Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

Datenschutz im Verein nach der Daten-schutzgrundverordnung (DS-GVO)

Informationen über die datenschutzrechtlichen Rahmenbedingungen beim Umgang mit personenbezogenen Daten in der Vereinsarbeit

- Gültig ab 25. Mai 2018 -

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit
Baden-Württemberg
Königstraße 10a
70173 Stuttgart
Telefon 0711/615541-0
Telefax 0711/615541-15
E-Mail: poststelle@lfdi.bwl.de
(Schutzbedürftige Daten sollten nicht unverschlüsselt per E-Mail oder via Telefax übertragen werden.)
PGP-Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962
Homepage: www.baden-wuerttemberg.datenschutz.de

Inhaltsübersicht

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

1.1 Datenschutzgrundverordnung und Bundesdatenschutzgesetz-neu als Rechtsgrundlage

Ab dem 25. Mai 2018 wird 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 ab 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.

1.2 Begriffsbestimmungen

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 (s. u. Nr. 3.3), auch bei der EDV-Wartung und der Aktenvernichtung.

1.3 Rechtmäßigkeit der Verarbeitung

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten richtet sich nach Art. 6 Abs. 1 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 Unionsrecht 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.

1.3.1 Rechtsgrundlagen

Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten kommen insbesondere Art. 6 Abs. 1 lit. b) und lit. f) DS-GVO in Betracht (Näheres dazu unter 2.1).

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.

1.3.2 Informationspflichten

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.

1.3.3 Schriftliche Regelungen zum Datenschutz: Datenschutzordnung

Den Verein trifft die Pflicht, die Grundzüge der Datenerhebung, -verarbeitung und -nutzung schriftlich festzulegen. **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 noch 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 **andere 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. 3.2) 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 die nicht zur regelmäßigen Nutzung der Daten befugt sind (s. u. Nr. 4.1) - darauf Zugriff 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** offenbart und welche in das Internet oder Intranet eingestellt werden.

Diese Datenschutzordnung sollte von der Mitgliederversammlung beschlossen werden. Wegen einer späteren Änderung s.o. Nr. 1.3.1.

1.3.4 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 Nr. 2, 4 und 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 erfolgt 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. 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 seines Sorgeberechtigten zulässig.

Als Anlage ist das **Muster einer Einwilligungserklärung** für die Veröffentlichung personenbezogener Mitgliederdaten im **Internet** beigefügt. Es empfiehlt sich, eine solche Einwilligung von Neumitgliedern bereits bei der Aufnahme in den Verein einzuholen. Altmitglieder können über die Vereinsmitteilungen eine allgemeine Informa-

tion mit einer derartigen Einwilligungserklärung und dem Hinweis auf das jederzeitige Widerrufsrecht erhalten. 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.

2. Erhebung personenbezogener Daten durch den Verein

2.1 Erhebung von 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. Es genügt dafür nicht, dass der Verein selbst Mitglied eines anderen Vereins oder Dachverbands ist. Dann ist Art. 26 DS-GVO zu beachten.

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. Berechtigt in diesem Sinne ist jeder Zweck, dessen Verfolgung nicht im Widerspruch zur Rechtsordnung steht und von der Gesellschaft nicht missbilligt wird. Aus dem vertraglichen Vertrauensverhältnis zwischen den Vereinsmitgliedern und dem Verein folgt jedoch, dass der Verein bei der Verarbeitung der personenbezogenen Daten seiner Mitglieder stets auf deren Datenschutzgrundrecht besonders Rück-

sicht zu nehmen hat. Die Mitgliederdaten dürfen deswegen nur ausnahmsweise für einen anderen Zweck als zur Betreuung und Verwaltung der Mitglieder und zur Erreichung des Vereinszwecks verwendet werden.

Soll die Erhebung, Verarbeitung und Nutzung 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. Neumitglieder sollten beim Eintritt in den Verein danach gefragt werden, ob es derartige schutzwürdige Belange in ihrer Person gibt. Es ist aber durchaus auch möglich, später in einem Rundschreiben, im Vereinsblatt oder per E-Mail die Mitglieder aufzufordern, derartige Belange vorzubringen, wenn der Verein eine Datenverarbeitung aufgrund des Art. 6 Abs. 1 lit. f) DS-GVO beabsichtigt. Der Verein sollte in einer Datenschutzordnung (s. o. Nr. 1.3.3) regeln, auf welchem Weg die Betroffenen ihre schutzwürdigen Interessen geltend machen können.

2.2 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. Von den Meldebehörden darf der Verein keine Gruppenauskünfte nach § 32 Abs. 3 Satz 1 des Meldegesetzes Baden-Württemberg einfordern. Dies ist selbst dann nicht zulässig, wenn der Verein karitative Ziele verfolgt. Vereine sind datenschutzrechtlich grundsätzlich ohne Einwilligung nicht be-

rechtigt, 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.

2.3 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.

2.4 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 (siehe dazu oben Nr. 1.3.2).

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 [s. u. Nr. 5.10]), 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. 5.3 und 5.6). 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. Weitere Informationen zum diesem Thema finden Sie im Kurzpapier der DSK unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/08/DSK_KPNr_10_Informationspflichten.pdf

3. Speicherung personenbezogener Daten

Der Verein kann Daten mittels herkömmlicher Karteien oder automatisiert speichern (vgl. Art. 2 Abs. 1 DS-GVO). Die Speicherung 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.

3.1 Sicherheit personenbezogener Daten

Nach Art. 32 DS-GVO sind bei der Verarbeitung personenbezogener Daten geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Hierbei müssen die Maßnahmen einen Schutz gegen jegliche Arten (datenschutz-) rechtswidriger Verarbeitung von personenbezogenen Daten bieten.

In Art. 32 Abs. 1 DS-GVO werden beispielhaft Mindestanforderungen wie Pseudonymisierung, Verschlüsselung und Maßnahmen zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie technische und organisatorische Maßnahmen zur schnellen Wiederherstellung von Systemen bei technischen Zwischenfällen und solche zur regelmäßigen Evaluierung der Wirksamkeit aller technisch-organisatorischen Maßnahmen genannt.

Diese Maßnahmen sollte der Verein - unabhängig von gesetzlichen Vorgaben - bereits aus eigenem Interesse umsetzen. So ist - um z.B. zu verhindern, dass die in einem Computersystem abgelegten Mitgliederdaten von Unbefugten genutzt werden können - an die Einrichtung von passwortgeschützten Nutzer-Accounts und eines Firewall-Systems sowie eine Verschlüsselung der Mitgliederdaten zu denken. Grundsätzlich sind die Maßnahmen auch dann geboten, wenn die Datenverarbeitung von Mitgliedern ehrenamtlich zu Hause mit eigener EDV-Ausstattung erledigt wird.

Die technischen und organisatorischen Maßnahmen sind von Art. 32 DS-GVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen zu treffen.

3.2 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 schreibt die DSGVO 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 gewährleistet ist (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 Rechtsinstrument**“ 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 Vertragsmustern. 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 bisheriger Rechtslage war der Auftragnehmer nicht als Dritter, sondern als Teil der verantwortlichen Stelle anzusehen mit der Folge, dass keine Datenübermittlung vorlag und somit und auch keine Einwilligung der Mitglieder in die Auftragsdatenverarbeitung erforderlich war. Eine solche Privilegierung kennt die DS-GVO jedoch nicht. Die Weitergabe von personenbezogenen Daten an den Auftragsverarbeiter stellt daher eine **Übermittlung** dar. Rechtsgrundlage für diese Verarbeitung ist Art. 6 Abs. 1 lit. f) DS-GVO. Denn ein berechtigtes Interesse i. S. des Art. 6 Abs. 1 lit. f) DS-GVO ist dann zu bejahen, wenn sich der Verantwortliche für diese Organisation seiner Datenverarbeitung entschieden hat.

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 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 und ob die Daten in Drittländern bzw. zu einem anderen Zweck als zum Zeitpunkt ihrer Erhebung von diesen verarbeitet werden (s.o. Nr. 1.3.1) 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 AV-Vertrags oder der gesetzlichen Pflichten des Verantwortlichen bzw. des Auftragsverarbeiters erforderlich sind.

Weitere Informationen zum diesem Thema finden Sie in Kurzpapier Nr. 13 der Datenschutzkonferenz „Auftragsverarbeitung“ abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/02/DSK_KpNr_13_Auftragsverarbeitung.pdf

3.3 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 im Gegensatz zum BDSG nach der DS-GVO grundsätzlich zulässig. Zu beachten sind dabei insbesondere die zusätzlichen Anforderungen an die **Sicherstellung des Datenschutzniveaus** beim Auftragsverarbeiter nach Kapitel V der DS-GVO. So muss gemäß Art. 28 Abs. 1, Art. 44 DS-GVO den Anforderungen der Art. 45 ff. DS-GVO auch im Ausland Rechnung getragen werden. Dies gilt auch bei einer Weiterübermittlung der personenbezogenen Daten durch die empfangende Stelle im Drittland (Art. 44 S. 1 DS-GVO).