Die Datenschutzgrundverordnung der EU:

Anlass zur Überprüfung des Datenschutzes im Verein

1. ***Am 25. Mai 2018 löst die Datenschutzgrundverordnung der EU (DS-GVO) alle bisherigen nationalen Gesetze zum Datenschutz ab***. Die DS-GVO ist direkt anwendbares europäisches Recht, das neue Bundesdatenschutzgesetz füllt nur noch einige wenige Spielräume aus, welche der europäische Gesetzgeber den Mitgliedstaaten zur eigenen Regelung überlassen hat. Für die Vereine hat es nur noch geringe Bedeutung, das noch nicht verabschiedete neue Landesdatenschutzgesetz für Baden-Württemberg hat praktisch keine Bedeutung für Vereine.

2. Das DS-GVO erfindet das Rad nicht neu, die bisherigen datenschutzrechtlichen Grundprinzipien gelten fort, sind allerdings nicht mehr so detailliert geregelt wie im noch geltenden Bundesdatenschutzgesetz. Die wesentlichen Grundprinzipien sind

   2.1. Das sogenannte ***„Verbot mit Erlaubnisvorbehalt***“, welches bedeutet, dass die Datenverarbeitung nur zulässig ist, wenn eine Einwilligung oder eine andere in Art. 6 DS-GVO normierte Ausnahme vorliegt. ***Im Vereinsrecht bedeutet dies, dass die Verarbeitung von Mitgliederdaten für die in der Satzung niedergelegten Vereinszwecke zulässig ist, wobei allerdings alle Grundprinzipien der Datenverarbeitung zu beachten sind***.

   2.2. Das Prinzip der ***Datensparsamkeit***, Art. 5 Abs. 1c DS-GVO, wonach die Verarbeitung personenbezogener Daten ***dem Zweck angemessen*** sein muss und auf das notwendige Maß zu beschränken ist.

   2.3. Der Grundsatz der ***Zweckbindung*****,** Art. 5 Abs. 1b DS-GVO, wonach personenbezogene Daten ***nur für festgelegte eindeutige und rechtmäßige Zwecke*** erhoben werden dürfen und auch spätere Änderungen des Verarbeitungszweckes mit dem ursprünglichen Erhebungszweck vereinbar sein müssen.

   2.4. Der Grundsatz der ***Datensicherheit,*** Art. 5 Abs. 1f DS-GVO, wonach geeignete technische und organisatorische Maßnahmen unter Berücksichtigung der Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Verletzung persönlicher Rechte zu ergreifen sind, um die Datensicherheit zu gewährleisten.

3. Organisatorische Anforderungen der DS-GVO

Die organisatorischen Anforderungen an die Datenverarbeitung sind nicht grundsätzlich neu, zum Teil aber gegenüber der heutigen Rechtslage verschärft, insbesondere durch die Verankerung einer Rechenschaftspflicht für Verantwortliche des Vereins, die Stärkung der Rechte Betroffener und der Aufsichtsbehörde (Landesbeauftragter für den Datenschutz).

3.1. Datenschutzorganisation des Vereins

3.1.1. Der Verantwortliche des Vereins für die Datenverarbeitung

Es ist ein Verantwortlicher des Vereins für die Datenverarbeitung zu bestimmen. Ausschließlich auf dessen Weisung dürfen Vereinsmitglieder oder Vereinsmitarbeiter, die Zugang zu personenbezogenen Daten haben, diese verarbeiten, Art. 30 DS-GVO. Dieser Verantwortliche führt ein Verzeichnis aller Datenverarbeitungstätigkeiten des Vereins, er hat gegenüber der Aufsichtsbehörde nachzuweisen, dass im Verein die datenschutzrechtlichen Grundsätze eingehalten werden.

Konkret bedeutet dies z.B., dass er ***nachweisen*** kann, welche personenbezogenen Daten zum Beispiel von Vereinsmitgliedern, aber auch von Vertragspartnern des Vereins gespeichert werden, welche Daten an Dritte weitergegeben werden, welches die Rechtsgrundlage hierfür ist, für welchen Zweck die Daten verwandt werden und wie lange sie gespeichert werden sollen.

Für diese Nachweise werden im Zweifel, wenigstens bei größeren Vereinen, ***schriftliche Dokumentationen*** hilfreich sein. Als Grundlage für diesen Nachweis bietet sich das von Art. 29 DS-GVO geforderte Verzeichnis von Datenverarbeitungstätigkeiten an, ergänzt eventuell durch weitere Informationen. Wichtig sind hier die Erwägungsgründe74 zu Art. 24 DS-GVO, welche die Verantwortung des für die Datenverarbeitung Verantwortlichen regelt. Darin heißt es:

> *„Die Verantwortung und Haftung des Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen und die Maßnahmen auch wirksam sind. Dabei sollte er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigen.“*

Verantwortlich für Fragen des Datenschutzes ist in Vereinen grundsätzlich der Vereinsvorstand. ***Datenschutz ist damit Chefsache***. Der Vereinsvorstand kann jedoch einen Verantwortlichen bestimmen, welcher sich um die Einhaltung der Datenschutzvorschriften kümmern muss und dafür auch persönlich verantwortlich ist. Aus dieser Verantwortlichkeit resultiert natürlich auch ein erhebliches Gewicht des Datenschutzverantwortlichen bei allen Entscheidungen, welche die Datenverarbeitung und deren Organisation im Verein betreffen. ***Ist im Verein kein konkreter Datenschutzverantwortlicher bestimmt, so ist gegenüber dem Landesdatenschutzbeauftragten der Vorstand direkt und gemeinschaftlich verantwortlich und haftet auch entsprechend direkt für Verstöße gegen den Datenschutz.***

3.1.2. IT-Sicherheit

Ziel der IT-Sicherheit ist der ***Schutz des Vereins*** durch die Vermeidung von wirtschaftlichen Schäden und die Minimierung von Risiken, welche für den Verein aus der Verletzung des Schutzes personenbezogener Daten entstehen können – etwa durch Schadensersatzansprüche der Betroffenen, durch Sanktionen des Landesdatenschutzbeauftragten oder durch Schäden an Hard-und Software des Vereins, die erhebliche Folgekosten verursachen können.

Schutzziele sind die ***Gewährleistung der Vertraulichkeit, Integrität (Unversehrtheit der Informationen) und Verfügbarkeit der Daten des Vereins***. Wichtig sind nicht nur ***Maßnahmen zur Abwehr von Angriffen von außen***, sondern insbesondere auch ein ***Berechtigungsmanagement***, welches innerhalb des Vereines festlegt, wer auf welche Daten zugreifen darf, die Einführung von Verschlüsselungstechniken, regelmäßige Aktualisierungen von Hard-und Software, Back-ups, aber auch ***das richtige Einsetzen der E-Mail-Kommunikation***. Über E-Mails sollten weder inhaltliche Informationen an falsche Empfänger versandt werden, noch über die „CC“ Funktion große Mengen an E-Mail-Adressen in aller Welt verstreut werden. Schon allein hierin liegt ein Verstoß gegen den Datenschutz, welcher durch die Nutzung der „BCC“ Funktion vermieden werden könnte.

3.1.3. Bestellung eines Datenschutzbeauftragten

Der Datenschutzbeauftragte soll den Verantwortlichen, also den Vereinsvorstand und den von diesem benannten Datenschutzverantwortlichen bei Fragen des Datenschutzes unterstützen. ***Die rechtliche Verantwortung dafür, dass der Datenschutz beachtet wird, liegt aber immer beim Verantwortlichen, also beim Vereinsvorstand und/oder dem von ihm benannten Datenschutzverantwortlichen.*** Vereine

können immer freiwillig einen Datenschutzbeauftragten bestellen, eine Pflicht hierzu besteht nur, wenn die Voraussetzungen des Art. 37 Abs. 1 DS-GVO erfüllt sind. ***Wenn sich im Verein nicht mindestens zehn Personen mit der Verarbeitung personenbezogener automatisierter Daten beschäftigen, besteht in der Regel keine Pflicht zur Bestellung eines Datenschutzbeauftragten.*** Wird aber ein Datenschutzbeauftragter bestellt, so ist dieser dem Landesbeauftragten für den Datenschutz zu melden und es ist zu veröffentlichen – sinnvollerweise im Internet – wie er erreichbar ist, zum Beispiel über eine E-Mail-Funktionsadresse.

3.1.4. Sicherstellung der Beachtung von Betroffenenrechten

Jeder Betroffene von der Datenverarbeitung eines Vereins, also zum Beispiel alle Mitglieder, deren Daten in der Mitgliederverwaltung verarbeitet werden, ist darüber zu ***informieren,*** was und zu welchem Zweck mit seinen Daten gemacht werden soll. Diese Information ist ***vor der entsprechenden Datenverarbeitung*** zu geben, Näheres Art. 12, 13, 14 DS-GVO.

Da im Verein auf jeden Fall Mitgliederdaten erhoben und verarbeitet werden ist es sinnvoll, in einer ***Datenschutzordnung*** festzulegen, „welche Daten beim Vereinseintritt - ggf. auch später - 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.“ (Datenschutz im Verein, Landesdatenschutzbeauftragter Baden-Württemberg, Mai 2017, S. 13).

Jeder Betroffene hat ein ***Auskunftsrecht*** über die von ihm durch den Verein gespeicherten oder sonst verarbeiteten Daten, die ihm vom Verantwortlichen konkret zu benennen sind. Aufgrund dieser Auskünfte muss der Betroffene in der Lage sein, zu beurteilen, ob er einen ***Anspruch auf Berichtigung, Löschung oder Sperrung seiner Daten*** geltend macht.

Neu in der DS-GVO ist das Recht des Betroffenen auf ***Datenübertragbarkeit***. Jeder Betroffene hat einen Anspruch darauf, die ihn betreffenden personenbezogenen Daten, die er einem Verantwortlichen

mitgeteilt hat, in einem gängigen Datenformat zur Verfügung gestellt zu bekommen oder darauf, dass diese an einen anderen Verantwortlichen (zum Beispiel an einen anderen Verein, zu dem der Betroffene gewechselt ist) weitergeleitet werden.
Die Vereine sollten darauf vorbereitet sein, ***Betroffenenrechten zeitnah nachzukommen***. Sollte sich der Betroffene bei der Aufsichtsbehörde beschweren, wird dieser den Verein zur Einhaltung seiner gesetzlichen Verpflichtung anhalten müssen und eventuell sein Fehlverhalten sanktionieren. Die Praxis wird zeigen, wie die Landesdatenschutzbeauftragten hier vorgehen, und ob und welche Übergangszeiten sie Vereinen bezüglich der Erfüllung ihrer Verpflichtungen nach der DS-GVO einräumen.

3.1.5. Informationspflichten bei Verletzung des Schutzes personenbezogener Daten

Wird der Schutz personenbezogener Daten verletzt, etwa durch unbeabsichtigtes oder unrechtmäßiges Handeln, das zur Vernichtung, zum Verlust, zu ihrer Veränderung, zur unbefugten Offenlegung bzw. zum unbefugten Zugang Dritter zu diesen Daten führt, so ist davon ***unaufgefordert die Aufsichtsbehörde in der Regel innerhalb von 72 Stunden zu informieren*** (Art. 33 Abs. 1 DS-GVO). Die Verletzung dieser Pflicht kann mit einem erheblichen Bußgeld (Art. 33 Abs. 4a DS-GV O) geahndet werden.

Der oder die durch die Verletzung des Schutzes ihrer Daten Betroffenen, sind dann zu ***benachrichtigen***, wenn die Schutzverletzung „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten“ dieser Personen zur Folge hat (Art. 34 Abs. 1 DS GVO).

Bei den Daten, welche Vereine in der Regel verarbeiten, dürfte dies eher nicht der Fall sein. ***Besondere Vorsicht ist natürlich geboten bei Gesundheitsdaten, wie sie in den ärztlichen Tauglichkeitszeugnissen enthalten sind. Besonders sensitiv sind auch alle Daten über Bankverbindungen und ähnliches. Da die Meldung an Betroffene rechtliche Folgen nach sich ziehen kann, ist hier besondere Vorsicht geboten.*** Eine Rücksprache mit dem Landesdatenschutzbeauftragten oder auch mit externen Beratern (auf den Datenschutz spezialisierte Rechtsanwaltskanzleien) kann im Einzelfall sinnvoll sein.

3.1.6. Auftragsverarbeitung

Schaltet ein Verein einen ***Dritten***, etwa eine externe Buchhaltung, ein, welche im Auftrag des Vereins dessen Daten verarbeitet, so kann er dies ohne ausdrückliche Einwilligung der Betroffenen tun, muss jedoch ***strenge***

Verfahrensvorschriften beachten, welche den Datenschutz gewährleisten sollen, vergleiche Art. 28f DS-GVO. Vorweg ist zu prüfen, ob der Auftragsverarbeiter zuverlässig die Garantie bietet, dass die datenschutzrechtlichen Vorschriften eingehalten werden. ***Der Verein muss sich dabei auch bewusst sein, dass er für Fehler und Mängel der Datenverarbeitung beim Auftragsverarbeiter haftet.*** Die Beziehung zum Auftragsvertreter ist durch einen ***schriftlichen Vertrag*** zu regeln, wobei sich der Auftraggeber ***umfangreiche Kontrollrechte*** einräumen lassen muss.

4. Sanktionen und Haftung

Die DS-GVO hat die ***Sanktionierung von Verstößen gegen den Datenschutz verschärft.*** Von der Aufsichtsbehörde (Landesdatenschutzbeauftragter) können ***Geldbußen*** verhängt werden. Vom Betroffenen können ***Schadensersatzleistungen und Schmerzensgeld*** eingeklagt werden, vergleiche Art. 82f DS-GVO und und §§ 42f des neuen Bundesdatenschutzgesetzes. Die Obergrenze für Geldbußen von 40 Millionen Euro ist ersichtlich auf große Unternehmen zugeschnitten, doch auch kleine Vereine sollten sich nicht allzu sicher fühlen, bei ernsthaften Datenschutzverstößen von Geldbußen verschont zu werden.

Der bayerische Landesdatenschutzbeauftragte nennt in seiner Broschüre „Erste Hilfe zu Datenschutz-Grundverordnung für Unternehmen und Vereine“ Beispiele für besonders häufige Datenschutzverstöße von Vereinen aus Tätigkeitsberichten der Aufsichtsbehörden. Typische Fälle seien danach

- ***Versendung von E-Mails mit offenem Verteiler***, sodass jeder Empfänger ohne Grund die E-Mail-Adressen der anderen Empfänger sehen kann,
- ***Aushang von Krankheitslisten*** von Mitarbeitern am „Schwarzen Brett“
- wiederholte ***Faxe mit medizinischen Daten an falsche Empfänger***

5. Was tun?

Der Verein sollte sich zunächst

- ein ***Verzeichnis*** seiner Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO erstellen,

- die ***Einbindung Externer in die Datenverarbeitung auf die Einhaltung der Verfahrensregeln überprüfen***, Art. 28 DS-GVO,

- die Rechtsgrundlage für die Verarbeitung personenbezogener Daten prüfen. Hierzu empfiehlt sich die ***Erstellung einer Datenschutzordnung***, welche die Verarbeitung der persönlichen Daten der Vereinsmitglieder beschreibt. Diese Datenschutzordnung ist entweder direkt in die Vereinssatzung aufzunehmen oder – dies ist vorzuziehen, da weit flexibler – in die Vereinssatzung ist eine ausdrückliche Ermächtigung zum Erlass einer Datenschutzordnung aufzunehmen und zu bestimmen, welches Organ – z.B. der Vorstand – diese Datenschutzordnung erlassen kann. Nach Erlass ist sie auf dem im Verein üblichen Wege ***den Mitgliedern bekannt zu geben***,

- prüfen, ob die ***Verantwortung für den Datenschutz im Verein*** klar geregelt ist. Ist ein ***Datenschutzverantwortlicher*** bestellt? Prüfung, ob ein Datenschutzbeauftragter zu bestellen ist,

- prüfen, ob ***Daten nur so lange gespeichert werden, wie ein sachlicher Grund vorliegt*** (Löschfristen),

- prüfen, ob die ***IT-Sicherheit*** den Anforderungen an ***Vertraulichkeit, Integrität und Verfügbarkeit der Systeme*** und Dienste der Datenverarbeitung genügen.

6. Fazit und Quellennachweise

Die oben genannten Anforderungen sind nicht gering und sie bleiben immer noch hinter dem zurück, was die DS-GVO, aber auch schon das heute geltende Datenschutzrecht, fordert. Auch wenn der Weg hin zu einer Datenverarbeitung, welche den gesetzlichen Anforderungen genügt, für viele Vereine lang und steinig sein wird und häufig auch kaum bis zum Inkrafttreten der DS-GVO zu bewältigen ist, so ***sollten doch die ersten Schritte bald getan werden***. In einem kleinen Luftsportverein ist die Datenverarbeitung letztlich doch sehr überschaubar und die organisatorischen und technischen Anforderungen des Datenschutzes sind Schritt für Schritt zu bewältigen.

Zur Hilfe seien hier Fundorte für die DS-GVO und das neue Bundesdatenschutzgesetz genannt:
DS-GVO: https://dsgvo-gesetz.de,
oder
Datenschutzgrundverordnung, hrsg. der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, dort als Broschüre umsonst zu beziehen oder im Internet zu finden unter

https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.html

Bundesdatenschutzgesetz (neu): https://dsgvo-gesetz.de/bdsg-neu

Als weiterführende Literatur (die auch für diesen Artikel herangezogen wurde) ist sehr zu empfehlen

Erste Hilfe zur Datenschutz-Grundverordnung, hrsg. vom Bayerischen Landesamt für Datenschutzaufsicht, zu beziehen für 5,50 €über den Beck Shop (http://m.beck-shop.de/item/3231343433383836) oder über Amazon,

sowie

Datenschutz im Verein, Landesbeauftragter für den Datenschutz Baden-Württemberg, 2017,

https://www.baden-wuerttemberg.datenschutz.de/datenschutz-im-verein/

Text: Hans-Dieter Rauscher, Juristische Beratung im BWLV