Ist Ihr Verein für die neue Datenschutzgrundverordnung (DSGVO) gewappnet?

Es dauert nicht mehr lange bis zum **25.Mai 2018**. Ab diesem Tag gelten europaweit die Vorschriften und Maßgaben der neuen DatenschutzgrundVO (DSGVO) sowie das neue Bundesdatenschutzgesetz (BDSG) vom 20. Juni 2017.

Die DSGVO gilt nicht nur für kommerzielle Unternehmen, sondern selbstverständlich auch für Vereine. (vgl. § 2 Abs. 4 S. 1 BDSG). Die DSGVO macht keinen Unterschied zwischen kleinen und großen Unternehmen und auch nicht zwischen wirtschaftlich arbeitenden Unternehmen und ideellen Vereinen. Auch spielt es weder eine Rolle, ob der Verein gemeinnützig ist oder nicht, noch ob der Verein in das Vereinsregister eingetragen („e.V.“) ist oder nicht.

Datenschutz spielt auch im Verein eine große Rolle, schließlich werden Mitgliederdaten verarbeitet. Mitgliederdaten stellen häufig auch persönliche Daten dar, weswegen oft die DSGVO bzw. das neue BDSG Anwendung finden.

So werden zum Beispiel persönliche Daten erhoben:

- bei der Abfrage und Speicherung von Mitglieder- (Name, Adresse…) und Kontodaten,
- bei der Weitergabe von Daten der Sportler (Name, Alter, etc.) an einen übergeordneten Verband,
- in einer Pressemitteilung an Dritte oder
- bei Gesundheitssportangeboten werden sensible Gesundheitsdaten der Teilnehmer abgefragt.

Über Datenschutz wird zwar allseits viel gesprochen, leider wird er aber immer noch vielfach nicht oder nur in unzureichendem Maße beachtet und umgesetzt. Ein Grund hierfür mag ein mangelndes Bewusstsein dafür sein, dass auch personenbezogene Daten ein schützenswertes Rechtsgut darstellen. Ihre Weitergabe bzw. die Kenntnisnahme durch Dritte betrifft unmittelbar die Privatsphäre und damit die Autonomie und Selbstbestimmung der betreffenden Person. Das Datenschutzrecht dient dem Schutz des Persönlichkeitsrechts derjenigen Menschen, auf die sich die personenbezogenen Daten beziehen.

Der Grundsatz der DSGVO besagt: Wer personenbezogene Daten verarbeitet, ist verantwortlich für die Einhaltung aller in der DSGVO aufgeführten Rechtsgrundsätze. Im Mittelpunkt des Datenschutzes und der neuen Verordnungen steht also der Umgang im Verein mit personenbezogenen Daten.

Welches sind die wesentlichen Neuerungen?

Konkret in der neuen DSGVO geregelt werden vor allem die Rechtsgrundlagen der Datenverarbeitung, die Rechte der Betroffenen und die Pflichten der Verantwortlichen.

Die Rechte der Nutzer werden durch neue Transparenz-und Informationspflichten der datenverarbeitenden Unternehmen gestärkt. Betroffene sollen leichter Zugang zu ihren Daten und der Information über deren Nutzung haben. Außerdem wird das bislang nur gerichtlich zugesprochene „Recht auf Vergessenwerden“, also der Anspruch auf Löschung personenbezogener Daten nun in Gesetzesform gegossen.

Neu ist beispielsweise die Pflicht für Unternehmen, elektronische Geräte und Anwendungen datenschutzfreundlich voreinzustellen. Ebenfalls neu eingeführt wird die Pflicht zur Datenschutz-Folgenabschätzung bei besonderen Risiken für die erhobenen Daten, etwa durch neue Technologien.
Außerdem gilt die DSGVO auch für Unternehmen, die ihren Sitz außerhalb der EU haben, wenn sich ihre Angebote an EU-Bürger wenden. Dies hat weitreichende Konsequenzen etwa für Unternehmen wie Facebook und Google mit Sitz in den USA.

Drastische Änderungen enthält die DSGVO bei der Höhe der Bußgelder. Im Extremfall kann bis zu 4% des weltweiten Jahresumsatzes eines Unternehmens anfallen. Damit soll eine abschreckende Wirkung erzielt werden. Zudem können bei datenschutzrechtlichen Verstößen Ansprüche auf Schadensersatz wegen immaterieller Schäden geltend gemacht werden (vgl. Art. 82 DSGVO). Ein solcher immaterieller Schaden kann beispielweise in einer Rufschädigung bestehen.

Die wichtigsten datenschutzrechtlichen Regelungen möchte ich an dieser Stelle vorstellen:

1) *Impressum des Vereins*

Nahezu jeder Verein präsentiert sich heutzutage im Internet. So hält auch Ihr Angelsport-Verband HH eine selbst gestaltete Vereinshomepage bereit.

Wer eine Homepage hat, braucht eine Anbieterkennzeichnung – im allgemeinen Sprachgebrauch ein Impressum. TMG). Die Impressumspflicht besteht für die in § 5 TMG genannten **Diensteanbieter,**
die **geschäftsmäßige, in der Regel gegen Entgelt** angebotene **Telemedien** bereithalten. Dabei ist der **Telemedienbegriff** weit auszulegen. Praktisch jeder Online-Auftritt ist ein Telemedium.

Bsp. für Telemedien (nicht abschließend):
- private Websites, Blogs, Onlineshops, Online-Portale (Internetauktion),
- Plattformen,
- Werbeseiten,
- E-Mail-Dienste,
- Suchmaschinen,
- Chatrooms,
- Fanseiten bei z. B. Facebook.

Da Ihr Angelsport-Verband Angebote bzw. Telemedien auf seiner Homepage bereithält, gilt für die Vereins-Webseite eine Impressumspflicht.

Das Impressum sollte folgenden Inhalt haben:

- Name des Vereins (e.V. beschreibt die Rechtsform), Anschrift des Vereins, die zur Vertretung des Vereins berechtigte/n Person/en (Vorstand nach § 26 BGB),
- Angaben zur Kontaktaufnahme mit E-Mail-Adresse,
- das für den Verein zuständige Registergericht/Amtsgericht und die Vereinsregisternummer,
- Vereine, die umsatzsteuerpflichtig sind, haben zudem die Umsatzsteueridentifikationsnummer (USt-IDNr.) nach § 27a Umsatzsteuergesetz anzugeben.

Hinweis: In Deutschland hat eine Umsatzsteuer-Identifikationsnummer (USt-IdNr.) das Format der einleitenden Buchstabenfolge „DE“ gefolgt von neun Ziffern, also z.B: DE123456789. Die im Impressum des Vereins angegebene Nummer ist nicht die Umsatzsteuer-Identifikationsnummer!

- Europäische Streitschlichtung
  Im Impressum ist ein Hinweis nebst anklickbarem Link auf die Online-Streitschlichtungsplattform („OS-Plattform“) der EU-Kommission zu erteilen.

- Formulierungsvorschlag: "Die Europäische Kommission stellt eine Plattform für die außergerichtliche Online-Streitbeilegung (OS-Plattform) bereit, aufrufbar unter http://ec.europa.eu/odr."

- „Haftung für Inhalte“ (vgl. Impressum des Vereins)
  In das Impressum gehören nicht zwingend ein Haftungsausschluss sowie ein Hinweis auf das Urheberrecht (vgl. Impressum des Vereins)

Wichtig: Es reicht nicht, die Informationen auf der Seite mit den Kontaktdaten zu erwähnen. Das Impressum muss eindeutig zu erkennen sein. Die Informationen müssen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein. Das bedeutet, dass im optimalen Fall eine immer sichtbare Verlinkung zum Impressum und damit zu den dort hinterlegten Daten vorhanden ist - entweder als Menüeintrag oder als permanenter Link im Kopf- oder Fußbereich der Homepage.

2) Datenschutzerklärung für die Vereinshomepage

Jede Homepage benötigt eine Datenschutzerklärung (§ 13 TMG). Zwar besteht nach dem Wortlaut des Art. 13 DSGVO keine Pflicht, über die Arten und den Umfang der Datenverarbeitungsvorgänge so zu informieren, wie es derzeit noch § 13 Abs. 1 TMG vorsieht.

Es spricht aber viel dafür, dass die Datenschutzerklärung auch weiterhin über sämtliche auf der Webseite ablaufende Datenvorgänge belehren muss. Zum einen

soll die Informationspflicht das Schutzniveau für die Betroffenen weiter anheben (vgl. Erwägungsgrund 10 der DSGVO).

Zum anderen wird die Belehrung über Art und Umfang der Datenvorgänge im Zusammenhang mit den übrigen Informationen von der DSGVO logisch vorausgesetzt.
Der Hinweis auf die Arten und den Umfang der Erhebung und Verarbeitung ist zudem eine logische Voraussetzung dafür, den jeweiligen Verarbeitungszweck nach Art. 13 Abs. 1 lit. c DSGVO zu definieren. Dieser kann nur dann dargestellt werden, wenn die betroffenen Daten im Kontext von Seiten des gleichermaßen identifiziert werden.

Diese muss von jeder Seite der Homepage aus jederzeit abrufbar sein. Daran ändert sich auch unter Geltung der neuen DSGVO nichts. Der Link muss eindeutig mit dem Menüpunkt „Datenschutz“ bezeichnet werden und neben dem Link zum Impressum stehen.

Wichtig: Es empfiehlt sich, sowohl das Impressum als auch die Datenschutzerklärung klar zu kennzeichnen und über einen einzelnen Klick erreichbar zu halten**,** und zwar von jeder Seite der Homepage aus. Es reicht nicht, die Datenschutzerklärung in das Impressum aufzunehmen, sondern die Datenschutzerklärung sollte ein separater Menüpunkt sein.

3) *Umgang mit personenbezogenen Daten im Verein*

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. Die Vereinssatzung bestimmt insoweit die Vereinsziele, für welche die Mitgliederdaten genutzt werden können.

Bei einem Aufnahmeantrag muss das potentielle neue Mitglied erkennen können, bei welchen Informationen es sich um freiwillige und bei welchen um Pflichtangaben

handelt. Bei den freiwilligen Angaben sollte noch der Hinweis erteilt werden, zu welchem Zweck diese Daten erhoben und genutzt werden.

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

Ein Verein muss zur Betreuung seiner Mitglieder deren personenbezogene Daten verarbeiten. 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 Person beziehen. Hierzu zählen im Verein z.B. das Datum des Vereinsbeitritts, sportliche Leistungen bei einem Wettbewerb und dergleichen).

a) Für den Vereinszweck notwendige Daten

Grundsätzlich dürfen nur solche personenbezogenen Daten erhoben werden, die für die Begründung und Durchführung der Mitgliedschaft erforderlich sind (vgl. § 28 Abs. 1 Nr. 1 BDSG). Das bedeutet für Sportvereine, dass sie nur solche Daten erheben dürfen, die für die Mitgliederbetreuung und -verwaltung sowie für die Verfolgung des Vereinsziels erforderlich sind.

Dabei handelt es sich insbesondere um folgende Daten:

4) Name und Anschrift des Mitglieds
5) Bankverbindung bei Lastschrifteinzug (Satzung!)
6) Übungsleiterlizenz

7) Funktion im Verein
8) Telefonnummer/E-Mail
9) Geburtsdatum (Wettkampfklasse)

Wichtig: Personenbezogene Daten dürfen ausschließlich zu dem Zweck verwendet werden, zu dem sie erhoben wurden.

b) Einwilligung des Betroffenen -Verbot mit Erlaubnisvorbehalt (§ 4 BDSG)

Grundsätzlich darf der Verein nur personenbezogene Daten erheben, verarbeiten oder nutzen, soweit eine Vorschrift des BDSG oder eine sonstige Vorschrift dies erlaubt oder anordnet oder soweit der Betroffene einwilligt: Dies ist ein Verbot mit Erlaubnisvorbehalt! (§ 4 BDSG); d.h. es ist alles verboten, was nicht erlaubt ist!

Gibt ein (Neu-)Mitglied seine Kontaktdaten (Anschrift, Telefonnummer und E-Mail-Adresse) sowie seine Bankverbindung zwecks Abbuchung des Mitgliedsbeitrages bekannt, liegt hierin regelmäßig die gleichzeitige Einwilligung, dass der Verein diese personenbezogenen Daten zum Zwecke der Mitgliederverwaltung speichert und nutzt. Diese Datennutzung erfolgt im Rahmen einer vertraglichen Beziehung, nämlich der Mitgliedschaft, und ist daher regelmäßig unproblematisch, da der Verein zur Erhebung dieser Daten im Rahmen des Art. 6 Abs. 1 S. 1 lit. f DSGVO ermächtigt ist.

Nach Art. 6 Abs. 1 S. 1 lit. f DSGVO wird es in Zukunft ausreichen, wenn der Verantwortliche ein „berechtigtes Interesse“ an der Verarbeitung von personenbezogenen Daten hat. Hiernach wird das „berechtigte Interesse“ nun dadurch eingeschränkt, dass die Datenverarbeitung „erforderlich“ und nicht nur „zweckmäßig“ (vgl. § 28 BDG) sein muss und das schutzwürdige Interesse des Betroffenen nicht das Interesse des Verantwortlichen übersteigen darf.

Alle Daten, die für die Durchführung des Vertrages erforderlich sind, dürfen zu diesem Zweck erhoben werden, alles, was darüber hinaus geht, darf nicht ohne Weiteres erhoben werden.

So wäre die Abfrage des Kundennamens und der – anschrift sowie der Telefonnumer unproblematisch, die Abfrage des Lebensalters sowie der E-Mail-Adresse (neben der Telefonnummer) hingegen problematisch. Deren Erhebung würde eine förmliche datenschutzrechtliche Belehrung des Betroffenen voraussetzen.

Wichtig: Geht die Erhebung, Verarbeitung und Nutzung über das Maß der üblichen Mitgliederverwaltung im Verein hinaus, muss der Betroffene zuvor seine ausdrückliche Einwilligung geben. Die Einwilligung muss grundsätzlich schriftlich und vor allem freiwillig erteilt werden (vgl. § 4a Abs. 1 BDSG). 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).

Dabei muss zukünftig ein besonderes Augenmerk auf der Formulierung der Einwilligung liegen, da diese „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ (Art. 7 Abs. 2 DSGVO) erfolgen muss. Dies bedeutet, dass kritisch geprüft werden muss, ob die bereits vorliegenden Einwilligungserklärungen der Vereinsmitglieder noch den aktuellen Anforderungen entsprechen.

Für Kinder unter 16 Jahren schreibt Art. 8 DSGVO vor, dass die Einwilligung nur dann wirksam ist, wenn sie entweder von den Eltern selbst erteilt wurde oder zumindest mit deren Zustimmung. Die Einwilligung des Kindes allein genügt dann nicht.

Wichtig: Es empfiehlt sich, bei Begründung der Mitgliedschaft ein ausdrückliches Einverständnis mit der Erhebung und Verarbeitung aller abgefragten Daten einzuholen. Dabei sollte die Einwilligung zum Zwecke des Nachweises stets schriftlich erteilt werden.

4) *Maßnahmen für Datenschutz und Datensicherheit im Verein*

Aus der bestehenden Datenschutzverantwortung ergibt sich eine Verpflichtung, Maßnahmen umzusetzen, die den Datenschutz und die Datensicherheit im Verein gewährleisten:

Hierzu zählen die Folgenden:

a) *Datenschutzklausel in der Vereinssatzung*

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 (z.B. „Datenschutzordnung“) niedergelegt werden.

Es ist empfehlenswert, sich beim Aufbau der Datenschutzregelungen am Wege der Daten von der Erhebung über die Speicherung, Nutzung, Verarbeitung (insbesondere Übermittlung) bis hin zur Sperrung und Löschung zu orientieren. Dabei ist konkret festzulegen, welche Daten (z.B. Name, Vorname, Adresse u.s.w.), welcher Personen (Vereinsmitglieder, Teilnehmer an Veranstaltungen oder Lehrgängen) für welche Zwecke verwendet werden, ggf. auch ob Vordrucke oder Formulare zum Einsatz kommen.

Wichtig: Es ist empfehlenswert, regelmäßig Schulungen für die mit der Datenverarbeitung befassten Funktionsträger anzubieten, nicht zuletzt, um eine notwendige Datenschutzkultur innerhalb des Vereins zu entwickeln.

b*) Verpflichtung auf das Datengeheimnis*

In der neuen DSGVO ist keine explizite Regelung zur Verpflichtung auf das Datengeheimnis enthalten. Jedoch finden sich auch in der DSGVO verschiedene Normen (Art. 5 und 24 DSGVO), die am Datengeheimnis anknüpfen und dem Verantwortlichen die Pflicht auferlegen, Daten rechtmäßig zu verarbeiten und dies auch nachweisen zu können.

Es ist daher nach wie vor empfehlenswert, die im Verein mit der sensiblen Datenverarbeitung beschäftigten Personen persönlich auf das Datengeheimnis zu verpflichten und bei Aufnahme ihrer Tätigkeit entsprechend zu belehren (Merkblatt,

Schulung etc.) Eine Schriftform der Verpflichtung ist nicht vorgeschrieben, aber aus Beweisgründen dringend zu empfehlen! Die Verpflichtung auf das Datengeheimnis gilt nicht nur für hauptamtliche Mitarbeiter im Verein, sondern auch für ehrenamtliche Mitarbeiter und FSJ´ler (Freiwilliges soziales Jahr) bzw. Praktikanten.

ACHTUNG:

Frage: Muss schriftlich erfasst sein, wer auf welche Daten Zugriff hat?

Die Zugriffsrechte der Mitarbeiter sollten stets überprüft und dokumentiert werden. Dabei sollte regelmäßig hinterfragt werden, wer tatsächlich Zugang zu allen personenbezogenen Daten benötigt. Man sollte dies im Verfahrensverzeichnis machen.

Frage: Müssen private und Vereins-PCs sauber getrennt werden?

Es sollte unbedingt auf eine saubere Trennung von privaten und Vereins-PCs geachtet werden.

Mitgliederdaten sollten daher auf privaten PCs nicht gespeichert werden und geschäftliche E-Mails auch nicht an private Rechner übersandt werden. Denn jeder Verein muss gem. § 9 BDSG durch technische und organisatorische Maßnahmen sicherstellen, dass die Mitgliederdaten nicht missbräuchlich verwendet werden, Unbefugte Kenntnis von den Mitgliederdaten erlangen oder Mitgliederdaten auf Grund unzureichender Datensicherung verloren gehen.

Verlangen Sie daher von dem Mitarbeiter, dass der PC in einem Raum steht, der für die Erledigung der Vereinsangelegenheiten geeignet ist (z. B. häusliches Arbeitszimmer). Ebenso muss sichergestellt sein, dass der PC mit einer Sicherheitshard- und -software ausgestattet wird, damit Passwortschutz möglich ist. Außerdem muss gewährleistet sein, dass sich fremde Personen nicht unbeaufsichtigt in dem Raum aufhalten, in dem sich der PC befindet. Auch Familienangehörige dürfen keine Gelegenheit haben, vereinsinterne Unterlagen einzusehen oder mit dem Rechner zu arbeiten. Lassen Sie von Ihrem Mitarbeiter unbedingt eine Verpflichtungserklärung nach dem Datenschutzgesetz unterschreiben (s.o.).

Auf der sicheren Seite sind Sie, wenn Sie Ihre Mitgliedsdaten nicht lokal auf einer Festplatte (oder einem anderen Speichermedium) vorhalten, sondern eine Online-

Software für die Mitgliederverwaltung nutzen. Dabei liegen die Daten auf einem gesicherten Server, auf den Sie online zugreifen.

Frage: Muss der Vereinsserver in Europa stehen?

Der Server sollte innerhalb Europas stehen, da es zur Zeit keine eindeutige Safe Harbour Regelung mehr gibt, zu beachten ist jedoch, dass die Daten in einem Datacenter in Deutschland oder einem EU-Mitgliedsland gespeichert werden. Dadurch ist sichergestellt, dass die Vorgaben der Datenschutz-Grundverordnung zwingend eingehalten werden.

c) Bestellung eines Datenschutzbeauftragten

Eine Verpflichtung des Vereins zur Bestellung eines Datenschutzbeauftragten ergibt sich, wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Auch Ehrenamtliche zählen in Bezug auf die Frage nach der relevanten Personenzahl mit.

Die Aufgaben des Datenschutzbeauftragten sind in Art. 39 DSGVO 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.

Besteht keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten, muss sich der Vereinsvorstand selbst um die Einhaltung des Datenschutzes durch den Verein kümmern.

Wichtig: Es ist nicht mehr möglich, dass der Vorstand im Sinne des § 26 BGB die Funktion des Datenschutzbeauftragten im Verein übernimmt. Neu ist zudem, dass der Datenschutzbeauftragte gemäß § 37 Abs. 8 DSGVO der jeweiligen Aufsichtsbehörde gemeldet werden muss.

d) Verzeichnis von Verarbeitungstätigkeiten

Die DSGVO verlangt in Art. 30 DSGVO, dass ein Verzeichnis aller Verarbeitungstätigkeiten erstellt werden muss. Das gilt auch für kleinere Vereine, da die Datenverarbeitung nicht nur gelegentlich erfolgt (Art. 30 Abs. 5 DSGVO). In einer Tabelle listet man auf, welche Daten wann, wie und warum im Unternehmen erhoben werden und wo diese gespeichert werden. Etwa die Daten der Mitglieder: Name, Adresse, Telefonnummer.

Ein Verzeichnis von Verarbeitungstätigkeiten muss dokumentieren, welche personenbezogenen Daten der Verein mit Hilfe welcher Verfahren auf welche Weise verarbeitet und welche technisch-organisatorischen Maßnahmen zum Schutz dieser Daten getroffen werden. Es muss sichergestellt werden, dass datenschutzrechtliche Belange bei Beginn und Änderung eines jeden Prozesses im Verein Berücksichtigung finden.

Erforderliche Angabe im Verzeichnis:

- Name und Kontaktdaten der Verantwortlichen (Vorstand und ggf. Datenschutzbeauftragter)
- Zweck der Verarbeitung (z.B. Lohnabrechnung, Mitgliederverwaltung, Antragsbearbeitung)
- Rechtsgrundlage der Verarbeitung (z.B. Einwilligung, Arbeitsvertrag, Mitgliedschaft)
- Beschreibung der Kategorien betroffener Personen (z.B. Mitarbeiter, Funktionsträger, Mitglieder) und der personenbezogenen Daten (z.B. Adressdaten, Geburtsdatum, Bankverbindung)
- Ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (z.B. Banken, Auftragsverarbeiter)
- Dauer der Speicherung (z.B. Hinweis auf steuerrechtliche Aufbewahrungsfristen)
- Beschreibung der technischen (z.B. Datensicherung) und organisatorischen Maßnahmen (z.B. Zugangskontrolle).

Wichtig: Es empfiehlt sich, eine Übersicht aller im Verein eingesetzten Anwendungen und Tools (IT-Verfahren und Dateien), in denen personenbezogene Daten verarbeitet werden, zu erstellen. Nehmen Sie zu dem Verarbeitungsnachweis zusätzlich auf, dass Sie die betroffenen Personen auf die Verarbeitung hingewiesen haben.

e) Aufbewahrungs- und Löschungsfristen

Für die gespeicherten personenbezogenen Daten sind Aufbewahrungs- und Löschungsregelungen vorzusehen, da diese nur solange gespeichert werden dürfen, wie sie zur Aufgabenerfüllung erforderlich sind (§§ 28, 35 Abs. 2 Satz 2, 3a Satz 1 BDSG). Sollten die Daten nicht länger benötigt werden (z.B. bei Austritt aus dem Verein), so haben die Betroffenen ein „Recht auf Vergessenwerden“. Das bedeutet: Fällt der Grund für die Datenspeicherung weg, müssen diese gelöscht werden. Welche Fristen vorzusehen sind, hängt im Einzelfall von dem jeweiligen Geschäftszweck des Vereins ab.

Anders als derzeit in § 35 Abs. 2 S. 2 Nr. 4 BDSG vorgeschrieben, wird es im Anwendungsbereich der DSGVO keine starren Löschfristen mehr für personenbezogene Daten geben. Auch das neue BDSG sieht keine fixen Löschfristen vor.

In der Datenschutzerklärung genügt für die Dauer der Speicherung von Daten folgender Hinweis:

„Die Dauer der Speicherung von personenbezogenen Daten bemisst sich anhand der jeweiligen gesetzlichen Aufbewahrungsfrist. Nach Ablauf der Frist werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung oder Vertragsanbahnung erforderlich sind und/oder unsererseits kein berechtigtes Interesse an der Weiterspeicherung fortbesteht. Gebietet die Ausübung von Interventionsrechten die Löschung, werden die entsprechenden Daten unverzüglich gelöscht."

Wichtig: Eine Angabe von Zeitspannen (10 Jahre o.ä.) ist nicht erforderlich, weil für verschiedene Datensätze je nach Gesetz auch verschiedene Aufbewahrungsfristen bestehen. Es genügt also, als Kriterium für die Dauer der Speicherung pauschal auf die gesetzlichen Aufbewahrungsfristen zu verweisen.

f) Technische und organisatorische Maßnahmen

Die neue DSGVO verpflichtet Verarbeiter von personenbezogenen Daten in Art. 32 DSGVO dazu ,“geeignete technische und organisatorische Maßnahmen (TOM) zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten:“ Hierzu zählen u.a. die Pseudonymisierung und die Verschlüsselung sowie die Gewährleistung der Vertraulichkeit.

Die technischen und organisatorischen Maßnahmen spielen eine besondere Rolle, weil sie den ganzen Datenschutz im Unternehmen “überwachen”. Es geht also zum großen Teil darum, wie die Daten der Betroffenen (Kunden, Lieferanten, Mitarbeiter etc.) geschützt und abgesichert sind.

Eine besondere Bedeutung kommt den TOM dann zu, wenn es zu einem meldepflichtigen Datenleck oder Datenschutzverstoß gekommen ist. Dann können die TOM dazu dienen zu belegen, dass angemessene Maßnahmen zum Schutz getroffen wurden. Dabei sollten Sie dafür sorgen, dass die TOM am besten so schnell wie möglich dokumentiert werden und nicht erst, wenn eine Behörde nach ihnen fragt.

5) Datenverarbeitung im Auftrag (Art. 4 Nr. 8 DSGVO)

Externe Dienstleister, mit denen der Verein zusammenarbeitet, bezeichnet die DSGVO als "Auftragsverarbeiter". Bei der Auftragsverarbeitung sind folgende Punkte zu beachten:

- eine sorgfältige Auswahl des Dienstleiters ("Auftragsverarbeiters"),
- datenschutzrechtliche Regelungen sollten in eine entsprechende vertragliche Vereinbarung aufgenommen werden,

- Kontrolle: Der Auftragsverarbeiter sollte seine Datenschutzmaßnahmen im Vertrag aufführen. Der Verein sollte die Einhaltung der Datenschutzbestimmungen kontrollieren
- Bei Beendigung des Vertrages müssen Unterlagen zurückgegeben werden und ggf. sind Löschungen vorzunehmen

Wird eine sog. Cloud verwendet, um personenbezogene Daten von Vereinsmitgliedern zu speichern, ist von einer Auftragsdatenverarbeitung i.S. des Art. 4 Nr. 8 DSGVO auszugehen. Das bedeutet, dass auch hier keine Einwilligung seitens der Mitglieder erforderlich ist – es sei denn, die Datenverarbeitung befindet sich außerhalb der Europäischen Union oder des EWR.

Mit diesen Auftragsdatenverarbeitern ist eine ADV Aufrtagsdatenverabreitungsvereinbarung nach DSGVO-Grundzügen zu schließen.

Frage: Speicherung und Archivierung von Daten in clouds?

Auch Vereine müssen gründlich darüber nachdenken, wem sie Daten Dritter anvertrauen. Ihnen droht für jeden Datenschutzverstoß im Extremfall ein Bußgeld bis zu 300 000 Euro. Wozu sich ein Nutzer eines Cloud-Dienstes rechtlich verpflichtet, welche Leistung er vom Diensteanbieter beanspruchen darf und wofür dieser haftet – all das ist Gegenstand vertraglicher Vereinbarungen. Für den Fall, dass es doch zu einem unberechtigten Zugriff kommt, muss man zudem Details zur Haftung vereinbaren. Rechtlich gesehen stellen sich bei Cloud-Verträgen unter anderem Fragen nach Gewährleistungs- und Schadenersatzansprüchen. Auch Handhabung und Schutz von Urheberrechten sollten Gegenstand eines Nutzungsvertrags sein.

Wer das Rechtsrisiko nicht eingehen will, einen nach dem deutschen Datenschutzrecht nicht geeigneten Anbieter (wie z.B. google oder apple) zu nutzen, muss ein nur national oder nur innerhalb der EU operierendes Unternehmen wie beispielsweise Strato oder T-Systems wählen. Wenn es mit einem solchen Cloud-Diensteanbieter zu Problemen kommt, ist zumindest gewährleistet, dass man gerichtlich gegen ihn vorgehen kann und außerdem leichter Zugriff auf die beim Anbieter gespeicherten Daten bekommt.

6) Übermittlung von personenbezogenen Daten 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) DSGVO ist die Übermittlung personenbezogener Daten an Dritte nur zulässig,

- mit wirksamer Einwilligung der betroffenen Person,
- zur Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist,
- zur Durchführung vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person,
- zur Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses,
- zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt,
- zur Wahrung berechtigter Interessen der Verantwortlichen oder eines Dritten, sofern nicht schutzwürdige Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person am Ausschluss einer solchen Übermittlung überwiegen,
- zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person oder
- zur Erfüllung hoheitlicher Aufgaben, die dem Verantwortlichen übertragen wurden.

ist.

Wichtig: Bei den Vereinsmitgliedern handelt es sich im Verhältnis zum Verein um Dritte. Vereinsmitglieder dürfen also nicht einfach auf die Daten der anderen Mitglieder Zugriff nehmen. So dürfen z.B. Mitgliederlisten nicht einfach an die Mitglieder ausgegeben werden. So dürfen personenbezogene Daten von Mitgliedern nur offenbart werden, wenn es für die Erreichung des Vereinszwecks unbedingt erforderlich ist z.B. bei Mannschaftsaufstellungen oder Spielergebnissen (vgl. Art. 6 Abs. 1 lit.b) und lit. f DSGVO).

7) Auskunfts- und „Recht auf Vergessenwerden“ des Betroffenen

a) *Auskunftsrecht*

Zentraler Punkt des Datenschutzes ist das Recht des Betroffenen auf Auskunft. Er muss darüber informiert werden, in welchem Umfang Daten von ihm gespeichert sind. Dieses Auskunftsrecht ist in Artikel 15 DSGVO zweistufig ausgestaltet. Danach hat die betroffene Person das Recht, von dem Verein eine Bestätigung darüber zu verlangen, ob (= 1. Stufe) überhaupt Daten verarbeitet werden. Ist dies der Fall, hat die Person ein Recht auf Auskunft über diese personenbezogenen Daten (= 2. Stufe).

Zudem besteht auch das Recht auf unentgeltliche Überlassung einer Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind. Wenn das Vereinsmitglied feststellt, dass die gespeicherten Daten nicht korrekt sind, hat es ein Recht auf Berichtigung (beispielsweise Namensänderung).

b) „Recht auf Vergessenwerden“

Die Mitglieder haben in den folgenden Fällen ein *Recht auf Vergessen* (d.h. die Löschung der Daten):

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

Eine weiteres Recht der Mitglieder und betroffenen Personen und damit eine Verpflichtung für den Verein besteht in der Benachrichtigungspflicht des Vereins bei der Verletzung datenschutz-rechtlicher Verpflichtungen. Diese Verpflichtung besteht nur dann nicht, wenn der Verein im Vorfeld die geeigneten technischen und organisatorischen Maßnahmen ergriffen hat.

8) Bußgeldvorschriften

Die gesamte Verordnung finden Sie übersichtlich abrufbar unter: **https://dsgvo-gesetz.de**

Zusammenfassung: Was ist zukünftig datenschutzrechtlich zu beachten?

- Verwenden Sie personenbezogene Daten nur für vereinsinterne Zwecke gemäß der Vereinssatzung,
- Geben Sie die personenbezogenen Daten nicht an Dritte weiter – es sei denn, Sie haben die schriftliche Einwilligung der betroffenen Person,
- Beschränken Sie den internen Zugriff auf die personenbezogenen Daten,
- Bestellen Sie einen Datenschutzbeauftragten, wenn in der Regel mindestens zehn Personen im Verein ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind,
- Erstellen Sie ein Verarbeitungsverzeichnisses nach Art. 30 DSGVO,
- Treffen Sie Vereinbarungen zur Auftragsdatenverarbeitung mit externen Dritten gem. Art. 28 DSGVO,
- Überarbeiten Sie frühere Einwilligungserklärungen gemäß den aktuellen Vorgaben der DSGVO,
- Überprüfen Sie die TOMs (=technischen und organisatorischen Maßnahmen),
- Erstellen Sie ein Sicherheitskonzept,
- Stellen sie sicher, dass die Betroffenenrechte gewährleistet sind.