überwiegt, dass bestimmte Informationen zu seiner Person nicht öffentlich werden.
Besondere Kategorien personenbezogener Daten, also zum Beispiel Bilder, die auf eine Erkrankung schließen lassen, sollten grundsätzlich nicht auf die Homepage.
Etwas anderes gilt, wenn entsprechende Einwilligungen vorliegen. Dann dürfen genau die Informationen auf die Hompage, hinsichtlich derer das Mitglied eingewilligt hat, dass die Informationen veröffentlicht werden. Dazu können dann auch Gesundheitsdaten zählen, wenn das Mitglied ausdrücklich auch darin eingewilligt hat (z.B.: bei Fotos vom Reha-Sport).

Dürfen Vereine über Social Media Kanäle Bilder oder Videos vom Vereinsgeschehen ohne weiteres veröffentlichen?
Nein, bei Social Media-Kanälen gilt das Gleiche wie für die Vereins-Homepage.

Brauchen wir von allen abgebildeten Personen nachträglich Einverständniserklärungen für veröffentlichte Bilder?
Auch hier kommt es darauf an. Geben die Bilder keine besonderen Kategorien personenbezogener Daten preis, könnte der Verein ein berechtigtes Interesse an der Öffentlichkeitsarbeit haben, wenn nicht überwiegende Interessen der betroffenen Person entgegen stehen. Stützt man die Verarbeitung auf berechtigte Interessen, sollte man aber auf der Homepage darauf hinweisen, dass die Personen auf den Fotos ein Recht haben, der Veröffentlichung zu widersprechen.
Liegen bereits Einwilligungen zu Fotos und deren Veröffentlichung vor und wurden diese korrekt, also freiwillig und informiert erteilt, müssen diese Einwilligungen nicht erneuert werden.
Grundsätzlich regen wir an, sparsam mit Fotos umzugehen, die Mitglieder eindeutig erkennbar zeigen. Ein Siegerportrait ist natürlich ok, aber bei Fotos von Kindern im Training empfehlen wir solche Aufnahmen für die Homepage auszuwählen, bei denen Gesichter nicht unbedingt erkennbar sind, oder im Zweifel eine Einwilligung einzuholen.
WEITERE INFORMATIONEN: Nähere Hinweise zur Verarbeitung personenbezogener Daten bei Fotografien finden Sie unter: www.datenschutz-mv.de/datenschutz/DS-GVO/Hilfsmittel-zur-Umsetzung/?topiclist.expand=none

Darf der Verein Vereinsinformationen über E-Mail an die Mitglieder versenden?
Ja.

Dürfen die Mitglieder untereinander über einen Messenger-Dienst kommunizieren?
Der Verein hat regelmäßig keine Kontrolle darüber, wie Mitglieder untereinander kommunizieren. Dafür ist der Verein auch nicht verantwortlich. Will der Verein aber selbst einen Messenger nutzen oder vorschlagen, sollte er darauf achten, einen Messenger-Dienst auszuwählen, der ein möglichst hohes Datenschutzniveau gewährt. Denn dann ist der Verein für den Einsatz des Messenger-Dienstes verantwortlich. Unter datenschutzrechtlichen Gesichtspunkten raten wir insofern von der Nutzung von WhatsApp ab.

1.7 Auftragsverarbeitung

Wann muss der Verein einen Auftragsverarbeitungsvertrag abschließen?
Wenn Dienstleister Aufgaben für den Verantwortlichen erfüllen (z.B. Adressverwaltung, externe Lohnabrechnung, Wartung IT) und in diesem Zusammenhang mit personenbezogenen Daten umgehen bzw. Einblick in diese haben, so spricht man von einer Auftragsverarbeitung. Eine solche ist auch dann gegeben, wenn ein Verein seine Mitgliederdaten nicht auf einer eigenen EDV-Anlage speichert, sondern hierfür einen Datenbankserver nutzt, den ein Dienstleistungsunternehmen zu diesem Zweck zur Verfügung stellt.
Der Verein darf nur Auftragsverarbeiter einsetzen, die eine hinreichende Garantie für eine datenschutzkonforme Datenverarbeitung gewährleistet ist.
WEITERE INFORMATIONEN: zu diesem Thema finden Sie im Kurzpapier Nr. 13 der Datenschutzkonferenz unter www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Kurzpapiere/Kurzpapier_Nr_13.pdf

MUSTER: Ein Muster für einen Auftragsverarbeitungsvertrag finden Sie hier: www.datenschutz-mv.de/datenschutz/DS-GVO/Hilfsmittel-zur-Umsetzung/

1.8 Datensicherung

Welche Mindestanforderungen müssen Vereine beachten?
Die DS-GVO fordert von dem Verantwortlichen (hier dem Verein), geeignete technische und organisatorische Maßnahmen zu treffen (und nachzuweisen), um sicherzustellen, dass die Verarbeitung gemäß der DS-GVO erfolgt (Art. 24 Abs. 1 DS-GVO). Das betrifft insbesondere die in Art. 32 Abs. 1 DS-GVO genannten erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
WEITERE INFORMATIONEN: Bitte beachten Sie hierzu auch unsere ausführlichen Informationen im Teil II / Kapitel 10

Ein Verein sollte mit Mitgliederdaten nur das tun, was er verantworten kann. Verantworten kann der Verein nur Datenverarbeitungen, die bestimmte Datenschutzgrundsätze erfüllen, zum Beispiel Vertraulichkeit. Hierzu zählt zum Beispiel die Verpflichtung auf die Datenschutzgrundsätze.

MUSTER: Eine Verpflichtungserklärung finden Sie hier: www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Kurzpapiere/Kurzpapier_Nr_19.pdf

Diese sollte von allen Personen im Verein unterschrieben werden, deren Aufgaben es erforderlich machen, personenbezogene Daten von anderen Mitgliedern zu verarbeiten.

2. Checkliste
11 Schritte für den Datenschutz

Schritte	Hinweise, Muster	Erledigt
1 Datenschutz zur Chefsache machen	Vorstand ist verantwortlich für die Umsetzung	
2 Bestandsaufnahme Datenverarbeitung	Wer verarbeitet personenbezogene Daten zu welchen Zwecken und in welchen Verfahren?	
3 Datenschutzbeauftragten bestellen (sofern gesetzlich notwendig) und bei der Aufsichtsbehörde melden	Meldung bei der Aufsichtsbehörde unter www.datenschutz-mv.de/kontakt/Mitteilung-von-Datenschutzbeauftragten/	
4 Zuständigkeiten für anstehende Aufgaben verteilen	to-do-Liste: Wer macht was bis wann?	
5 Verarbeitungsverzeichnis erstellen	www.datenschutz-mv.de/datenschutz/DS-GVO/Hilfsmittel-zur-Umsetzung/ Ausfüllhinweise dazu finden sie ebenfalls dort	
6 Datenschutzerklärung auf Website überprüfen, ggf. anpassen und (wenn notwendig) Kontaktdaten des Datenschutzbeauftragten angeben	Muster einer Einwilligungserklärung für die Veröffentlichung von Mitgliederdaten im Internet in Teil I / Kapitel 3. Muster	
7 Rechtsgrundlage zur Datenerhebung überprüfen – Rechtmäßigkeit	Hinweise dazu in Teil II / Kapitel 4. Rechtsgrundlagen	
8 Einwilligungserklärungen überprüfen und ggf. anpassen	Muster von Einwilligungserklärungen in Teil I / Kapitel 3. Muster	

9 Datenschutzvereinbarung mit externen Auftragsverarbeitern prüfen oder neu schließen	www.datenschutz-mv.de/datenschutz/DS-GVO/Hilfsmittel-zur-Umsetzung/	
10 Prozess bei Datenpannen und der Geltendmachung von Betroffenenrechten festlegen	Meldung an Aufsichtsbehörde unter: www.datenschutz-mv.de/kontakt/meldung-einer-datenpanne/	
11 Technische und organisatorische Maßnahmen zur Datensicherung treffen	Hinweise dazu in Teil II / Kapitel 10	

Wiederkehrende Aufgaben		
Verzeichnis zur Datenverarbeitung jährlich auf Aktualität und Anpassungsbedarf prüfen		
Vorstand, Mitarbeiter*innen im Verein regelmäßig zur Einhaltung des Datenschutzes informieren/schulen	www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Kurzpapiere/Kurzpapier_Nr_19.pdf	

3. Muster

Muster einer Einwilligungserklärung für die Veröffentlichung von Mitgliederdaten im Internet

Hinweis:
Einwilligungen müssen informiert und freiwillig sein. Sie können also nicht pauschal sondern nur bezogen auf eine konkrete Verarbeitung erteilt werden. Daher sollte für jede Einwilligungserklärung ein gesondertes Formular verwendet werden. Auf keinen Fall soll die Einwilligungserklärung in die Datenschutzhinweise „gepackt" werden. Auf jedem Formular ist genau anzugeben, welche Daten zu welchem Zweck verarbeitet werden.

Formulierungsvorschlag:
Der Vereinsvorstand weist hiermit darauf hin, dass ausreichende technische Maßnahmen zur Gewährleistung des Datenschutzes getroffen wurden. Dennoch kann bei einer Veröffentlichung von personenbezogenen Mitgliederdaten im Internet ein umfassender Datenschutz nicht garantiert werden. Daher nimmt das Vereinsmitglied die Risiken für eine eventuelle Persönlichkeitsrechtsverletzung zur Kenntnis und ist sich bewusst, dass:

- die personenbezogenen Daten auch in Staaten abrufbar sind, die keine der Bundesrepublik Deutschland vergleichbaren Datenschutzbestimmungen kennen,
- die Vertraulichkeit, die Integrität (Unverletzlichkeit), die Authentizität (Echtheit) und die Verfügbarkeit der personenbezogenen Daten nicht garantiert ist.

Das Vereinsmitglied trifft die Entscheidung zur Veröffentlichung seiner Daten im Internet freiwillig und kann seine Einwilligung gegenüber dem Vereinsvorstand jederzeit widerrufen.

ERKLÄRUNG

„Ich habe das Infoblatt „Datenverarbeitung im Verein" zur Kenntnis genommen.

.....

(Angaben zum Datenblatt)

Ich bestätige das Vorstehende zur Kenntnis genommen zu haben und willige in Kenntnis dessen und des anliegenden Infoblattes ein, dass der Verein

.....

(Name des Vereins)

folgende Daten zu meiner Person:

Allgemeine Daten	*Spezielle Daten von Funktionsträgern*
Vorname	Anschrift
Zuname	Telefonnummer
Fotografien	Faxnummer
Sonstige Daten (z.B.: Leistungsergebnisse, Lizenzen, Mannschaftsgruppe u.ä.)	E-Mail-Adresse

wie angegeben auf folgender Internetseite des Vereins

.....

(Online-Dienst/Internet; Zugangsadresse)

veröffentlichen darf."

.....

Ort und Datum Unterschrift

(Bei Minderjährigen Unterschrift eines Erziehungsberechtigten)

Ich willige ausdrücklich auch darin ein, dass nachfolgende Gesundheitsdaten von mir (bitte konkret angeben, z. Bps. Fotos, Erwähnung des Namens im Zusammenhang mit einem Behindertensportverein etc...) zu oben genannten Zwecken und unter oben genannten Voraussetzungen verarbeitet werden.

.....

Ort und Datum Unterschrift

(Bei Minderjährigen Unterschrift eines Erziehungsberechtigten)

Muster einer Einwilligungserklärung für die Verarbeitung von Gesundheitsdaten von Mitgliederdaten

Formulierungsvorschlag:

Ich bin darauf hingewiesen worden, dass ausreichende technische Maßnahmen zur Gewährleistung des Datenschutzes getroffen wurden.
Das Infoblatt „Datenschutz im Verein“ habe ich zur Kenntnis genommen.

.....

Ort und Datum Unterschrift

(Bei Minderjährigen Unterschrift eines Erziehungsberechtigten)

Ich bin damit einverstanden, dass folgende Gesundheitsdaten

	Bitte konkret angeben
Grad der Behinderung	
Bestimmte Erkrankungen	
Allergien	
Lebensmittelunverträglichkeiten	

von dem Verein

.....

zur Erfüllung der satzungsgemäßen Vereinszwecke sowie den Zuwendungsgebern zum Nachweis verarbeitet werden dürfen. Diese Einwilligung bezieht sich nicht auf die Nutzung meiner Gesundheitsdaten zu Zwecken der Öffentlichkeitsarbeit. Ich weiß, dass die Verarbeitung meiner Daten auf freiwilliger Basis auf Grundlage dieser Einwilligung erfolgt. Mir ist bekannt, dass ich die Einwilligung ohne für mich nachteilige Folgen verweigern bzw. jederzeit mit Wirkung für die Zukunft widerrufen kann.

Meine Widerrufserklärung richte ich an:

.....

(Adresse und Kontaktdaten des Vereins ergänzen)

.....

Ort und Datum Unterschrift

(Bei Minderjährigen Unterschrift eines Erziehungsberechtigten)

Muster für die Erfüllung der Informationspflicht bei Erhebung von personenbezogenen Daten gemäß Art. 13 DS-GVO

Allgemeines Formular:

1. Name und Kontaktdaten des Verantwortlichen

Verantwortlicher im Sinne des Art. 13 Abs. 1 lit. a) DS-GVO ist
Name Verein:
Straße:
PLZ, Ort:
Tel.:
E-Mail:
Vorstand:

2. Kontaktdaten des Datenschutzbeauftragten

Die Kontaktdaten des Datenschutzbeauftragten müssen nur dann angegeben werden, wenn ein solcher benannt ist. Ausreichend ist hierbei die Angabe eines Funktionspostfachs.
Formulierungsbeispiel:
Unseren Datenschutzbeauftragten erreichen Sie unter folgender E-Mail-Adresse:
Datenschutzbeauftragter@Musterverein.de

3. Zwecke und Rechtsgrundlage der Verarbeitung

Bei einem Verein können je nach Ausrichtung ganz verschiedene Zwecke, für die personenbezogene Daten verarbeitet werden, anfallen. Jeder Zweck ist hierbei gesondert aufzunehmen.
Auch ist für jeden Zweck gesondert die Rechtsgrundlage der Verarbeitung anzugeben. Jeder Verein sollte sich daher zunächst einen Überblick darüber verschaffen, welche Daten zu welchem Zweck verarbeitet werden und sodann prüfen, auf welcher Grundlage die Verarbeitung erfolgt. Als Rechtsgrundlagen kommen insbesondere in Betracht:

- Art. 6 Abs. lit. a DS-GVO: Einwilligung der betroffenen Person
- Art. 6 Abs. lit. b DS-GVO: bei Datenverarbeitungen zur Erfüllung des Mitgliedsvertrags / der Satzung
- Art. 6 Abs. lit. f DS-GVO: bei Datenverarbeitungen zur Wahrung berechtigter Interessen des Vereins

Formulierungsbeispiele:

(die im Folgenden genannten Zwecke sind nur beispielhaft und nicht abschließend):
Der Musterverein verarbeitet folgende personenbezogene Daten:

- Zum Zwecke der Mitgliederverwaltung werden der Name, Vorname, Sportbereich/

Abteilung verarbeitet (ggf. sind weitere Daten, die im konkreten Fall verarbeitet werden, zu nennen).
Die Rechtsgrundlage hierfür ist Art. 6 Abs. lit. b) DS-GVO.

- Zum Zwecke der Beitragsverwaltung wird die Bankverbindung verarbeitet (ggf. sind weitere Daten, die im konkreten Fall verarbeitet werden, zu nennen).
  Die Rechtsgrundlage hierfür ist Art. 6 Abs. lit. b) DS-GVO.
- Zum Zwecke der Lohnabrechnung werden von den Beschäftigten des Mustervereins der Name, der Vorname, die Adresse, ggf. die Religionszugehörigkeit, Steuernummer verarbeitet (ggf. sind weitere Daten, die im konkreten Fall verarbeitet werden, zu nennen).
  Die Rechtsgrundlage hierfür ist Art. 6 Abs. lit. b) DS-GVO.
- Zum Zwecke der Außendarstellung werden Fotos der Mitglieder/von Veranstaltungen auf der Vereinswebseite www.Musterverein.de veröffentlicht.
  Die Rechtsgrundlage hierfür ist Art. 6 Abs. lit a) DS-GVO.
- Nur zum Zwecke der Eigenwerbung des Mustervereins wird Werbung an die E-Mail-Adresse der Mitglieder versendet.
  Die Rechtsgrundlage hierfür ist Art. 6 Abs. lit. f) DS-GVO.

4. Berechtigte Interessen des Vereins

Berechtigte Interessen eines Vereins spielen immer dann eine Rolle, wenn der Verein bestimmte Daten verarbeiten möchte, diese Daten jedoch weder für die Erfüllung des Vereinszwecks (laut Mitgliedsvertrags/Satzung) benötigt werden, noch eine Einwilligung der Vereinsmitglieder in die entsprechende Datenverarbeitung vorliegt. Die berechtigten Interessen können daher von Verein zu Verein ganz verschieden sein.

Formulierungsbeispiele für berechtigte Interessen (nicht abschließend):

- Der Musterverein übermittelt ohne vertragliche oder sonstige Verpflichtung auf freiwilliger Basis Mitgliederlisten an den Dachverband... (konkret benennen), um (Grund für das Interesse der Datenübermittlung nennen).
- Der Musterverein hat ein berechtigtes Interesse daran, personenbezogene Daten Dritter, die dem Verein bekannt sind (etwa von Personen, die regelmäßig Eintrittskarten für Spiele beziehen), zum Zwecke der Eigenwerbung zu verarbeiten.
- Der Musterverein hat ein berechtigtes Interesse daran, bei dem Verkauf von Eintrittskarten für Fußballspiele Name, Vorname, Anschrift und Geburtsdatum von unbekannten Personen zu erheben, um zu überprüfen, ob gegen diese ein Stadionverbot ausgesprochen worden ist oder ob sie als gewaltbereit anzusehen sind.

5. Empfänger der personenbezogenen Daten

Übermittelt der Verein personenbezogene Daten seiner Mitglieder an Dritte, so hat der Verein . . . . . .
hierüber zu informieren. Je nach Verarbeitungstätigkeit sind verschiedene Empfänger denkbar. Es ist daher je nach Verarbeitungstätigkeit darüber zu informieren, welche personenbezogenen Daten jeweils an welche Empfänger übermittelt werden.

Formulierungsbeispiele (nicht abschließend):

- Als Mitglied des Muster-Kreisverbandes… (Verband konkret benennen) ist der Verein verpflichtet, seine Mitglieder an den Verband zu melden. Übermittelt werden dabei Name, Adresse,… (Daten bitte konkret nennen). Bei Mitgliedern mit besonderen Aufgaben (z.B. Vorstandsmitglieder) wird zusätzlich die Bezeichnung ihrer Funktion im Verein übermittelt.
- Im Rahmen der Cloud-Mitgliederverwaltung werden die personenbezogenen Daten unserer Mitglieder bei… (Name des Cloud-Anbieters) gespeichert.

6. Drittlandstransfer

(Nur) falls der Verein die Absicht hat, personenbezogene Daten der Mitglieder an ein Drittland
zu übermitteln (z.B. wenn im Rahmen der Cloud-Mitgliederverwaltung die Speicherung in den USA erfolgt), so ist hierauf hinzuweisen.

7. Speicherdauer

Der Verein hat anzugeben, wie lange er welche Daten aufbewahrt. Grundsätzlich müssen personenbezogene Daten gelöscht werden, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Daher ist je nach Zweck der Erhebung die Speicherdauer gesondert anzugeben.

Formulierungsbeispiele (nicht abschließend):

- Die für die Daten Mitgliederverwaltung notwendigen Daten (bitte konkret nennen) werden 2 Jahre nach Beendigung der Vereinsmitgliedschaft gelöscht.
- Die für die Lohnabrechnung der im Verein beschäftigten Personen notwendigen Daten (bitte konkret nennen) werden nach 10 Jahren gelöscht (gesetzliche Aufbewahrungsfrist).
- Die für die die Beitragsverwaltung notwendigen Daten (bitte konkret nennen) werden nach 10 Jahren gelöscht.
- Die IP-Adressen, die beim Besuch der Vereinswebseite gespeichert werden, werden nach 30 Tagen gelöscht.
- Im Falle des Widerrufs der Einwilligung werden die Daten unverzüglich gelöscht.

8. Betroffenenrechte

Dem Vereinsmitglied steht ein Recht auf Auskunft (Art. 15 DS-GVO) sowie ein Recht auf Berichtigung (Art. 16 DS-GVO) oder Löschung (Art. 17 DS-GVO) oder auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) oder ein Recht auf Widerspruch gegen die Verarbeitung (Art. 21 DS-GVO) sowie ein Recht auf Datenübertragbarkeit (Art. 20 DS-GVO) zu.

Das Vereinsmitglied hat das Recht, seine datenschutzrechtliche Einwilligungserklärung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Das Vereinsmitglied hat ferner ein Beschwerderecht beim Landesbeauftragten für Datenschutz und Informationsfreiheit, Lennestraße 1, 19053 Schwerin

9. Pflicht zur Bereitstellung der Daten

Üblicherweise erfolgt im Verein die Bereitstellung der Daten für den Vertragsabschluss (Mitgliedsvertrag/Satzung). Sollte darüber hinaus die Bereitstellung gesetzlich oder vertraglich vorgeschrieben sein, so ist hierauf – sowie zusätzlich auf die Folgen einer Nichtbereitstellung – hinzuweisen – z.B.: ein Angelschein für den Angelverein).

10. Automatisierte Entscheidungsfindung einschließlich Profiling

Ein Hinweis hierauf ist nur dann erforderlich, wenn eine automatisierte Entscheidungsfindung (einschließlich Profiling) gemäß Art. 22 Abs. 1 und Abs. 4 DS-GVO durch den Verein erfolgt.

Art. 22 DS-GVO findet jedoch nur dann Anwendung, wenn die Entscheidung zum Nachteil der betroffenen Person erfolgt und wenn sie durch eine automatisierte Verarbeitung erfolgt ist

(z.B. Profiling, Ablehnung Online-Kreditantrag). Eine derartige automatisierte Entscheidungsfindung ist bei Vereinen allerdings i.d.R. kaum denkbar, so dass ein Hinweis hierauf i.d.R. nicht erfolgen muss.

Einfaches Formulierungsbeispiel für kleine Vereine, die Mitgliederdaten nicht in Drittstaaten übermitteln

Information zur Datenverarbeitung nach Art. 13 DS-GVO

Liebes Vereinsmitglied,
der Schutz Deiner personenbezogenen Daten ist uns sehr wichtig. Damit Du weißt, wer was warum mit Deinen Daten bei uns im Verein macht und wie Du das kontrollieren und ggf. dagegen vorgehen kannst, stellen wir Dir die nachfolgende Information zur Verfügung:

1. **Verantwortlicher nach DS-GVO**
   (Name und Anschrift des Vereins)

2. **Datenschutzbeauftragter**
   (Kontaktdaten – nur falls vorhanden)

3. **Rechtsgrundlage und Zweck der Verarbeitung**
   Deine Mitgliedschaft ist ein Vertrag. Zudem haben wir eine Satzung, in der die Ziele unseres Vereins geregelt sind. Unsere Vereinsziele sind: (bitte aus der Satzung abschreiben)
   Damit wir als Verein diesen Vertrag erfüllen und die Vereinsziele erreichen können, benötigen wir von Dir personenbezogene Daten. Stellst Du uns diese nicht zur Verfügung, können wir Deine Mitgliedschaft nicht bearbeiten. Deshalb erlaubt uns auch ein Gesetz, Deine Daten zu verarbeiten. Falls Du nachschlagen willst, findest Du dieses Gesetz hier: Artikel 6 Absatz 1 Buchstabe b Datenschutz-Grundverordnung.

4. **Empfänger Deiner Daten**
   (hier bitte die Kategorien von Empfängern aus dem Verarbeitungsverzeichnis übernehmen und ggf. nachfolgende Angaben ergänzen)
   Natürlich sind unserer Dienstleister verpflichtet, vertraulich mit Deinen Daten umzugehen. Alle Mitarbeiter im Verein sind zudem ausdrücklich auf wichtige Datenschutzgrundsätze verpflichtet worden.

5. **Wie lange bewahren wir Deine Daten auf?**
   Wir vernichten Deine Daten, wenn Deine Mitgliedschaft bei uns endet, es sei denn, ein Gesetz schreibt uns vor, die Daten länger zu speichern. (ggf. hier bitte die Speicherfristen aus dem Verarbeitungsverzeichnis ergänzen.)

6. **Deine Rechte**

Du kannst von uns Auskunft erhalten, ob und wenn ja welche Daten wir von Dir wie verarbeiten. Du kannst beantragen, dass wir Deine Daten löschen oder falsche Daten berichtigen. Du kannst auch beantragen, dass wir die Verarbeitung einschränken, also beispielsweise nur noch speichern, aber nicht mehr weitergeben. Zudem kannst Du verlangen, dass wir Dir die Daten, die Du uns bereitgestellt hast, in einem maschinenlesbaren Format zur Verfügung stellen.

Zur Geltendmachung Deiner Rechte kannst Du Dich jederzeit vor Ort oder unter den oben angegebenen Kontaktdaten an uns wenden. Wir werden Deinen Anspruch dann prüfen.

Außerdem kannst Du Dich bei der für uns zuständigen Datenschutzaufsichtsbehörde beschweren, wenn Du glaubst, dass wir Deine Daten unrechtmäßig verarbeiten.

Die Anschrift der für uns zuständigen Aufsichtsbehörde lautet:

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Lennéstraße 1, 19053 Schwerin | www.datenschutz-mv.de

Dein Verein

Beispiel eines Informationsblatts für den rein informatorischen Besuch einer Vereins-Homepage

Der Verein ..... verarbeitet bei Aufruf und Nutzung dieser Website personenbezogene Daten im Sinne des Art. 4 Nr. 1 Datenschutz-Grundverordnung (DS-GVO). Betroffene Personen haben das Recht, nach Art. 13 DS-GVO informiert zu werden.

1. Name und Kontaktdaten des Verantwortlichen
Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO ist (Name des Vereins):
Postanschrift:
E-Mail:
Website:

2. Kontaktdaten des Datenschutzbeauftragten
Falls vorhanden, bitte hier die Kontaktdaten des Datenschutzbeauftragten ergänzen

3. Zwecke der Verarbeitung
Wir betreiben diese Website um Öffentlichkeitsarbeit zu betreiben. Hieran haben wir ein berechtigtes Interesse gem. Art. 6 Abs. 1 lit. f DS-GVO.
Die bei der bloß informatorischen Nutzung unserer Website erhobenen Daten werden technisch benötigt, um unsere Website auf Ihrem Endgerät anzuzeigen und um die Systemsicherheit zu gewährleisten.

4. Kategorien personenbezogener Daten, die verarbeitet werden
Bei der informatorischen Nutzung unserer Website erheben wir nur die personenbezogenen Daten, die Ihr Browser an den Server unserer Website übermittelt:

- IP-Adresse des anfragenden Rechners
- Datum und Uhrzeit des Zugriffs
- Name und URL der abgerufenen Datei
- URL oder Provider von der / von dem aus die Datei angefordert wurde
- Verwendeter Browser einschließlich Daten zu den verwendeten Einstellungen der Oberflächendarstellung (Schriftgröße, Schriftart, verwendete Farben etc.) sowie das Betriebssystem Ihres Rechners
- Zugriffsstatus des Web-Servers (Datei übertragen, Datei nicht gefunden, Kommando nicht ausgeführt, etc.)

Darüber hinaus werden bei der informatorischen Nutzung unserer Website so genannte transiente Cookies auf Ihrem Rechner gespeichert. Cookies sind kleine Textdateien, die auf Ihrem Endgerät dem von Ihnen verwendeten Browser zugeordnet gespeichert werden und durch die uns bestimmte Informationen zufließen. Cookies können keine Programme ausführen oder Viren auf Ihren Computer übertragen. Sie dienen dazu, unser Internetangebot insgesamt benutzerfreundlicher und effektiver zu machen.

Transiente Cookies werden automatisiert gelöscht, wenn Sie den Browser schließen. Dazu zählen insbesondere die von uns ausschließlich verwendeten Session Cookies. Diese Speichern eine so genannte Session-ID, mit welcher sich verschiedene Anfragen Ihres Browsers der gemeinsamen Sitzung zuordnen lassen. Dadurch kann Ihr Rechner innerhalb einer Sitzung wiedererkannt werden, wenn Sie auf unsere Website zurückkehren. Die Session-Cookies werden automatisch gelöscht, wenn Sie den Browser schließen.
Sie können Ihre Browser-Einstellung entsprechend Ihren Wünschen konfigurieren und die Annahme von Cookies ablehnen. Wir weisen Sie darauf hin, dass Sie dann eventuell nicht alle Funktionen dieser Website nutzen können.

5. Rechtsgrundlage für die Verarbeitung
Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch uns ist Art. 6 Abs. 1 Buchst. f DS-GVO.

6. Empfänger oder Kategorien von Empfängern
Die bei der informatorischen Nutzung unserer Website erhobenen personenbezogenen Daten werden durch die Mitarbeiterinnen und Mitarbeiter verarbeitet.
Die technische Infrastruktur für die Verarbeitung personenbezogener Daten stellt uns (...) zur Verfügung. Dabei greift diese auf technische Dienstleistungen von Unterauftragnehmern zurück.

7. Speicherdauer
Die bei der informatorischen Nutzung unserer Website erhobenen personenbezogenen Daten werden nach einem Tag gelöscht (bitte sicherstellen).

8. Rechte der betroffenen Person
Sie haben uns gegenüber das Recht,
- gemäß Art. 15 DS-GVO Auskunft über Ihre von uns verarbeiteten personenbezogenen Daten zu verlangen,
- gemäß Art. 16 DS-GVO die Berichtigung Sie betreffender unrichtiger personenbezogener Daten zu verlangen,
- gemäß Art. 17 DS-GVO die Löschung Ihrer bei uns gespeicherten personenbezogenen Daten zu verlangen, insbesondere, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind und
- gemäß Art. 18 DS-GVO die Einschränkung der Verarbeitung Sie betreffender personenbezogener Daten zu verlangen, etwa wenn Sie die Richtigkeit Sie betreffender personenbezogener Daten bestreiten und wir dies überprüfen müssen.

Darüber hinaus haben Sie gemäß Art. 21 DS-GVO uns gegenüber das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten einzulegen.
Zudem können Sie sich bei der für uns zuständigen Aufsichtsbehörde beschweren.

Die Anschrift der für uns zuständigen Aufsichtsbehörde lautet:
Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Lennéstraße 1, 19053 Schwerin | www.datenschutz-mv.de

9. E-Mail-Sicherheit

Wenn Sie uns eine E-Mail senden, so wird Ihre E-Mail-Adresse nur für die Korrespondenz mit Ihnen verwendet.
Wenn Sie eine E-Mail mit schutzwürdigem Inhalt an uns senden wollen, so empfehlen wir dringend, diese zu verschlüsseln, um eine unbefugte Kenntnisnahme und Verfälschung auf dem Übertragungsweg zu verhindern.

Ihr Verein

Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher gem. Artikel 30 Abs. 1 DS-GVO

Vorblatt

Angaben zum Verantwortlichen
Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.
Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse
Internet-Adresse

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen
Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Angaben zum Vertreter des Verantwortlichen
Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.
Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)
* sofern gem. Artikel 37 DS-GVO benannt
Anrede Titel
Name, Vorname
Straße
Postleitzahl
Ort Telefon
E-Mail-Adresse

Verarbeitungstätigkeit: lfd. Nr.:
Benennung:

Datum der Einführung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a)	
Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b)	
Optional: Name des eingesetzten Verfahrens	
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ ...
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)	☐ ☐ ☐ Besondere Kategorien personenbezogener Daten (Art. 9): ☐
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)	☐ Intern(Zugriffsberechtigte) Abteilung/ Funktion ☐ extern Empfängerkategorie ☐ Drittland oder internationale Organisation (Kategorie)

ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt:
Nennung der konkreten Datenempfänger	☐ Drittland oder internationale Organisation (Name)
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)	

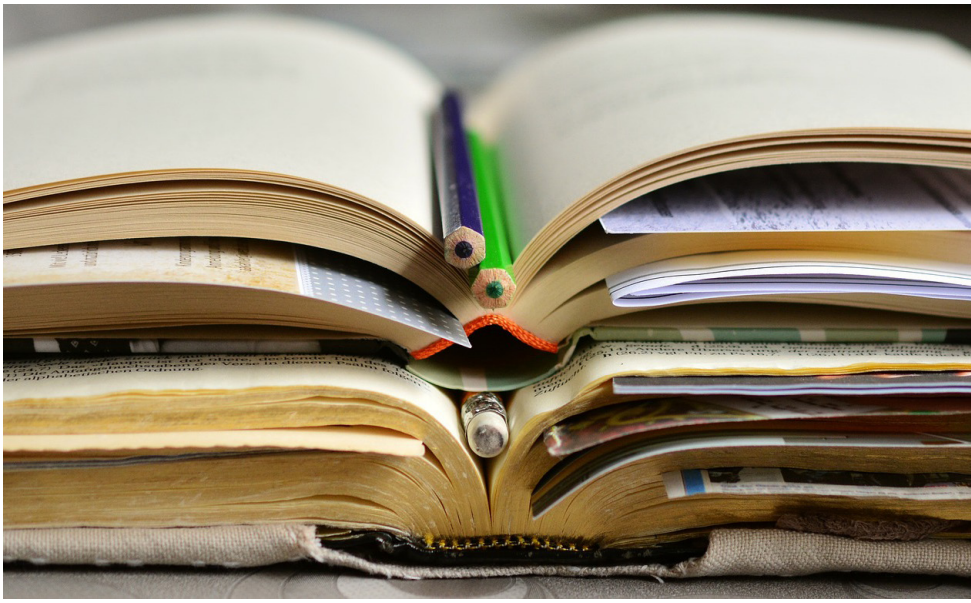
Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DS-GVO (Art. 30 Abs. 1 S. 2 lit. g)
Siehe TOM-Beschreibung in den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten", Ziff. 6.7. und 6.8

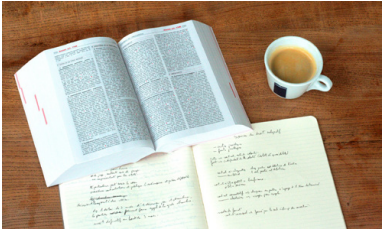
.....

Verantwortlicher Datum Unterschrift

TEIL II

DS-GVO-Vertiefung – Ausführliche Orientierungshilfe zu Einzelfragen





4. Rechtsgrundlagen für den Umgang mit personenbezogenen Daten von Mitgliedern und sonstigen Personen

4.1 Datenschutzgrundverordnung und Bundesdatenschutzgesetz – neu als Rechtsgrundlage

Seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DS-GVO) in Deutschland und in allen anderen Mitgliedstaaten der Europäischen Union geltendes Recht. Die DS-GVO ist ab diesem Zeitpunkt unmittelbar anwendbar und verdrängt die bisher geltenden datenschutzrechtlichen Regelungen. An einigen Stellen der Grundverordnung ist der nationale Gesetzgeber ermächtigt, die Regelungen der Verordnung zu konkretisieren und zu ergänzen (sogenannte Öffnungsklauseln). Hiervon hat der Gesetzgeber durch die Schaffung des BDSG-neu Gebrauch gemacht. Rechtsgrundlage für die Verarbeitung personenbezogener Daten sind daher seit dem 25. Mai 2018 die DS-GVO (mitsamt ihren „Erwägungsgründen“) und das BDSG-neu.
Verarbeitet ein Verein (Verband) ganz oder teilweise automatisiert personenbezogene Daten seiner Mitglieder und sonstiger Personen oder erfolgt eine nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, ist nach Art. 2 Abs. 1 DS-GVO deren Anwendungsbereich eröffnet.
Unerheblich ist dabei, ob der Verein ins Vereinsregister eingetragen ist und damit eine eigene Rechtspersönlichkeit besitzt, oder ob es sich um einen nicht rechtsfähigen Verein handelt.
Da die DS-GVO nicht mehr zwischen öffentlichen und nicht-öffentlichen Stellen unterscheidet, gelten für Vereine grundsätzlich sämtliche Vorschriften der DS-GVO.

4.2 Begriffsbestimmungen – personenbezogene Daten sind …

Personenbezogene Daten sind nicht nur die zur unmittelbaren Identifizierung einer natürlichen Person erforderlichen Angaben, wie etwa Name, Anschrift und Geburtsdatum, sondern darüber hinaus alle Informationen, die sich auf eine in sonstiger Weise identifizierte oder identifizierbare natürliche Personen beziehen (Art. 4 Nr. 1

DS-GVO), wie beispielsweise Familienstand, Zahl der Kinder, Beruf, Telefonnummer, E-Mail-Adresse, Anschrift, Eigentums- oder Besitzverhältnisse, persönliche Interessen, Mitgliedschaft in Organisationen, Datum des Vereinsbeitritts, sportliche Leistungen, Platzierung bei einem Wettbewerb und dergleichen. Dies gilt für Informationen jedweder Art, also für Schrift, Bild oder Tonaufnahmen. Nicht von der DS-GVO geschützt werden Angaben über Verstorbene, wie etwa in einem Nachruf für ein verstorbenes Vereinsmitglied im Vereinsblatt oder die Nennung auf einer Liste der Verstorbenen (Erwägungsgrund 27 DS-GVO).
Statt einer Unterteilung in die Erhebung, Verarbeitung oder Nutzung der Daten wie bisher wird in der DS-GVO einheitlich der Begriff Verarbeitung verwendet. Der Begriff ist sehr weit gefasst und umfasst jeden Vorgang oder jede Vorgangsreihe in Zusammenhang mit personenbezogenen Daten. Als Verarbeitungsarten nennt die DS- GVO neben dem Erheben, Erfassen, Verwenden, Offenlegen, Verbreiten, Abgleichen das Löschen sowie das Vernichten (Art. 4 Nr. 1 DS-GVO).
Dateisystem ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob die Sammlung zentral, dezentral oder nach funktionalen oder geographischen Gesichtspunkten geordnet geführt wird (Art. 4 Nr. 6 DS-GVO). Dazu zählen auch Papier-Akten.
Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DS-GVO). Dem Verein (Verband) sind seine unselbständigen Untergliederungen wie Abteilungen, Ortsvereine oder Ortsgruppen sowie seine Funktionsträger, Auftragnehmer (s. u. Nr. 3.2), und seine Mitarbeiter, soweit diese im Rahmen der Aufgabenerfüllung für den Verein tätig werden, zuzurechnen. Die Vereinsmitglieder einerseits sowie die Dachverbände andererseits, in denen der Verein selbst Mitglied ist, sind dagegen als außerhalb des Vereins stehende Stellen und damit als Dritte anzusehen.
Auftragsverarbeiter ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DS-GVO). Eine Auftragsverarbeitung spielt beispielsweise bei der Verlagerung der Mitgliederverwaltung in eine Cloud eine wichtige Rolle, auch bei der EDV-Wartung und der Aktenvernichtung.

4.3 Rechtmäßigkeit der Verarbeitung

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten richtet sich nach Art. 6 Abs. 1 DS-GVO, bei besonderen Kategorien personenbezogener Daten (z. Bsp. Gesundheitsdaten) zusätzlich nach Art. 9 DS-GVO. Damit eine Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage, die sich aus der DS-GVO, aus

dem sonstigen Unions-recht oder dem Recht der Mitgliedsstaaten ergibt, verarbeitet werden (Art. 6 Abs. 1 DS-GVO; Erwägungsgrund 40 DS-GVO). Datenschutzrechtlich ist nicht etwa alles erlaubt, was nicht ausdrücklich verboten ist. Vielmehr bedarf umgekehrt jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage.

RECHTSGRUNDLAGEN

Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten kommen insbesondere Art. 6 Abs. 1 lit. b) und lit. f) DS-GVO in Betracht. Die Mitgliedschaft in einem Verein ist als Vertragsverhältnis zwischen den Mitgliedern und dem Verein anzusehen, dessen Inhalt im Wesentlichen durch die Vereinssatzung und sie ergänzende Regelungen (z.B. eine Vereinsordnung) vorgegeben wird. Eine Vereinssatzung bestimmt insoweit die Vereinsziele, für welche die Mitgliederdaten genutzt werden können.
Erhebt ein Verein personenbezogene Daten von einer betroffenen Person (z. B. Vereinsmitglied, Teilnehmer an einem Wettbewerb oder Lehrgang), so sind die Zwecke, für welche die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen (Art. 5 Abs. 1 lit. b) DS-GVO).
Hierbei ist jedoch zu beachten, dass die Vereinssatzung einer Inhaltskontrolle nach § 242 des Bürgerlichen Gesetzbuches (BGB) unterliegt. Das Vereinsmitglied ist vor unbillig überraschenden Bestimmungen und Belastungen zu schützen, mit denen es beim Vereinsbeitritt nicht rechnen konnte. Regelungen in der Vereinssatzung, die verfassungsrechtlich geschützte Positionen der Mitglieder beeinträchtigen, sind daher unwirksam. Dies kann etwa dann der Fall sein, wenn der Verein durch die Satzung eine Verarbeitung personenbezogener Daten vorsieht, die weder für die Begründung und Durchführung des zwischen Mitglied und Verein durch den Beitritt zustande kommenden rechtsgeschäftsähnlichen Schuldverhältnisses noch für die Erreichung des Vereinszwecks erforderlich ist.
Auch später darf die Vereinsatzung in Bezug auf die Verarbeitung personenbezogener Daten nicht einfach durch Mehrheitsbeschluss geändert werden. Erfordert der neue Vereinszweck eine weitergehende Verarbeitung personenbezogener Daten, darf die Satzung nur insoweit geändert werden, wie der neue Verarbeitungszweck mit dem ursprünglichen in einem Zusammenhang steht (vgl. Art. 6 Abs. 4 lit. a) DS- GVO, Erwägungsgrund 50). Aus dem Vertragsverhältnis folgt, dass der Verein bei der Erhebung, Verarbeitung und Nutzung von Daten die Datenschutzgrundrechte seiner Mitglieder angemessen berücksichtigen muss.
Bei Gesundheitsdaten kommt regelmäßig aber nur eine Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO in Betracht.

HINWEISPFLICHT BEI DATENERHEBUNG

Bei der Gestaltung von Erhebungsbögen und (Online-)Formularen, die zur Datenerhebung eingesetzt werden, ist die Hinweispflicht des Art. 13 DS-GVO zu beachten. Erhebt ein Verein personenbezogene Daten vom Betroffenen, muss dieser nach Art. 13 DS-GVO belehrt werden

Vereinsmitglieder sind deswegen bei der Datenerhebung darauf aufmerksam zu machen, welche Angaben für die Mitgliederverwaltung und welche für die Verfolgung des Vereinszwecks bestimmt sind. Sollen Daten zum Zwecke der Verfolgung des Vereinsziels oder der Mitgliederverwaltung und -betreuung an andere Stellen übermittelt werden (etwa an einen Dachverband, damit dieser Turniere ausrichten kann, an eine Unfallversicherung oder an die Gemeinde, muss auch darauf hingewiesen werden. Insbesondere ist das Mitglied darauf hinzuweisen, welche Angaben im Vereinsblatt veröffentlicht oder in das Internet eingestellt werden, etwa im Falle der Wahl als Vorstandsmitglied (s. u. Nr. 5.1 und 5.3). Kann dem Vereinsmitglied ein bestimmter Vorteil, etwa ein Versicherungsschutz, nur gewährt werden, wenn es dazu bestimmte Angaben macht, muss es darauf aufmerksam gemacht werden, welche Nachteile die Verweigerung dieser Informationen mit sich bringt.

Erfolgt eine Erhebung personenbezogener Daten **direkt bei der betroffenen Person**, so hat der Verein aus Gründen der Transparenz von Datenverarbeitungsprozessen zum Zeitpunkt der Datenerhebung eine entsprechende **datenschutzrechtliche Unterrichtung** vorzunehmen (Art. 13 Abs. 1 und Abs. 2 DS-GVO). Daraus folgt, dass der Verein in jedem Formular, das er zur Erhebung personenbezogener Daten nutzt, auf Folgendes hinweisen muss:

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
- Kontaktdaten des Datenschutzbeauftragten
- Zwecke der Verarbeitung (bitte im Einzelnen aufzählen)
- Rechtsgrundlage der Verarbeitung
- berechtigte Interessen i.S.d. Art. 6 Abs. 1 lit. f) DS-GVO
- Empfänger oder Kategorien von Empfängern (z.B. Weitergabe personenbezogener Daten an eine Versicherung, an den Dachverband, an alle Vereinsmitglieder, im Internet)
- Absicht über Drittlandtransfer (z.B. bei Mitgliederverwaltung in der Cloud), sowie Hinweis auf (Fehlen von) Garantien zur Datensicherheit
- Speicherdauer der personenbezogenen Daten
- Belehrung über Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht gegen Verarbeitung)
- Hinweis auf jederzeitiges Widerrufsrecht der Einwilligung
- Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde

Teilt der Verantwortliche die vorgesehenen Informationen nicht, nicht vollständig oder inhaltlich unrichtig mit, so verletzt er seine Informationspflichten. Das ist gemäß Art.83 Abs. 5 lit. b) DS-GVO bußgeldbewehrt.

Werden personenbezogene Datei auf **andere Weise** als bei der betroffenen Person erhoben, so richten sich die Informationspflichten nach Art. 14 Abs. 1 und Abs. 2 DS-GVO. Die meisten der Informationspflichten aus Art. 14 Abs. 1 und Abs. 2 DS-GVO haben denselben Inhalt wie Art. 13 Abs. 1 und Abs. 2 DS-GVO. **Zusätzlich** muss der Verein die betroffene Person über die **Kategorie** der verarbeiteten personenbezogenen Daten und über die Quelle der erhobenen Daten informieren. Der Verein muss

diese Informationen innerhalb einer angemessenen Frist, spätestens jedoch innerhalb eines Monats nach der Erhebung erteilen (Art. 14 Abs. 3 lit a) DS-GVO). Ein Verstoß gegen die Informationspflicht kann eine Geldbuße gemäß Art. 83 Abs. 5 lit. b) DS-GVO zur Folge haben.

WEITERE INFORMATIONEN: zum diesem Thema finden Sie im Kurzpapier der DSK unter www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Kurzpapiere/Kurzpapier_Nr_10.pdf

VEREINSINTERNE REGELUNGEN ZUM DATENSCHUTZ

Der Verein sollte, die Grundzüge der Datenverarbeitung schriftlich festlegen. Entsprechende Datenschutzregelungen können entweder in die Vereinssatzung aufgenommen oder in einem gesonderten Regelwerk niedergelegt werden. Für Letzteres gibt es keine feste Bezeichnung; am gebräuchlichsten sind z.B. die Begriffe „Datenschutzordnung", „Datenschutzrichtlinie" oder „Datenverarbeitungsrichtlinie". Die Datenschutzordnung kann, wenn die Vereinssatzung nichts anderes bestimmt, vom Vorstand oder von der Mitgliederversammlung beschlossen werden und muss nicht die Qualität einer Satzung haben.

Es ist empfehlenswert, sich beim Aufbau der Datenschutzregelungen am Weg der Daten von der Erhebung über die Speicherung, Nutzung, Verarbeitung (insbesondere Übermittlung) bis zu ihrer Sperrung und Löschung zu orientieren. Dabei ist jeweils **konkret festzulegen, welche Daten** (z.B. Name, Vorname, Adresse, E-Mail- Adresse usw.) welcher Personen (z.B. Vereinsmitglieder, Teilnehmer an Veranstaltungen oder Lehrgängen, Besucher von Veranstaltungen) **für welche Zwecke** verwendet werden, ggf. auch, ob Vordrucke und Formulare zum Einsatz kommen. Die bloße Wiedergabe des Wortlauts der Bestimmungen der DS-GVO bzw. des BDSG- neu sind in keinem Fall ausreichend. Die DS-GVO bzw. das BDSG-neu machen die Zulässigkeit der Verarbeitung von Daten vielfach von Interessenabwägungen abhängig oder stellt sie unter den Vorbehalt der Erforderlichkeit. Im Interesse der Rechtssicherheit sollten diese abstrakten Vorgaben soweit irgend möglich konkretisiert und durch auf die Besonderheiten und Bedürfnisse des jeweiligen Vereins angepasste eindeutige Regelungen ersetzt werden.

Der Verein sollte insbesondere schriftlich festlegen, welche Daten beim Vereinseintritt für die **Verfolgung des Vereinsziels** und für die **Mitgliederbetreuung und -verwaltung** notwendigerweise erhoben werden. Auch sollte geregelt werden, welche Daten für welche **anderen Zwecke** des Vereins oder zur Wahrnehmung **der Interessen Dritter** bei den Mitgliedern in Erfahrung gebracht werden. Ferner muss geregelt werden, welche **Daten von Dritten** erhoben werden, wobei hier auch der Erhebungszweck festzulegen ist. Auch sollte erkennbar sein, welche Angaben für Leistungen des Vereins erforderlich sind, die nicht erbracht werden können, wenn der Betroffene nicht die dafür erforderlichen Auskünfte gibt.

Der Verein sollte außerdem regeln, welcher **Funktionsträger** zu welchen Daten Zugang hat und zu welchem Zweck er Daten von Mitgliedern und Dritten verarbeiten

und nutzen darf. Ferner sollte geregelt werden, welche Daten zu welchem Zweck im Wege der **Auftragsdatenverarbeitung** (s. u. Nr. 6.1) verarbeitet werden.
Des Weiteren sollte der Verein festlegen, zu welchem Zweck welche Daten von wem an welche Stellen (das können auch Vereinsmitglieder sein) **übermittelt** werden bzw. welche Daten so gespeichert werden (dürfen), dass **Dritte** – also Personen, die nicht zur regelmäßigen Nutzung der Daten befugt sind (s. u. Kapitel 5) – darauf Zu-griff nehmen können. Der Kreis dieser Zugriffsberechtigten muss genau beschrieben sein. Auch muss geregelt werden, unter welchen Voraussetzungen welche Datenübermittlung erfolgen darf, insbesondere welche **Interessen des Vereins oder des Empfängers** dabei als berechtigt anzusehen sind. Auch sollte festgelegt werden, zu welchem Zweck die Empfänger die erhaltenen Daten nutzen dürfen und ob sie sie weitergeben können. Ferner sollte geregelt sein, welche Daten üblicherweise am **„Schwarzen Brett“** oder in den **Vereinsnachrichten veröffentlicht** und welche in das Internet oder Intranet eingestellt werden.
Diese Datenschutzordnung sollte von der Mitgliederversammlung beschlossen werden. Auf keinen Fall sollte in der Satzung aber geregelt werden, dass die Verarbeitung aller Datenkategorien generell immer nur mit Einwilligung zulässig sein soll.

EINWILLIGUNG

Eine **Einwilligung** in die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist erforderlich, soweit der Verein in weitergehendem Maße personenbezogene Daten verarbeitet, als er aufgrund der unten unter Kapitel 5. dargestellten Regelungen befugt ist. **Es empfiehlt sich nicht, Einwilligungen für Datenverarbeitungsmaßnahmen einzuholen, die bereits aufgrund einer gesetzlichen Erlaubnis möglich sind. Denn dadurch wird beim Betroffenen der Eindruck erweckt, er könne mit der Verweigerung der Einwilligung oder ihrem späterem Widerruf die Datenverarbeitung verhindern.** Hat der Verein aber von vornherein die Absicht, im Falle der Verweigerung des Einverständnisses auf die gesetzliche Verarbeitungsbefugnis zurückzugreifen, wird der Betroffene getäuscht, wenn man ihn erst nach seiner ausdrücklichen Einwilligung fragt, dann aber doch auf gesetzliche Ermächtigungen zurückgreift.
Eine Einwilligung ist datenschutzrechtlich nur wirksam, wenn sie auf der **freien Entscheidung des Betroffenen** beruht und dieser zuvor ausreichend und verständlich darüber **informiert** worden ist, welche Daten aufgrund der Einwilligung für welchen Zweck vom Verein verarbeitet werden sollen. Insbesondere soll darauf aufmerksam gemacht werden, welche verschiedenen Verarbeitungsvorgänge i.S. des Art. 4 lit. a) DS-GVO vorgesehen sind, unter welchen Voraussetzungen die Daten an **Dritte weitergegeben** werden, dass die **Erklärung freiwillig** ist, wie lange die Daten bei wem gespeichert sein sollen und was die Einwilligung rechtlich für die betroffene Person bedeutet. Soweit es nach den Umständen des Einzelfalles erforderlich ist, oder wenn die betroffene Person das verlangt, soll sie auch über die Folgen der Verweigerung der Einwilligung belehrt werden (§ 51 Abs. 4 Sätze 3 und 4 BDSG-neu). Auch soll die

betroffene Person vor der Abgabe der Einwilligung darauf aufmerksam gemacht werden, dass sie diese **stets widerrufen** kann (§ 51 Abs. 3 Satz 3 BDSG-neu). Eine Dokumentation dieser Informationen ist nicht vorgeschrieben, doch ist der Erklärungsempfänger ggf. beweispflichtig, dass bzw. mit welchem Inhalt die Hinweise er- folgt sind. Die Aufnahme in einem Verein darf grundsätzlich nicht von der Einwilligung in die Datenverarbeitung für vereinsfremde Zwecke abhängig gemacht werden (Art. 7 Abs. 4 DS-GVO).

Im Gegensatz zum BDSG, das für Einwilligungen grundsätzlich die Schriftform und nur ausnahmsweise auch die elektronische Form zulässt, ermöglicht die DS-GVO, dass die Einwilligung **schriftlich, elektronisch, mündlich** oder sogar **konkludent** erfolgen kann.

Jedoch muss der Verein für den Fall, dass die Verarbeitung auf einer Einwilligung beruht, nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat (Art. 7 Abs. 1 DS-GVO). Aus diesem Grund ist zu anzuraten, Einwilligungen zum Zwecke des **Nachweises** schriftlich einzuholen oder die Abgabe einer Einwilligung anderweitig zu dokumentieren.

Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche oder elektronische Erklärung, muss bereits das **Ersuchen um Einwilligung** in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von anderen Sachverhalten klar zu unterscheiden ist (Art. 7 Abs. 2 Satz 1 DS-GVO; § 51 Abs. 2 BDSG-neu). Nicht zuletzt deswegen muss die Einwilligungspassage selbst, wenn sie Teil eines größeren Textes ist, **optisch hervorgehoben** werden. Dies kann durch drucktechnische Hervorhebung oder Absetzen vom sonstigen Erklärungstext geschehen. Die Einwilligung sollte sich nicht im Informationsblatt „verstecken“ sondern deutlich davon getrennt sein. Da grundsätzlich für jede Art der Datenverarbeitung i. S. des Art. 6 lit. a) DS-GVO und für **jeden Verarbeitungsvorgang** eine **gesonderte Einwilligung** eingeholt werden muss (Erwägungsgrund 43 DS-GVO), soll bei Einwilligungen zu Datenübermittlungen an verschiedene Empfänger für unterschiedliche Zwecke der Vordruck so gestaltet sein, dass ein Beitrittswilliger bei der Abgabe seiner Erklärung durch Ankreuzen differenzieren kann.

Datenschutzrechtliche Einwilligungen der Vereinsmitglieder können nicht durch Mehrheitsbeschlüsse der Mitgliederversammlung oder des Vorstands ersetzt werden. Eine sogenannte „Widerspruchslösung“, wonach die Einwilligung unterstellt wird, wenn der Betroffene einer Datenverarbeitungsmaßnahme – etwa der Veröffentlichung seiner Personalien im Internet – nicht ausdrücklich widerspricht, stellt keine wirksame Einwilligung dar.

Eine starre Altersgrenze in Bezug auf die Einwilligungsfähigkeit kennt die DS-GVO außerhalb des Art. 8 DS-GVO (diese Vorschrift gilt nur im Zusammenhang mit kindorientierten Telemedien, wie z.B. an Kinder gerichtete Onlineshops und -spiele) nicht. **Kinder** und **Jugendliche** können daher in die Verarbeitung ihrer personenbezogenen Daten selbst einwilligen, wenn sie in der Lage sind, die Konsequenzen der Verwendung ihrer Daten zu übersehen und sich deshalb auch verbindlich dazu zu äußern.

Maßgeblich ist der jeweilige Verwendungszusammenhang der Daten und der Reifegrad bzw. die Lebenserfahrung des Betroffenen. Bei Kindern unter 13 Jahren ist regelmäßig davon auszugehen, dass sie die Konsequenzen der Verwendung ihrer Daten nicht übersehen können. Ist die Einsichtsfähigkeit zu verneinen, ist die Verarbeitung seiner personenbezogenen Daten nur mit Einwilligung eines Sorgeberechtigten zulässig.

Es empfiehlt sich, eine Einwilligung von Neumitgliedern bereits bei der Aufnahme in den Verein einzuholen. Altmitglieder sollten, wenn möglich, ihre Einwilligungserklärung wiederholen. Alteinwilligungen sind nur dann noch weiter gültig, wenn sie bereits informiert und freiwillig erteilt wurden. Dabei sollte ein Formular Folgendes berücksichtigen:

- Das Vereinsmitglied erteilt seine Einwilligung freiwillig und kann sie jederzeit widerrufen. Das Mitglied kann den Umfang der zu veröffentlichenden Daten von vornherein beschränken.
- Dem Mitglied muss die Tragweite seiner Erklärung bewusst sein. Das ist nur der Fall, wenn es weiß, welche seiner Daten in das Internet eingestellt werden sollen.

5. Erhebung personenbezogener Daten durch den Verein

5.1 Erhebung nur von erforderlichen Daten der Vereinsmitglieder

Ein Verein darf aufgrund des Art. 6 Abs. 1 lit. b) DS-GVO beim Vereinsbeitritt (Aufnahmeantrag oder Beitrittserklärung) und während der Vereinsmitgliedschaft nur solche Daten von Mitgliedern erheben, die für die Begründung und Durchführung des zwischen Mitglied und Verein durch den Beitritt zustande kommenden rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich sind. Damit dürfen alle Daten erhoben werden, die zur **Verfolgung der Vereinsziele** und für die **Betreuung und Verwaltung der Mitglieder** (wie etwa Name, Anschrift, in der Regel auch das Geburtsdatum, ferner Bankverbindung, Bankleitzahl und Kontonummer) **notwendig** sind.
Der Abschluss von **Versicherungsverträgen** zugunsten des Vereins oder seiner Mitglieder ist vom Vereinszweck gedeckt, soweit Risiken bestehen, gegen die sich der Verein nicht zuletzt aus Fürsorgegründen versichern muss, so dass die Daten, die dafür erforderlich sind, erhoben werden dürfen. Grundsätzlich nicht erforderlich ist dagegen die Frage nach der früheren Mitgliedschaft des Beitrittswilligen in einer konkurrierenden Organisation. Die vom Verein erhobenen Daten werden nur dann „gleichzeitig“ Daten eines anderen Vereins, etwa eines **Dachverbandes**, wenn das Vereinsmitglied auch der anderen Vereinigung ausdrücklich und aufgrund eigener Erklärung beitritt.
Nach Art. 6 Abs. 1 lit. f) DS-GVO kann der Verein Daten bei seinen Mitgliedern für einen **anderen Zweck** als zur Verfolgung eigener Vereinsziele und zur Mitgliederbetreuung und -verwaltung **erheben**, wenn der Verein ein **berechtigtes Interesse** daran hat. Zulässig ist es danach aber nicht, Daten, die der Verein zu den Vereinszwecken erhoben hat, zu anderen Zwecken weiterzuverwenden (Zweckänderung). Das ist nur unter den engen Voraussetzungen des Art. 6 Abs. 4 DS-GVO zulässig.
Soll die Verarbeitung personenbezogener Daten aufgrund des Art. 6 Abs. 1 lit. f) DS-GVO erfolgen, ist dies nur zulässig, sofern nicht die **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person** (Datenschutzgrundrechte) überwiegen. Neu ist, dass die DS-GVO davon ausgeht, dass ein solches Überwiegen insbesondere dann vorliegt, wenn es sich bei der betroffenen Person um ein „Kind“ handelt. Bei Kindern **unter 16 Jahren** überwiegen hierbei regelmäßig die schutzwürdigen Interessen des betroffenen Kindes, im Alter zwischen 16 und 18 Jahren kann hingegen eine Abwägung mit anderen Interessen erfolgen.
Überwiegende Interessen oder Grundrechte und Grundfreiheiten können wirtschaftliche und berufliche Belange ebenso sein, wie der Wunsch des Betroffenen, dass seine

Privat-, Intim- und Vertraulichkeitssphäre gewahrt wird. Sollen hierzu Bestandsdaten der Mitglieder verwendet werden und mit den berechtigten Interessen andere Zwecke verfolgt werden, als mit der ursprünglichen Datenerhebung, sollte immer eine Einwilligung eingeholt werden.

5.2 Erhebung von Daten Dritter

Nach Art. 6 Abs. 1 lit. f) DS-GVO kann der Verein Daten von anderen Personen als von Vereinsmitgliedern (z.B. von Gästen, Zuschauern, Besuchern, fremden Spielern, Teilnehmern an Lehrgängen und Wettkämpfen) erheben, soweit dies zur Wahrnehmung **berechtigter Interessen** des Vereins erforderlich ist und sofern nicht die **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person** überwiegen. Ein berechtigtes Interesse besteht grundsätzlich nur an den Daten, die für eine eindeutige Identifizierung erforderlich und ausreichend sind, d.h. Name, Vorname, Anschrift und Geburtsdatum, nicht jedoch Personalausweis- oder Passnummer. So kann es zulässig sein, beim Verkauf von Eintrittskarten etwa für ein Fußballspiel Identifizierungsdaten von dem Verein nicht bekannten Zuschauern zu erheben, um abzuklären, ob gegen sie ein Stadionverbot ausgesprochen worden ist oder ob sie als gewaltbereit anzusehen sind. Vereine sind datenschutzrechtlich grundsätzlich ohne Einwilligung nicht berechtigt, bei Dritten **Erkundigungen** (etwa als Zuchtverband bei den Käufern von Tieren einer bestimmten Hunderasse) – oder **Kontrollen** (etwa als Tierschutzverein) vorzunehmen, selbst wenn sich die Vereinigung solches zum satzungsmäßigen Ziel gesetzt hat.

5.3 Erhebung von Personaldaten der Beschäftigten des Vereins

Die Verarbeitung personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses ist in Art. 88 DS-GVO und § 26 BDSG-neu gesondert geregelt. Als Beschäftigte sind die in § 26 Abs. 8 BDSG-neu aufgeführten Personen anzusehen. Soweit ein Verein daher Personen in einem abhängigen hauptamtlichen Verhältnis beschäftigt (z.B. Mitarbeiter der Vereinsgeschäftsstelle, Trainer) ist § 26 BDSG-neu anwendbar. Danach dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

6. Datenverarbeitung mit Hilfe von Dienstleistern

Die Speicherung personenbezogener Daten eines Vereins kann auch durch ein Serviceunternehmen im Wege der Auftragsdatenverarbeitung erfolgen. Sofern der Verein eigene Beschäftigte hat, müssen deren Personaldaten getrennt von den sonstigen Daten, insbesondere den Mitgliederdaten, gespeichert werden.

6.1 Datenverarbeitung im Auftrag

Insbesondere kleine Vereine bedienen sich zur Finanzierungs- und Adressverwaltung mitunter Sparkassen und sonstiger Dienstleister. Diese werden als Auftragsverarbeiter nach Weisung des Vereins tätig. Eine Datenverarbeitung im Auftrag ist auch dann gegeben, wenn ein Verein seine Mitgliederdaten nicht auf einer eigenen EDV- Anlage speichert, sondern hierfür über das Internet einen Datenbankserver nutzt, den ein Dienstleistungsunternehmen zu diesem Zweck zur Verfügung stellt. Durch die Inanspruchnahme von Dienstleistungen der Post (Briefversand) oder des Betreibers eines Mailservers (beim Versenden von E-Mails) kommt keine Datenverarbeitung im Auftrag zustande.

Nach der DS-GVO ist für die **Auftragsverarbeitung kennzeichnend**, dass der Auftragsverarbeiter über die bloße Beauftragung hinaus gegenüber dem Verantwortlichen **weisungsabhängig** ist, selbst wenn der Auftragsverarbeiter über ein umfassenderes Know-how als sein Auftraggeber verfügt und einen gewissen Spielraum für selbständige Entscheidungen hat, und der Auftragsverarbeiter vom Verantwortlichen **überwacht** wird, selbst wenn der Verantwortliche dazu eine andere Stelle einschaltet. Gegenüber den bisher geltenden Regelungen des § 11 BDSG-alt schreibt die DS-GVO teils erheblich **weitergehende Pflichten** und Verantwortlichkeiten für den **Auftragsverarbeiter** fest. Er tritt insoweit nicht mehr hinter seinen Auftraggeber zurück, sondern ist selbst Adressat eigenständiger, also nicht mehr nur vom Verantwortlichen abgeleiteter Pflichten, bei deren Nichtbeachtung er unmittelbar vom Betroffenen bzw. von den Behörden in Anspruch genommen werden kann.

Im Fall der Datenverarbeitung im Auftrag ist zu beachten, dass der Verein nur Auftragsverarbeiter einsetzen darf, die eine hinreichende Garantie für eine datenschutzkonforme Datenverarbeitung gewährleisten (vgl. Art 28 Abs. 1 DS-GVO). Der **Nachweis** für diese Qualifikation kann über entsprechende **Zertifizierungen** gemäß Art. 42 DS-GVO und anerkannte Verhaltenskodizes nach Art. 40 DS-GVO geführt werden (Art. 28 Abs. 5 DS-GVO).

Die Auftragsverarbeitung darf nur auf der Grundlage eines **bindenden Vertrages** erfolgen. Art. 28 Abs. 3 und Abs. 6 DS-GVO sieht vor, dass auch **„ein anderes Recht-**

sinstrument“ als ein eigens ausgehandelter Vertrag nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten Basis der Auftragsdatenverarbeitung sein kann. Die Auftraggeber bzw. Auftragnehmer haben somit künftig die Auswahl zwischen individuellen Verträgen, Standardverträgen, die die EU-Kommission bereitstellt, Standardverträgen, die die Aufsichtsbehörde bereitstellt, und zertifizierten Vertrags- mustern.

MUSTER: Eine Formulierungshilfe finden Sie z.B. hier: www.datenschutz-mv.de/datenschutz/DS-GVO/Hilfsmittel-zur-Umsetzung/

Sowohl der Vertrag als auch die alternativen Rechtsinstrumente müssen den in Art. 28 Abs. 3 DS-GVO **festgelegten Anforderungen** genügen. Im Einzelnen muss festgelegt sein:

- Gegenstand und Dauer der Auftragsdatenvereinbarung
- Umfang, Art und Zweck der Datenerhebung
- Art der zu verarbeitenden personenbezogenen Daten
- Kategorie der von der Datenverarbeitung betroffenen Personen
- Pflichten und Rechte des Verantwortlichen
- Umfang der Weisungen, die zu dokumentieren sind
- Verpflichtung des vom Auftragsverarbeiter eingesetzten Personals auf das Datengeheimnis
- technische und organisatorische Maßnahmen
- zulässige Unterauftragsverhältnisse
- Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Erfüllung der in Kapitel III der DS-GVO vorgeschriebenen Rechte der betroffenen Personen
- Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei den in Art. 32 ff. DS-GVO festgeschriebenen Verpflichtungen, insbesondere bei der Meldepflicht von Datenschutzverstößen
- Abwicklung nach Beendigung der Auftragsverarbeitung
- Kontrollrechte des Auftraggebers

Gemäß Art. 28 Abs. 9 DS-GVO muss der Vertrag entweder **schriftlich** oder in einem **elektronischen Format**, also nicht mehr – wie bisher – mit qualifizierter elektronischer Signatur, abgefasst sein. Hierfür genügt jedoch nicht jede bestätigende E- Mail, vielmehr sind nur solche elektronische Formate akzeptabel, die beiden Parteien zu ihrer Information zugänglich sind, und wenn damit dokumentiert ist, welcher Vertragsinhalt bestätigt wurde. Die Erklärung soll deswegen der „**Textform**“ i. S. des § 126b BGB entsprechen. Im Ergebnis muss der Vertragspartner in der Lage sein, das akzeptierte Dokument „bei sich“ zu speichern und auszudrucken.

Nach der DS-GVO ist der Auftragnehmer kein Dritter, sondern quasi „verlängerter Arm“ des Verantwortlichen. Eine gesonderte Rechtsgrundlage um die Daten dem Auftragnehmer offenzulegen, ist nicht erforderlich.

WEITERE INFORMATIONEN: Näheres finden Sie im Kurzpapier 13 zur Auftragsverarbeitung: www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Kurzpapiere/Kurzpapier_Nr_13.pdf

Der **Verantwortliche** ist grundsätzlich für jedwede Verarbeitung personenbezogener Daten, die er selbst vornimmt oder von ihm durch einen Auftragsverarbeiter veranlasst wird, verantwortlich (Art. 24, Art. 4 Nrn. 2, 7 und 8 DS-GVO).
Der Verantwortliche hat die **Gewährleistung der in Kapitel III der DS-GVO** aufgeführten Betroffenenrechte (Informationspflichten, Auskunftsansprüche, Recht auf Löschung und Berichtigung, Recht auf Einschränkung der Verarbeitung, Recht auf Datenübertragbarkeit, Widerspruchsrecht) sicherzustellen. Dabei muss er den betroffenen Personen nach Art. 13 Abs. 1 lit. e) und f), Abs. 3, Art. 14 Abs. 1 lit. e) und f), Abs. 4, Art. 15 Abs. 1 lit. c) DS-GVO auch **mitteilen**, dass Auftragsverarbeiter als Empfänger ihrer Daten in Betracht kommen. Auch muss der Verantwortliche nach Art. 19 DS-GVO den Auftragsverarbeiter als Empfänger von Daten unterrichten, wenn diese berichtigt oder gelöscht wurden bzw. wenn deren Verarbeitung nach Art. 18 DS-GVO einzuschränken ist.
Der Verantwortliche hat den Auftragsverarbeiter grundsätzlich fortwährend zu **kontrollieren**, ob dieser die Einhaltung der Datenschutzvorschriften gewährleisten kann. Nach Art. 29 DS-GVO ist der Verantwortliche berechtigt und verpflichtet, dem Auftragsverarbeiter **Weisungen** zu erteilen, soweit diese zur Durchsetzung des Auftragsverarbeitungs-Vertrags oder der gesetzlichen Pflichten des Verantwortlichen bzw. des Auftragsverarbeiters erforderlich sind.

6.2 Cloud-Mitgliederverwaltungsdienste

Auch bei der Verlagerung personenbezogener Daten von Vereinsmitgliedern in eine Cloud liegt eine Auftragsdatenverarbeitung vor. Auftragsverarbeiter können nach den Vorschriften der Auftragsverarbeitung grundsätzlich sowohl im **EU-Raum** wie auch in **Drittländern** tätig werden.
Der räumliche Anwendungsbereich der DS-GVO umfasst nach deren Art. 3 Abs. 1 alle Datenverarbeitungsvorgänge, die in der EU erfolgen, und die von einem Verantwortlichen oder einem Auftragsverarbeiter mit Hauptsitz oder einer Niederlassung in der EU veranlasst werden, unabhängig davon, wo die Datenverarbeitung konkret erfolgt. Die Regelungen der DS-GVO finden ferner unter bestimmten Voraussetzungen Anwendung, wenn zwar der Verantwortliche oder der Auftragsverarbeiter nicht in der EU ansässig ist, aber die betroffene Person sich in der EU befindet (Art. 3 Abs. 2 DS-GVO). Die Weitergabe von personenbezogenen Daten an Auftragsverarbeiter in ein Land außerhalb der EU ist nach der DS-GVO nur unter den zusätzlichen Voraussetzungen der Art. 44 DS-GVO zulässig.

7. Nutzung von personenbezogenen Daten

7.1 Nutzung von Mitgliederdaten

Innerhalb eines Vereins sind die Aufgaben in der Regel abgegrenzt und bestimmten Funktionsträgern zugewiesen. Wer für was zuständig ist, wird durch die Satzung oder die Geschäftsordnung bestimmt. Für den Umgang mit Mitgliederdaten gilt, dass jeder Funktionsträger nur die für die Erfüllung seiner Aufgaben erforderlichen Mitgliederdaten kennen, verarbeiten oder nutzen darf. So darf etwa der Vorstand auf alle Mitgliederdaten zugreifen, wenn er diese zur Aufgabenerledigung benötigt. Auch müssen der Vereinsgeschäftsstelle alle Mitgliederdaten regelmäßig für die Mitgliederverwaltung und -betreuung zur Verfügung stehen, während es in der Regel für den Kassierer genügt, wenn er die für den Einzug der Mitgliedsbeiträge relevanten Angaben (Name, Anschrift und Bankverbindung) kennt. Dabei dürfen die Daten grundsätzlich nur zur Verfolgung des Vereinszwecks bzw. zur Betreuung und Verwaltung von Mitgliedern genutzt werden (Art. 6 Abs. 1 lit. b) DS-GVO).

7.2 Nutzung von Daten Dritter

Daten Dritter, etwa von Lieferanten, Besuchern oder Aushilfsspielern anderer Vereine, dürfen gespeichert und genutzt werden, wenn dies für die Begründung oder Durchführung eines rechtsgeschäftlichen Schuldverhältnisses (Vertrag) mit diesen Personen erforderlich ist (Art. 6 Abs. 1 lit. b) DS-GVO) oder der Verein ein berechtigtes Interesse daran hat und nicht erkennbar ist, dass dem schutzwürdigen Interessen der Betroffenen entgegenstehen (Art. 6 Abs. 1 lit. f) DS-GVO, s. o. Nr. 2.1). Diese Daten dürfen grundsätzlich nur zu dem Zweck verwendet werden, zu dem sie der Verein erhoben oder erhalten hat. Lediglich dann, wenn eine Weiterverarbeitung der Daten mit dem Zweck der ursprünglichen Datenerhebung als vereinbar anzusehen ist, ist eine Zweckänderung zulässig (Art. 6 Abs. 4 DS-GVO). Denn ein Vertragspartner darf sich in der Regel darauf verlassen, dass der Verein seine Daten nur im Rahmen des Vertragsverhältnisses nutzt.

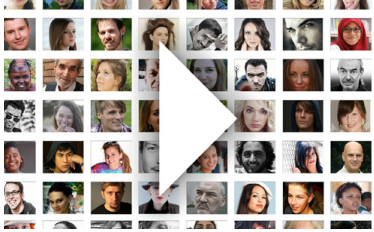
7.3 Nutzung der Daten des Vereins für Spendenaufrufe und Werbung

Vereine haben regelmäßig ein erhebliches Interesse an der Mitglieder- und Spendenwerbung, um einen ausreichenden Mitgliederbestand und genügend finanzielle Mittel sicherzustellen. Die Daten seiner **Vereinsmitglieder** darf der Verein nur für **Spendenaufrufe** und für **Werbung** zur Erreichung der **eigenen Ziele des Vereins** nutzen (Art. 6 Abs. 1 lit. b) DS-GVO). Die Nutzung von Mitgliederdaten für die **Werbung Dritter** ist ohne Einwilligung der Mitglieder grundsätzlich nicht zulässig.

Daten **Dritter**, etwa von Personen, die regelmäßig Eintrittskarten für Spiele beziehen, darf der Verein für Werbezwecke nutzen, wenn diese entweder darin eingewilligt haben (s.o. Kapitel 8.5) oder der Verein die Daten von Anfang an zu Werbezwecken erhoben hat, weil er berechtigte Interessen an der Nutzung zu Werbezwecken hat und keine Interessen oder Grundrechte des Dritten überwiegen (Art. 6 Abs. 1 lit. f) DS-GVO). Einzubeziehen in diese Interessenabwägung sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen (Erwägungsgrund 47 DS-GVO).

Die vernünftigen Erwartungen werden bei werblichen Ansprachen maßgebend durch die Informationen nach Art. 13, 14 DS-GVO zu den Zwecken der Datenverarbeitung bestimmt. Informiert der Verein daher transparent und umfassend über eine vorgesehene Nutzung der Daten, geht die Erwartung der betroffenen Person in aller Regel auch dahin, dass ihre Daten entsprechend genutzt werden. Zu beachten ist jedoch, dass die von der Werbung betroffene Person ein **jederzeitiges Widerspruchsrecht** hat (Art. 21 Abs. 2 DS-GVO), auf das der Verein ausdrücklich **hinzuweisen** hat (Art. 21 Abs. 4 DS-GVO). Ein solcher Widerspruch hat zur Folge, dass die personenbezogenen Daten für Werbezwecke nicht mehr verwendet werden dürfen (Art. 21 Abs. 3 DS-GVO). Widerspricht der Adressat der Nutzung seiner Daten für Werbezwecke gegenüber dem Verein, ist dies zu respektieren. Telefonische Werbung bei Dritten ist ohne ausdrückliche Einwilligung des Betroffenen nicht zulässig, ebenso wenig in der Regel E-Mail-Werbung.

Wenn der Verein nach den genannten Grundsätzen Daten seiner Mitglieder für Werbung nutzen darf, so kann er auch eine Firma beauftragen, mit Hilfe der Daten, die ihr der Verein im Rahmen einer Auftragsdatenverarbeitung zugänglich macht, solche Werbemaßnahmen durchzuführen. Dabei ist die eingeschaltete Firma zu verpflichten, sowohl die vom Verein überlassenen, als auch die bei der Werbeaktion erhobenen Daten nicht für eigene Zwecke – insbesondere für Werbeaktionen für Dritte – zu nutzen und sämtliche Daten nach Abschluss der Aktion vollständig an den Verein abzuliefern.



8. Verarbeitung personenbezogener Daten durch den Verein, insbesondere Übermittlung an Dritte

Zur Datenübermittlung gehört jede Art von Veröffentlichung personenbezogener Angaben, z.B. in einer Tageszeitung oder im Internet. Nach Art. 6 Abs. 1 lit. b) DS-GVO können die Daten von Mitgliedern weitergegeben werden, wenn dies zur Erreichung des Vereinszwecks, insbesondere zur Verwaltung und Betreuung der Mitglieder erforderlich ist.

8.1 Datenübermittlung an Vereinsmitglieder

Bei den Vereinsmitgliedern untereinander handelt es sich um Dritte. Vereinsmitglieder dürfen also nicht einfach auf die Daten der anderen Mitglieder Zugriff nehmen, sei es, dass an sie Mitgliederlisten ausgegeben werden, sei es, dass die Personalien aller Mitglieder im Vereinsheim oder an einer anderen Stelle ausgehängt oder so in das Internet eingestellt werden, dass die anderen Mitglieder die Daten unter Verwendung eines Passworts abrufen können. Vielmehr müssen die rechtlichen Voraussetzungen für die Zulässigkeit einer Übermittlung vorliegen.
Besteht der Vereinszweck darin, die persönlichen oder geschäftlichen Kontakte zu pflegen, ist die Herausgabe einer Mitgliederliste zur Erreichung des Vereinsziels nach Art. 6 Abs. 1 lit. b) DS-GVO grundsätzlich zulässig. Dieser Vereinszweck muss sich aus der Satzung ergeben. Dies kann insbesondere bei Selbsthilfe- und Ehemaligenvereinen der Fall sein. Welche Angaben dabei in die Mitgliederliste aufgenommen werden dürfen, hängt vom jeweiligen Vereinszweck ab, wobei die Interessen und die schutzwürdigen Belange der Mitglieder angemessen zu berücksichtigen sind. Der Verein muss dabei sicherstellen, dass die Mitglieder, die ihre schutzwürdigen Interessen durch die Herausgabe der Mitgliederliste beeinträchtigt sehen, die Möglichkeit haben, der Aufnahme ihrer Daten in diese zu widersprechen. Die Daten in der Mitgliederliste sollten sich möglichst auf die zur Kontaktaufnahme notwendigen Angaben beschränken. Bei der Herausgabe der Mitgliederliste ist darauf hinzuweisen, dass diese nur für Vereinszwecke verwendet werden darf und eine Verwendung für andere Zwecke (insbesondere für kommerzielle Zwecke) sowie die Überlassung der Liste an außenstehende Dritte nicht zulässig ist. Ein solcher Hinweis soll verhindern, dass beispielsweise Vereinsmitglieder oder außenstehende Dritte die Liste für ihre beruflichen oder politischen Zwecke nutzen.
Dient die Datenübermittlung an andere Vereinsmitglieder nicht der Förderung des

Vereinszwecks, können personenbezogene Daten der Vereinsmitglieder durch den Verein an andere Vereinsmitglieder nur mit einer Einwilligung übermittelt werden.
Es darf nicht verkannt werden, dass Vereinsmitglieder sich grundsätzlich darauf verlassen dürfen, dass der Verein ihre Daten ausschließlich für die Förderung der Vereinszwecke und zu Verwaltung und Betreuung der Mitglieder nutzt. Dieser Zweck ist im Informationsblatt und im Verarbeitungsverzeichnis benannt. Daran ist der Verein gebunden. (Art. 5 Abs. 1 lit. b DS-GVO –Zweckbindung-).

8.2 Bekanntgabe zur Wahrnehmung satzungsmäßiger Mitgliederrechte

Regelungen in Vereinssatzungen sehen vielfach vor, dass beispielsweise Anträge auf Einberufung einer außerordentlichen Mitgliederversammlung oder auf Ergänzung der Tagesordnung der Mitgliederversammlung davon abhängig gemacht werden, dass eine bestimmte **Mindestzahl von Mitgliedern** die Einberufung bzw. Ergänzung verlangt. Wenn der Verein nicht generell eine Mitgliederliste oder ein Mitgliederverzeichnis herausgibt, kann es erforderlich sein, dass er Mitgliedern beispielsweise durch Einsicht in diese Unterlagen oder durch Überlassung einer Adressliste ermöglicht, eine ausreichende Anzahl anderer Mitglieder für die Unterstützung eines solchen Antrags zu erreichen.
Die Bekanntgabe von Mitgliederdaten für diesen Zweck ist wegen der Pflicht des Vereins, die Ausübung satzungsmäßiger Rechte zu ermöglichen, regelmäßig im Vereinsinteresse erforderlich, ohne dass **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person** überwiegen (Art. 6 Abs. 1 lit. f) DS-GVO). Um Missbräuchen entgegenzuwirken, empfiehlt es sich, von den Mitgliedern, denen die Adressen bekannt gegeben werden, eine Zusicherung zu verlangen, dass die Adressen nicht für andere Zwecke verwendet werden. Bei Vereinen, bei denen ein Interesse der Mitglieder besteht, dass ihre Daten vertraulich behandelt werden oder bei denen die Zugehörigkeit zum Verein ein besonders sensitives Datum darstellt (z.B. Parteien, Gewerkschaften, Selbsthilfegruppen), können jedoch **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person** dem Interesse einer Bekanntgabe ihres Namens und ihrer Anschrift überwiegen. In solchen Fällen sollte der Verein eine Regelung in der Satzung treffen oder die Mitglieder ausreichend informieren, ohne ihre Daten bekannt zu geben. Dies kann etwa dadurch geschehen, dass in einer Vereinspublikation auf den beabsichtigten Antrag, die Gründe und den Antragsteller hingewiesen und auf diese Weise interessierten Mitgliedern die Möglichkeit der Kontaktaufnahme zur Unterstützung eröffnet wird.

8.3 Mitteilungen in Aushängen und Vereinspublikationen

In vielen Vereinen ist es üblich, personenbezogene Informationen an einem „Schwarzen Brett“ oder in Vereinsblättern bekannt zu geben. Obwohl sich das „Schwarze Brett“ meist auf dem Vereinsgelände befindet und das „Vereinsnachrichtenblatt“ in erster Linie für Vereinsmitglieder bestimmt ist, handelt es sich hier um die Übermittlung dieser Angaben an einen nicht überschaubaren Kreis von Adressaten, die davon Kenntnis nehmen können, weil nie ausgeschlossen werden kann, dass auch Fremde die Anschlagtafeln auf dem Vereinsgelände oder das Mitteilungsblatt lesen. Personenbezogene Daten dürfen dabei nach Art. 6 Abs. 1 lit.b) und lit. f) DS-GVO nur offenbart werden, wenn es für die **Erreichung des Vereinszwecks** unbedingt erforderlich ist – was etwa bei Mannschaftsaufstellungen oder Spielergebnissen angenommen werden kann – oder wenn der Verein oder die Personen, die davon Kenntnis nehmen können, ein berechtigtes Interesse an der Veröffentlichung haben und **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person** nicht überwiegen. Letzteres ist stets bei Mitteilungen mit ehrenrührigem Inhalt der Fall, etwa bei Hausverboten, Vereinsstrafen und Spielersperren.

Insbesondere die Veröffentlichung von Sportgerichtsurteilen in vollem Wortlaut würde die Betroffenen unnötig an den Pranger stellen und damit deren schutzwürdige Belange beeinträchtigen. In diesen Fällen genügt es nämlich, wenn der Betroffene und die Funktionsträger des Vereins oder die von ihm Beauftragten (z.B. Schiedsrichter) davon wissen. Doch müssen letztere dabei nicht über die Höhe der verhängten Geldbuße, die Art des Verstoßes, über die Verfahrenskosten sowie über die Urteilsbegründung im Einzelnen unterrichtet werden. Soll das Urteil zur Warnung anderer Sportler oder sonstiger Mitglieder eines Vereins veröffentlicht werden, genügt hierfür eine Veröffentlichung in anonymisierter Form.

Persönliche Nachrichten mit einem Bezug zum Verein wie Eintritte, Austritte, Spenden (ohne Angabe der Höhe), Geburtstage und Jubiläen können veröffentlicht werden, wenn dem Verein keine schutzwürdigen Belange des Betroffenen bekannt sind, die dem entgegenstehen. Es empfiehlt sich, beim Eintritt in den Verein darauf aufmerksam zu machen, welche Ereignisse üblicherweise am „Schwarzen Brett“ oder im Vereinsblatt veröffentlicht werden und darum zu bitten, mitzuteilen, wenn dies nicht gewünscht wird. Informationen aus dem persönlichen Lebensbereich eines Vereinsmitglieds (z.B. Eheschließungen, Geburt von Kindern, Abschluss von Schul- und Berufsausbildungen) dürfen nur veröffentlicht werden, wenn das Mitglieder ausdrücklich seine Einwilligung erklärt hat. Vergleichbares gilt für die Bekanntgabe der Höhe der Spende eines Vereinsmitgliedes. Spender und Sponsoren außerhalb des Vereins dürfen nur mit ihrem Einverständnis öffentlich bekannt gegeben werden, da ihr Interesse an vertraulicher Behandlung grundsätzlich überwiegt.

Die „dienstlichen“ **Erreichbarkeitsdaten von Funktionsträgern** des Vereins, insbesondere der Vorstände, können in der Regel in der genannten Form bekannt gegeben werden. Dagegen dürfen Mitgliederlisten für gewöhnlich nur am „Schwarzen Brett“ ausgehängt oder im Vereinsblatt veröffentlicht werden, wenn die Betroffenen insoweit eingewilligt haben.

8.4 Datenübermittlung an Dachverbände und andere Vereine

Dachverbände, bei denen ein Verein Mitglied ist, sind im Verhältnis zu seinen Mitgliedern datenschutzrechtlich Dritte. Personenbezogene Daten der eigenen Mitglieder dürfen an andere Vereine im Rahmen der Erforderlichkeit nur übermittelt werden, soweit diese dort benötigt werden, um die Vereinsziele des übermittelnden Vereins oder um die Ziele des anderen Vereins zu verwirklichen, etwa bei der überregionalen Organisation eines Turniers, und sofern keine **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person** überwiegen (Art. 6 Abs. 1 lit. b) und lit f) DS-GVO).
Ist ein Verein **verpflichtet**, die Daten seiner Mitglieder regelmäßig einer Dachorganisation – beispielsweise einem Bundes- oder Landesverband – zu übermitteln (etwa in Form von Mitgliederlisten), sollte dies in der **Vereinssatzung geregelt** werden.
Dadurch wird klargestellt, dass die Übermittlung im Vereinsinteresse erforderlich ist und keine Interessen oder Grundrechte und Grundfreiheiten der Vereinsmitglieder überwiegen (Art. 6 Abs. 1 lit. f) DS-GVO) und die Daten auch zu diesem Zweck erhoben werden. Fehlt eine Satzungsregelung, sollten die Mitglieder (Neumitglieder möglichst bereits im Aufnahmeverfahren) über die Übermittlung ihrer Daten an die Dachorganisation und den Übermittlungszweck informiert und ihnen Gelegenheit zu Einwendungen gegeben werden. Der Verein ist darüber hinaus verpflichtet, dafür Sorge zu tragen, dass die von ihm weitergegebenen Mitgliederdaten **vom Dritten nicht zweckentfremdet genutzt** werden (etwa durch Verkauf der Mitgliederadressen für Werbezwecke) oder dies allenfalls mit Einverständnis des Vereins und Einwilligung der betroffenen Mitglieder geschieht.
Sollen Mitgliederlisten oder im Einzelfall sonstige Mitgliederdaten auf **freiwilliger Basis** ohne vertragliche oder sonstige Verpflichtung an Dachverbände oder andere Vereine weitergegeben werden, ist dies nur unter den oben genannten Voraussetzungen zulässig. Soweit die Weitergabe im berechtigten Interesse des Vereins oder des Empfängers erfolgen soll, empfiehlt es sich in Zweifelsfällen, die Mitglieder vor der beabsichtigten Datenübermittlung zu informieren und ihnen die Möglichkeit zu geben, Einwendungen gegen die Weitergabe ihrer Daten geltend zu machen.
Bietet der Dachverband eine **Versicherung** für die Mitglieder eines Vereins an, die z.B. in erster Linie dem Verein dient, um sich gegen Haftungsansprüche seiner Mit-

glieder zu schützen, wenn diese beim Sport oder bei vergleichbar gefahrgeneigten Tätigkeiten verunglücken, hat der Verein zwar ein berechtigtes Interesse, die für die Begründung des Versicherungsverhältnisses erforderlichen Daten seiner Mitglieder dem Dachverband zuzuleiten., es ist jedoch damit zu rechnen, dass schutzwürdige Interessen der Mitglieder darauf überwiegen, dass eine Weitergabe unterbleibt. Hier ist – gerade mit Blick auf oft „offensive" Versicherungsmarketing-Praktiken – Sensibilität geboten. Im Zweifel sollten Vereinsmitglieder vom Verein über die Möglichkeit (und die Vorteile) des Abschlusses bei gerade dieser Versicherung informiert werden. Sie können dann selbst entscheiden, ob sie sich dort (oder anderswo) versichern lassen (s. auch Nr. 8.5).
Will aber der Dachverband erreichen, dass sich die Vereinsmitglieder in eigenem Interesse bei ihm oder bei einer von ihm vermittelten Versicherung versichern können, darf der Verein deren Daten nur mit ihrer Einwilligung an den Dachverband übermitteln.
Andererseits ist es zulässig, dass ein Verein, der eine bestimmte Anzahl **Delegierter** zur Delegiertenversammlung des Dachverbandes entsenden darf, dem Dachverband eine Namensliste seiner Mitglieder übermittelt, soweit dies erforderlich ist, um feststellen zu können, ob die entsandten Delegierten auch Mitglieder eines Vereins sind, der Delegierte entsenden darf. Es muss stets durch entsprechende Vereinbarungen mit dem Dachverband sichergestellt sein, dass die ihm zugänglich gemachten Daten dort für keinen anderen Zweck genutzt werden, also nicht etwa für Werbemaßnahmen des Dachverbandes oder gar Dritter.

8.5 Datenübermittlung an Sponsoren und Firmen zu Werbezwecken (insbesondere Versicherungen)

Nicht selten verlangen **Sponsoren** als Gegenleistung für ihre Unterstützung die Bekanntgabe von Mitgliederdaten, die dann zu Werbezwecken eingesetzt werden. Aber auch für manche **Wirtschaftsunternehmen** sind die Daten von Vereinsmitgliedern für Werbezwecke interessant. Die Bekanntgabe von Mitgliederdaten für Werbezwecke ist aber in der Regel vom Vereinszweck nicht gedeckt. Sofern also die Bekanntgabe von Mitgliederdaten an Sponsoren und Wirtschaftsunternehmen für Werbezwecke weder in der Satzung noch durch Mitgliederbeschluss festgelegt ist, sollten die Vereine bei der Übermittlung von Mitgliederdaten an Sponsoren und Wirtschaftsunternehmen zu Werbezwecken grundsätzlich eine Einwilligung einholen.
Der Verein darf personenbezogene Daten der Mitglieder für Werbezwecke daher nur übermitteln, wenn diese entweder darin **eingewilligt** haben oder die Daten schon von Anfang an auch zu Werbezwecken erhoben worden sind (Infoblatt!), der Verein oder ein Dritter **berechtigte Interessen** an der Nutzung zu Werbezwecken hat und keine Interessen oder Grundrechte und Grundfreiheiten der Mitglieder überwiegen.

Entscheidend sind auch hier die vernünftigen Erwartungen der betroffenen Person. Informiert der Verein transparent und umfassend über eine entsprechende werbliche Nutzung, geht die Erwartung der betroffenen Person in aller Regel auch dahin, dass ihre Daten entsprechend genutzt werden.

Zu beachten ist auch hier, dass das Mitglied ein **jederzeitiges Widerspruchsrecht** hat, auf das der Verein ausdrücklich **hinweisen** muss. Dies kann beispielsweise dadurch geschehen, dass in den Aufnahmeantrag oder in die Satzung ein entsprechender Hinweis aufgenommen wird. Es ist darüber hinaus empfehlenswert, im Rahmen der Jahreshauptversammlung nochmals auf das Widerspruchsrecht hinzuweisen. Erfolgt ein solcher Widerspruch, hat dies zur Folge, dass die personenbezogenen Daten für Werbezwecke nicht mehr verwendet werden dürfen (Art. 21 Abs. 3 DS-GVO). Die Namen der Vereinsmitglieder, die der Übermittlung ihrer Daten für Werbezwecke widersprochen haben, sind in eine separate sogenannte Sperrdatei aufzunehmen. Vor jeder Übermittlung der Mitgliederdaten an Sponsoren und Wirtschaftsunternehmen zu Werbezwecken ist dann ein Abgleich mit der Sperrdatei durchzuführen.

Bei der Weitergabe der Mitgliederdaten muss auch der Umstand berücksichtigt werden, dass der Datenempfänger diese Daten wiederum für Werbezwecke anderer Unternehmen weitergeben oder nutzen kann. Deshalb sollte die Verwendung der weitergegebenen Daten unbedingt auf den konkreten Werbezweck des Datenempfängers beschränkt und eine Nutzung oder Übermittlung der Daten für fremde Werbezwecke vertraglich ausgeschlossen werden. Daten von Mitgliedern, bei denen ein entgegenstehendes Interesse erkennbar ist, dürfen auf keinen Fall weitergegeben werden.

In der Praxis ergeben sich bei Vereinen häufig Probleme mit der Weitergabe von Mitgliederdaten an Versicherungsunternehmen oder Versicherungsvertreter im Rahmen von **Gruppenversicherungsverträgen**. Dabei handelt es sich um Rahmenverträge zwischen Vereinen und Versicherungsunternehmen, die den Vereinsmitgliedern unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen.

Die Datenschutzaufsichtsbehörden vertreten hierzu inzwischen die Auffassung, dass ein Verein im Rahmen eines Gruppenversicherungsvertrags dem Versicherungsunternehmen bzw. dem Versicherungsvertreter die Daten seiner Mitglieder nur übermitteln darf, wenn das betreffende Mitglied eine ausdrückliche und informierte **schriftliche Einwilligung** erteilt hat. Dies gilt für **Neu-** und für **Altmitglieder**, die bei Abschluss des Gruppenversicherungsvertrags bereits Vereinsmitglieder waren, gleichermaßen. Die Einwilligungserklärung sollte zweckmäßigerweise bereits in der Beitrittserklärung oder im Aufnahmeantrag vorgesehen werden, wobei das Mitglied darüber aufzuklären ist, welche Daten an welches Unternehmen weitergegeben werden sollen.

Einzelne Versicherungen haben für Vereine eine „Stellungnahme zur Zulässigkeit von Datenübermittlungen“ oder ähnlich betiteltes Papier erarbeitet, in dem geringere Anforderungen an den Datenschutz genannt werden. Vereine sollten sich hiervon nicht irritieren lassen und der Rechtsauffassung der Datenschutzaufsichtsbehörden folgen. Dies empfiehlt sich auch im Hinblick auf die künftig im Raum stehenden Bußgelder.

Besondere Kategorien personenbezogener Daten (Gesundheitsdaten) dürfen zu Werbezwecken grundsätzlich nur mit einer ausdrücklichen Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO verarbeitet werden. Die Verarbeitung dieser Daten auf Grundlage eines berechtigten Interesses nach Art. 6 Abs. 1 lit. f DS-GVO ist STETS unzulässig (Art. 9 Abs. 1 DS-GVO).

8.6 Veröffentlichungen im Internet

Das **Internet** bietet für Vereine und Verbände große Chancen zur Selbstdarstellung, birgt aber auch Risiken für die betroffenen Vereinsmitglieder. Die Veröffentlichung von personenbezogenen Daten im Internet ohne Passwortschutz stellt datenschutzrechtlich eine Übermittlung dieser Daten an Jedermann dar. Sie ist nicht zuletzt wegen der weltweiten Verbreitung der Informationen, weil dieses Medium nichts mehr vergisst, wegen der elektronischen Recherchierbarkeit und weil die Möglichkeit der Auswertung von Internetinformationen für Zwecke der Profilbildung und Werbung besteht, grundsätzlich nicht unproblematisch. So besitzt die Information, dass jemand z.B. eine bestimmte Sportart ausübt, einer bestimmten Altersgruppe zuzurechnen ist oder ein unfallträchtiges Hobby hat, u.U. auch für andere Stellen Relevanz (Arbeitgeber, Werbeindustrie). Auch können diese Daten in Staaten abgerufen werden, die keine der DS-GVO vergleichbare Schutzbestimmungen kennen. Ferner ist die Authentizität der Daten nicht garantiert, da diese einfach verfälscht werden können. Deswegen ist die **Veröffentlichung** personenbezogener Daten durch einen Verein im **Internet** grundsätzlich **unzulässig**, wenn sich der Betroffene nicht **ausdrücklich** damit **einverstanden** erklärt hat.
Allerdings gibt es auch hier Ausnahmen. So dürfen die **Funktionsträger** eines Vereins auch ohne ausdrückliche Einwilligung mit ihrer „dienstlichen“ Erreichbarkeit in das Internet auf der Homepage des Vereins eingestellt werden. Die private Adresse des Funktionsträgers darf allerdings nur mit seinem Einverständnis veröffentlicht werden. Informationen über **Vereinsmitglieder** (z.B. Spielergebnisse und persönliche Leistungen, Mannschaftsaufstellungen, Ranglisten, Torschützen usw.) oder Dritte (z.B. Spielergebnisse externer Teilnehmer an einem Wettkampf) können ausnahmsweise auch ohne Einwilligung kurzzeitig ins Internet eingestellt werden, wenn die Betroffenen darüber **informiert** sind und keine schutzwürdigen Interessen oder Grundrechte und Grundfreiheiten der Veröffentlichung im Einzelfall überwiegen. Rechtsgrundlage hierfür ist Art. 6 Abs. 1 lit. f) DS-GVO. Die zulässige Dauer der Veröffentlichung hängt von der Bedeutung des Ereignisses, auf das sich die Veröffentlichung bezieht, und dem daraus abzuleitenden Informationsinteresse der Öffentlichkeit ab.
Die von einem Verein oder Verband ausgerichteten Veranstaltungen (z. B. Spiele in der Bezirksklasse) sind öffentlich. Die Namen und die Ergebnisse werden im Rahmen solcher Veranstaltungen üblicherweise öffentlich bekannt gegeben. Die in Ranglisten

enthaltenen Daten sind zwar nicht allgemein zugänglich, stammen jedoch aus allgemein zugänglichen Quellen und stellen nur eine Zusammenfassung und Auswertung dieser Daten dar.
Um den Eingriff in das Persönlichkeitsrecht in Grenzen zu halten, dürfen bei derartigen Veröffentlichungen jedoch allenfalls **Nachname, Vorname, Vereinszugehörigkeit** und eventuell in begründeten Ausnahmefällen der **Geburtsjahrgang** aufgeführt werden Bei einer Veröffentlichung eines Fotos, des vollen Geburtsdatums (Tag, Monat und Jahr), der privaten Anschrift oder der Bankverbindung des Betroffenen überwiegen dessen Interessen; sie wäre daher nur mit ausdrücklicher Einwilligung des Betroffenen zulässig. Im Übrigen muss – wie oben aufgeführt – sichergestellt sein, dass die Daten nach angemessener Zeit gelöscht werden.

8.7 Veröffentlichungen im Intranet

Wenn ein Verein seinen Mitgliedern und Funktionsträgern Informationen über das Internet in **passwortgeschützten Bereichen** (Intranet) zur Verfügung stellt, können über die Vergabe von Benutzerkennungen und Passwörtern **individuelle Zugriffsberechtigungen** eingerichtet werden. Dies hat den Vorteil, dass beliebige Dritte die Daten nicht einsehen können, berechtigte Nutzer jedoch jederzeit über das Internet auf diejenigen personenbezogenen Daten zugreifen können, die sie zur Wahrnehmung ihrer Rechte und Pflichten als Mitglied oder Funktionsträger des Vereins benötigen.

8.8 Personenbezogene Auskünfte an die Presse und sonstige Massenmedien

Veröffentlichungen in Verbandszeitschriften und in sonstigen allgemein zugänglichen Publikationen dürfen genauso wie Pressemitteilungen und -auskünfte nur in personenbezogener Form erfolgen, wenn es sich um ein Ereignis von öffentlichem Interesse handelt. Dabei ist darauf zu achten, dass die schutzwürdigen Belange der betroffenen Vereinsmitglieder gewahrt werden. Ausschlaggebend ist, ob die Veranstaltung, über die berichtet werden soll, öffentlich ist oder war, was der Betroffene gegenüber der Presse selbst erklärt hat und was die Presse ihrerseits in Erfahrung bringen konnte. Personenbezogene Daten können dabei u.U. offenbart werden, wenn es um besondere Leistungen eines Mitglieds geht oder wenn der Verein wegen des Ausschlusses eines Mitglieds in der Öffentlichkeit ins Gerede gekommen ist und eine Information im Interesse des Vereins oder der Öffentlichkeit erforderlich erscheint. Stets darf der Verein dabei nur die unbedingt notwendigen persönlichen Angaben offenbaren.

Auskünfte zum privaten, nicht vereinsbezogenen Bereich eines Vereinsmitglieds sollten ohne Einwilligung grundsätzlich nicht erfolgen. Hier überwiegt das schutzwürdige Interesse des Betroffenen stets das Informationsinteresse der Allgemeinheit.

8.9 Übermittlung für Zwecke der Wahlwerbung

Die Übermittlung von Mitgliederdaten an politische Parteien bzw. Gruppierungen oder an Kandidaten bei Wahlen für Zwecke der Wahlwerbung ist ohne schriftliche Einwilligung der Betroffenen unzulässig. Mitglieder des Vereinsvorstands, andere Personen, die im Verein eine Funktion haben, oder Vereinsmitglieder dürfen für Zwecke der eigenen Wahlwerbung nicht auf personenbezogene Daten der Mitglieder des Vereins zurückgreifen. Diese Daten wurden für die Verfolgung des Vereinszwecks (der Vereinszwecke) erhoben und gespeichert. Eine Nutzung für jede Art von Wahlwerbung verletzt schutzwürdige Belange der Mitglieder, ist eine Zweckänderung und ist deswegen unzulässig.

8.10 Übermittlung von Mitgliederdaten an die Gemeindeverwaltung

Verlangt eine Gemeindeverwaltung, die an einen Verein freiwillige finanzielle Leistungen erbringt, deren Höhe von der Mitgliederzahl oder der Anzahl bestimmter Mitglieder (etwa der Anzahl der Jugendlichen, die in Mannschaften mitspielen) abhängt, zu Kontrollzwecken die Vorlage von Listen mit den Namen der Betroffenen, ist der Verein grundsätzlich berechtigt, diese Daten zu übermitteln, weil es sowohl zur Wahrnehmung berechtigter eigener Interessen – nämlich um in den Genuss der Vereinsförderung durch die Gemeinde zu kommen – als auch zur Wahrnehmung berechtigter Interessen eines Dritten, der Gemeinde, erforderlich ist, soweit Interessen oder Grundrechte der betroffenen Vereinsmitglieder einer Datenübermittlung nach Art. 6 Abs. 1 lit. f) DS-GVO nicht überwiegen. Die Gemeinde darf diese Daten nur verwenden, um nachzuprüfen, ob die ihr vom Verein übermittelten Zahlen zutreffend sind und muss die Daten danach umgehend löschen.
Dieser Zweck muss aber von Anfang an transparent gemacht werden. Eine spätere Entscheidung, Bestandsdaten zu diesem Zweck zu verwenden, ist eine Zweckänderung. Hier sollte vorsorglich eine Einwilligung eingeholt und über den neuen Zweck informiert werden. Datenübermittlung an den Arbeitgeber eines Mitglieds und an die Versicherung
Krankenversicherungen sind grundsätzlich berechtigt zu erfahren, gegen wen und in welchem Umfang ihnen ein Regressanspruch wegen der Verletzung einer Person,

an die sie deswegen Leistungen erbracht haben, durch ein Vereinsmitglied zusteht. Für die gesetzlichen Krankenversicherungen ergibt sich dies aus § 67a des Zehnten Buchs des Sozialgesetzbuchs, für die privaten Krankenversicherer aus Art. 6 Abs. 1 lit. b) DS-GVO wegen des Versicherungsvertrags zwischen dem Geschädigten und seiner Versicherung. Der Verein darf diese Anfragen grundsätzlich nach Art. 6 Abs. 1 lit f) DS-GVO i.V.m. § 24 Abs. 1 Nr. 2 BDSG beantworten, wenn nicht die Interessen der betroffenen Person an dem Ausschluss überwiegen. Dabei wird es allerdings genügen, der Versicherung nur den Namen des Schädigers mitzuteilen, damit sie sich an diesen wenden kann. Sollte dies nicht ausreichen, können auch weitere Angaben, etwa über den Spielverlauf, erfolgen. Weil der Verein auch hier die schutzwürdigen Belange des Betroffenen angemessen berücksichtigen muss, ist dieser vor der Übermittlung der Daten i.d.R. anzuhören.

9. Recht auf Löschung und Einschränkung personenbezogener Daten

Das Recht auf Löschung richtet sich nach Art. 17 Abs. 1 DS-GVO. Danach sind personenbezogene Daten unverzüglich zu löschen, sofern sie für die **Zwecke**, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, die betroffene Person ihre **Einwilligung widerruft** oder **Widerspruch** gegen die Verarbeitung einlegt, die personenbezogenen Daten **unrechtmäßig verarbeitet** wurden oder wenn die Löschung zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich ist.
Bezüglich des Zwecks muss der Verein daher festlegen, welche Arten von Daten bis zu welchem Ereignis (z.B. Austritt aus dem Verein, Tod) oder für welche Dauer verarbeitet werden. Mit Erreichen des festgelegten Zeitpunkts muss eine Einschränkung der Verarbeitung erfolgen, sofern die betroffene Person sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt und eine Einschränkung verlangt (Art. 18 Abs. 1 lit c) DS-GVO; sog. Protokolldatei). Ansonsten sind sie mit Zweckerreichung zu löschen. Die Länge der Einschränkung der Verarbeitung orientiert sich grundsätzlich daran, wie lange mit Rückfragen des Betroffenen, mit Gerichtsverfahren oder mit sonstigen Vorgängen zu rechnen ist, die die Kenntnis des Datums noch erforderlich machen. Auch die Länge der Dokumentationsfristen sollte für jede Datenart vorgegeben werden. Eingeschränkte Daten dürfen ohne Einwilligung des Betroffenen nur noch verarbeitet werden, wenn Rechtsansprüche durch den Verantwortlichen geltend gemacht, ausgeübt oder verteidigt werden, wenn Rechte einer anderen natürlichen oder juristischen Person geschützt werden sollen oder wenn dies aus Gründen eines wichtigen öffentlichen Interesses der Union oder des Mitgliedsstaates geschieht (Art. 18 Abs. 2 DS-GVO).
Der Verein hat die Möglichkeit, ein Vereinsarchiv zu führen und dort auch Vorgänge mit personenbezogenen Daten, die für eine aktive Nutzung nicht mehr benötigt werden, aufzubewahren. Dabei sollte jedoch sichergestellt sein, dass nur ein sehr kleiner zuverlässiger Personenkreis dazu Zugang hat. Die Nutzung des Archivguts in personenbezogener Form ist nur sehr eingeschränkt zulässig. Die Einzelheiten sollten ebenfalls geregelt werden. Wichtig ist auch, dass der Verein Unterlagen, die nicht mehr benötigt werden, so entsorgt, dass Dritte keine Kenntnis von den darin enthaltenen personenbezogenen Daten erlangen können. Insbesondere dürfen Mitglieder- und Spenderlisten nicht einfach in Müllcontainer geworfen werden. Hierfür gibt es spezielle Datenschutztonnen, die insbesondere bei besonders schutzwürdigen Daten genutzt werden sollten (Gesundheitsdaten). Diese Tonnen werden von zertifizierten Entsorgern geleert. Aber auch weniger schutzbedürftigen Daten sind zumindest zu schreddern, bevor sie in normalen Papiercontainern entsorgt werden.
Beim **Ausscheiden** oder dem **Wechsel von Funktionsträgern** ist sicherzustellen, dass

sämtliche Mitgliederdaten entweder ordnungsgemäß gelöscht oder an den Nachfolger oder einen anderen Funktionsträger des Vereins übergeben werden und keine Kopien und Dateien mit Mitgliederdaten beim bisherigen Funktionsträger verbleiben. Auch hierzu sollte der Verein Regelungen treffen.
Die erforderlichen Regelungen zu Speicherfristen sowie zur Sperrung und Löschung von Daten und ggfs. zur Nutzung von Archivgut können entweder in der **Vereinssatzung** oder außerhalb der Satzung in einer **Datenschutzordnung** bzw. in einer gesonderten **Datenlöschkonzeption** getroffen werden.
WEITERE INFORMATIONEN zu diesem Thema finden Sie in Kurzpapier Nr. 11 der Datenschutzkonferenz „Recht auf Löschung / Recht auf Vergessenwerden", abrufbar unter www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Kurzpapiere/Kurzpapier_Nr_11.pdf

10. Technische und organisatorische Maßnahmen

Die DS-GVO fordert geeignete technische und organisatorische Maßnahmen, um die Risiken für die Rechte und Freiheiten natürlicher Personen ausreichend zu mindern. Das betrifft sowohl Maßnahmen zur Gewährleistung der Rechte Betroffener (Kapitel III DS-GVO), als auch Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 DS-GVO).
Herauszufinden, welche technischen und organisatorischen Maßnahmen tatsächlich erforderlich sind, ist ohne eine entsprechende Systematik kaum möglich. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat das Standard-Datenschutzmodell (SDM) verabschiedet (www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V_1_1.pdf), dessen Methodik in vereinfachter Form auch für Vereine geeignet ist, um die rechtlichen Anforderungen der DS-GVO in technische und organisatorische Maßnahmen zu überführen.
Die Methodik des SDM systematisiert technische und organisatorische Maßnahmen auf der Basis der Gewährleistungsziele Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung (als technische Sicherung der Zweckbindung) und Intervenierbarkeit (als technische Gestaltung von Verfahren zur Ausübung von Betroffenenrechten). Auf diese Weise unterstützt das SDM die Auswahl geeigneter Maßnahmen.

10.1 Gewährleistungsziele

DER BEGRIFF „GEWÄHRLEISTUNGSZIEL“

Das SDM verwendet für die Beschreibung von bestimmten aus dem Datenschutzrecht resultierenden Anforderungen den Begriff „Gewährleistungsziel“. Diese Anforderungen zielen auf Eigenschaften einer rechtskonformen Verarbeitung, die durch technische und organisatorische Maßnahmen „gewährleistet“ werden müssen.
Die folgenden datenschutzrechtlichen Anforderungen, die sowohl übergreifend in der DS-GVO als auch in allen deutschen Datenschutzgesetzen enthalten sind und deren Erfüllung Voraussetzung für die Rechtmäßigkeit einer personenbezogenen Datenverarbeitung bilden, werden vom Konzept der Gewährleistungsziele erfasst:

- die Zweckbindung einer Datenverarbeitung mit Personenbezug,
- die Begrenzung der Datenverarbeitung auf das erforderliche Maß (Datenminimierung),
- die Berücksichtigung der Betroffenenrechte, wonach bei einer Verarbeitung personenbezogener Daten Abläufe (Prozesse) vorzusehen sind, um insbesondere

Betroffene informieren, die erforderlichen Auskünfte erteilen und Daten berichtigen und löschen zu können,
- die Transparenz von Verarbeitungstätigkeiten als Voraussetzung dafür, dass die rechtlich festgelegten Anforderungen an eine Verarbeitung nachvollziehbar sind, und zwar sowohl für den Vereinsvorstand, als auch für die Beschäftigten des Vereins und die Vereinsmitglieder sowie für die Aufsichtsbehörden überprüfbar sind,
- die Sicherheit der Verarbeitung der vom Verein eingesetzten Datenverarbeitungssysteme in Bezug auf die Rechte und Freiheiten natürlicher Personen (Art. 32 Abs. 1 DS-GVO).

MASSNAHMEN NACH GEWÄHRLEISTUNGSZIELEN SYSTEMATISIERT

In diesem Abschnitt werden Datenschutzmaßnahmen aufgeführt, die in der Datenschutzprüfpraxis vieler Datenschutzaufsichtsbehörden seit vielen Jahren erprobt sind. Diese Maßnahmen sind jeweils den Gewährleistungszielen des SDM zugeordnet. Einige Maßnahmen werden dabei bewusst mehrfach aufgeführt, weil sie der Umsetzung mehrerer Gewährleistungsziele dienen.

(1) Das Gewährleistungsziel *Datenminimierung* (Art. 5 Abs. 1 lit. c DS-GVO) hat zum Ziel, die Verarbeitung hinsichtlich der verarbeiteten Informationen und der Zahl der an der Verarbeitung beteiligten Personen zu minimieren.

Das Gewährleistungsziel Datenminimierung kann erreicht werden, indem insbesondere
- nur die Daten erhoben werden, die tatsächlich erforderlich sind,
- nur die Personen Zugriff zu vorhandenen Daten haben, die diese Daten für die Erfüllung ihrer Aufgaben im Verein wirklich benötigen,
- nur Programme installiert und Funktionen freigeschaltet werden, die zur Erfüllung der Aufgaben im Verein erforderlich sind,
- klar geregelt wird, wer Zugang zu welchen Daten haben darf (Berechtigungskonzept),
- nicht mehr erforderliche Daten zum frühestmöglichen Zeitpunkt (möglichst automatisch) gelöscht oder anonymisiert werden (siehe dazu auch Punkt 5 Erhebung personenbezogener Daten)

(2) Das Gewährleistungsziel *Verfügbarkeit* (Art. 32 Abs. 1 lit. b und c und Art. 5 Abs. 1 lit. e DS-GVO) bezeichnet die Anforderung, dass personenbezogene Daten zur Verfügung stehen müssen und ordnungsgemäß für die vorgesehene Verarbeitung verwendet werden können.

Typische Maßnahmen zur Gewährleistung der Verfügbarkeit sind:
- Anfertigung von Sicherheitskopien von Daten und Konfigurationen nach einem definierten Zeitplan,
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt),
- Redundanz von Hard- und Software sowie Infrastruktur (bspw. Ersatzserver, Ersatzrouter)
- Klärung von Reparaturstrategien und Ausweichprozessen bei defekter Technik,

- Dokumentation der Installation von Hard- und Software, um bei Ausfällen oder planmäßigem Austausch Ersatztechnik in Betrieb nehmen zu können,
- Vertretungsregelungen für abwesende Mitarbeitende.

(3) Das Gewährleistungsziel *Integrität* (Art. 32 Abs. 1 lit. b und Art. 5 Abs. 1 lit. f DS-GVO) bezeichnet die Eigenschaft, dass die zu verarbeitenden Daten unversehrt, vollständig und aktuell bleiben.

Typische Maßnahmen zur Gewährleistung der Integrität bzw. zur Feststellung von Integritätsverletzungen sind:

- Festlegung bzw. Einschränkung von Schreib- und Änderungsrechten an Daten und Software,
- dokumentierte Zuweisung von Berechtigungen und Rollen,
- Einsatz von Prüfsummen, elektronische Siegeln und Signaturen,
- regelmäßige Prüfung der Aktualität von Daten,
- stichprobenartige Kontrolle der ordnungsgemäßen Funktionalität von Hard- und Software,

(4) Das Gewährleistungsziel *Vertraulichkeit* (Art. 5 Abs. 1 lit. f und Art. 32 Abs. 1 lit. b DS-GVO) bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen kann.

Typische Maßnahmen zur Gewährleistung der Vertraulichkeit sind:

- Festlegung eines Rechte- und Rollen-Konzeptes nach dem Erforderlichkeitsprinzip,
- Implementierung eines hinreichend sicheren Authentisierungsverfahrens, beispielsweise Passwortschutz oder kombinierte Verfahren aus Passwort und einem Generator für Einmal-PINs oder Einmal-Passwörter,
- Eingrenzung des Zugriffs auf personenbezogene Daten auf solche Vereinsmitglieder, die jeweils zuständig, fachlich befähigt, zuverlässig und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen,
- Festlegung und Kontrolle der Nutzung zugelassener Ressourcen und Kommunikationskanäle,
- Unterbringung der Informationstechnik in für die Verarbeitungstätigkeit angemessen ausgestatteten Gebäuden und Räumen,
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen etc.),
- Verschlüsselung von gespeicherten oder transferierten Daten,
- Schutz vor äußeren Einflüssen (Spionage, Hacking) bspw. durch Einsatz von Firewalls.

(5) Das Gewährleistungsziel *Nichtverkettung* (Art. 5 Abs. 1 lit. b und c DS-GVO) bezeichnet die Anforderung, dass personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht unbefugt zusammengeführt, also „verkettet“ werden dürfen. Es dient der technischen Umsetzung des o. g. Zweckbindungsgrundsatzes.

Typische Maßnahmen zur Gewährleistung der Nichtverkettung sind:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten,
- Schließung/Sperrung von nicht benötigten Schnittstellen bei Verarbeitungsverfahren und Komponenten,
- Trennung nach den im Verein ausgeübten Aufgaben, bei größeren Vereinen auch nach Organisations-/Abteilungsgrenzen,
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten,
- abschließende Weisungen gegenüber Auftragsverarbeitern (siehe dazu auch Teil II / Kapitel 6)

(6) Das Gewährleistungsziel *Transparenz* (Art. 5 Abs. 1 lit. a DS-GVO) bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme besitzt.Typische Maßnahmen zur Gewährleistung der Transparenz sind:

- Dokumentation von Verarbeitungstätigkeiten insbesondere mit den Bestandteilen Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Beschreibungen von Verarbeitungstätigkeiten, Zusammenspiel mit anderen Verarbeitungstätigkeiten (siehe dazu auch TEIL I/Kapitel 1.5),
- Dokumentation von Tests, der Freigabe und ggf. der Datenschutzfolgenabschätzung von neuen oder geänderten Verarbeitungstätigkeiten (siehe dazu auch TEIL II/Kapitel 10.2 und 10.3),
- Dokumentation der Verträge mit den internen Mitarbeitenden, mit externen Dienstleistern und mit Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen (siehe dazu TEIL II /Kapitel 5 und 6
- Dokumentation von Einwilligungen und Widersprüchen
- Protokollierung von Zugriffen und Änderungen,
- Dokumentation der Verarbeitungsprozesse mittels Protokollen und regelmäßige Auswertung dieser Protokolle,

(7) Das Gewährleistungsziel *Intervenierbarkeit* bezeichnet die Anforderung, dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung, Löschung und Datenportabilität (Art. 16, 17, 18 und 20 DS-GVO) jederzeit wirksam gewährt und der für die Verarbeitung Verantwortliche (hier: der Verein) verpflichtet ist, die entsprechenden Maßnahmen umzusetzen.
Typische Maßnahmen zur Gewährleistung der Intervenierbarkeit sind:

- detaillierte Information der von der Verarbeitung Betroffenen (siehe auch TEIL I/ Kapitel 1.3)
- differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten (siehe auch TEIL I/Kapitel 3)),
- Benennung eines Ansprechpartners (ggf. eines Datenschutzbeauftragten – siehe

dazu TEIL I/Kapitel 1.4 sowie TEIL II/Kapitel 10.4) zur Erleichterung der Durchsetzung von Betroffenenrechten,

- Schaffung von Abläufen und technischen Voraussetzungen, um alle zu einer Person gespeicherten Daten berichtigen, sperren, löschen und zur Auskunft zusammenstellen zu können.
- Dokumentation der Behebung von Störungen an Systemen und von Änderungen an Systemen und Abläufen zur Verarbeitung personenbezogener Daten sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes,
- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem,
- Nachverfolgbarkeit der Verarbeitungsvorgänge zur Gewährung der Betroffenenrechte

10.2 Benennung eines Datenschutzbeauftragten

Der Verein hat einen Datenschutzbeauftragen zu benennen, wenn dessen **Kerntätigkeit** in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische **Überwachung der betroffenen Person** erforderlich macht (z.B. Videoüberwachung im Stadion) oder die Kerntätigkeit in der **Verarbeitung besonderer Kategorien von Daten** gemäß Art. 9 DS-GVO (z.B. Gesundheitsdaten in Selbsthilfegruppen) oder von **personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten** gemäß Art. 10 DS-GVO besteht (Art. 37 Abs. 1 lit. b) und lit c) DS-GVO). Die Verarbeitung personenbezogener Daten als primärer Geschäftszweck dürfte jedoch bei Vereinen in der Regel nicht der Fall sein.
Darüber hinaus ist ein Datenschutzbeauftragter zu benennen, wenn **mindestens 10 Personen ständig** mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Nimmt der Verein Verarbeitungen vor, die einer **Datenschutzfolgeabschätzung** gemäß Art. 35 DS-GVO (s.u. Nr. 7.2) unterliegen, so ist ebenfalls ein Datenschutzbeauftragter zu benennen (§ 38 Abs. 1 BDSG-neu).
Der Datenschutzbeauftragte benötigt Kenntnisse zum Datenschutz und ist verpflichtet, sich weiter zu bilden.
Zur Vermeidung einer Interessenkollision dürfen die Aufgaben des Datenschutzbeauftragten nicht vom Vereinsvorstand oder dem für die Datenverarbeitung des Vereins Verantwortlichen wahrgenommen werden, da diese Personen sich nicht selbst wirksam überwachen können. Der Datenschutzbeauftragte muss nicht Mitglied des Vereins sein (Art. 37 Abs. 6 DS-GVO).
Die **Aufgaben** des Datenschutzbeauftragten sind in Art. 39 DS-GVO geregelt. Insbesondere obliegt dem Datenschutzbeauftragten die Pflicht, den Verein bzw. die dort mit der Verarbeitung personenbezogener Daten Beschäftigten hinsichtlich ihrer

datenschutzrechtlichen Pflichten zu **unterrichten** und zu **beraten**. Zudem wirkt er auf die **Überwachung** und **Einhaltung** datenschutzrechtlicher Vorschriften hin. Er hat insbesondere die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen. Zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten.
Der Verein hat die **Kontaktdaten** des Datenschutzbeauftragten zu **veröffentlichen** und die Daten der zuständigen **Aufsichtsbehörde mitzuteilen**. Für die Veröffentlichung der Kontaktdaten ist es ausreichend, wenn die E-Mail-Adresse des Datenschutzbeauftragten auf der Vereinshomepage frei zugänglich genannt wird.
Besteht keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten, muss sich der Vereinsvorstand selbst um die Einhaltung des Datenschutzes durch den Verein kümmern. Er kann auch auf freiwilliger Basis einen Datenschutzbeauftragten bestellen.
WEITERE INFORMATIONEN finden Sie in Kurzpapier Nr. 12 der Datenschutzkonferenz „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“, abrufbar unter www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Kurzpapiere/Kurzpapier_Nr_12.pdf

10.3 Verzeichnis von Verarbeitungstätigkeiten

Gemäß Art. 30 DS-GVO hat jeder Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten zu führen. Zwar besteht bei Verantwortlichen, bei denen weniger als 250 Mitglieder beschäftigt sind, zunächst eine Ausnahme von der Verzeichnisführungspflicht. Diese Ausnahme gilt jedoch nicht, wenn die Verarbeitung ein **Risiko** für die Rechte und Freiheiten der betroffenen Personen birgt, wenn die **Verarbeitung nicht nur gelegentlich** oder eine Verarbeitung **sensibler Daten** i.S. von Art. 9 oder Art. 10 DS-GVO erfolgt (Art. 30 Abs. 5 DS-GVO).

Da jedoch in jedem Verein die Verarbeitung personenbezogener Daten nicht nur gelegentlich erfolgt, ist auch bei Vereinen mit weniger als 250 Mitarbeitern ein Verzeichnis von Verarbeitungstätigkeiten zu führen.

Das Verzeichnis muss zwingend folgende Angaben enthalten (Art. 30 Abs. 1 DS-GVO):
- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind bzw. noch offengelegt werden
- Angaben über Drittlandtransfer einschließlich Angabe des Drittlandes sowie

Dokumentierung geeigneter Garantien
- wenn möglich Fristen für die Löschung der verschiedenen Datenkategorien
- wenn möglich Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO

Das Verarbeitungsverzeichnis muss **schriftlich** oder in einem **elektronischen Format** geführt werden (Art. 30 Abs. 3 DS-GVO). Der Verantwortliche ist verpflichtet, der Aufsichtsbehörde das Verzeichnis auf deren **Anfrage** zur Verfügung zu stellen. Ein Einsichtsrecht für betroffene Personen oder „Jedermann" besteht nach der DS-GVO nicht mehr.

WEITERE INFORMATIONEN finden Sie in Kurzpapier Nr. 1 der Datenschutzkonferenz „Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO", unter www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Kurzpapiere/Kurzpapier_Nr_1.pdf

10.4 Datenschutz-Folgeabschätzung

Der Verein hat nur dann eine Datenschutz-Folgeabschätzung vorzunehmen, wenn die Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke ein **hohes Risiko** für die Rechte und Freiheiten für die betroffene Person zur Folge hat (Art. 35 Abs. 1 DS-GVO). Dies insbesondere dann der Fall, wenn eine **umfangreiche Verarbeitung besonderer Kategorie von Daten** gemäß Art. 9 DS-GVO erfolgt oder wenn im Wege der Verarbeitung auf Grundlage von personenbezogenen Daten **systematische und umfassende Bewertungen persönlicher Aspekte** vorgenommen werden, die als Grundlage für Entscheidungen dienen, die Rechtswirkungen gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen (Art. 35 Abs. 3 DS-GVO).

Eine Datenschutz-Folgeabschätzung hat eine Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke sowie möglicher berechtigter Interessen des Verantwortlichen, eine Beschreibung der Notwendigkeit der Abwicklung sowie ihrer Verhältnismäßigkeit, eine Bewertung der Risiken und eine Beschreibung des Maßnahmen zur Risikoreduzierung zu enthalten (Art. 37 Abs. 7 DS-GVO). Eine Datenschutz-Folgeabschätzung dürfte aber bei Vereinen nur in seltenen Fällen notwendig sein.

WEITERE INFORMATIONEN finden Sie in Kurzpapier Nr. 5 der Datenschutzkonferenz „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO" unter www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Kurzpapiere/Kurzpapier_Nr_5.pdf