Leitfaden zur Umsetzung der Datenschutz-Grundverordnung (DSGVO) im Verein

Ab dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung der europäischen Union (DSGVO). Auch Vereinen werden zum Beispiel von den Mitgliedern viele persönliche Daten anvertraut. Die Daten der Mitglieder bieten häufig Einblicke in deren privaten Verhältnisse. Es ist somit für den Verein, der personenbezogene Daten als Verantwortlicher erhebt, zwingend erforderlich, die Vorgaben des Datenschutzes zu kennen und die Regelungen der DSGVO umzusetzen und einzuhalten.

Dieser Leitfaden soll kurz und verständlich über die wesentlichen inhaltlichen Vorgaben der DSGVO und die damit verbundenen Pflichten beim Umgang mit Daten innerhalb des Vereins informieren.

Bitte beachten Sie, dass aufgrund der stetigen Änderung der Rechtsprechung sowie teilweise noch sehr unterschiedlichen Auslegung der Bestimmungen der DSGVO keine Haftung für die nachfolgenden Ausführungen und Hinweise übernommen werden kann.

Inhalt

1. Anwendungsbereich der DSGVO

a. Arten der Verarbeitung

Die DSGVO gilt für die automatisierte sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten. Das bedeutet, dass jede elektronische Datenverarbeitung, sollte sie auch nur auf einen PC, Laptop oder sogar Smart-Phone vorgenommen werden, dem Anwendungsbereich der DSGVO unterfällt. Das Gleiche gilt für ein geordnetes Karteisystem (auf Papier), wenn zum Beispiel personenbezogene Daten auf Karteikarten, einer ausgedruckten Mitgliederliste oder in einzelnen Akten „gespeichert“ werden.

b. Personenbezogene Daten

Personenbezogene Daten sind nach der DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Name zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen,

genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 4 Nr. 1 DSGVO).

Personenbezogene Daten können beispielsweise der Name, die Adresse, die E-Mail Adresse, die Mitgliedsnummer, die Steuernummer, die Bankverbindung, aber auch die Religionszugehörigkeit oder auch ein Foto, auf dem die betroffene Person abgebildet ist, sowie die ungekürzte IP-Adresse (Zugangsnummer Internet) sein.

c. Verarbeiten personenbezogener Daten

Der Begriff Verarbeiten umfasst das Erheben, Speichern, Ändern, Nutzen, Übermitteln, Verknüpfen, Weitergeben oder Löschen der Daten. Es ist somit letztendlich egal, was mit personenbezogenen Daten gemacht wird, es handelt sich stets um ein Verarbeiten im Sinne der DSGVO. Dies gilt selbst dann, wenn einer anderen Person gestattet wird, personenbezogene Daten nur kurz einzusehen (Weitergabe).

Nur die Verarbeitung von personenbezogenen Daten für ausschließlich persönliche und familiäre Tätigkeiten und Zwecke (z. B. private Adressbücher und Fotosammlungen) fällt nicht in den Anwendungsbereich der DSGVO. Sobald die Verarbeitung personenbezogener Daten jedoch auch die Vereinsarbeit in welcher Form auch immer betrifft, ist der Anwendungsbereich der DSGVO eröffnet.

2. Verzeichnis von Verarbeitungstätigkeiten

Art. 30 DSGVO fordert grundsätzlich, dass alle Verantwortlichen ein Verzeichnis von Verarbeitungstätigkeiten führen müssen. Verantwortlicher ist jeder, der mit personenbezogenen Daten anderer umgeht. In dem Verzeichnis über Verarbeitungstätigkeiten muss dokumentiert werden, in welchem Zusammenhang mit personenbezogenen Daten und zu welchem Zweck gearbeitet wird.

Die DSGVO sieht zwar vor, dass Unternehmen und Einrichtungen die weniger als 250 Mitarbeiter beschäftigen von der Verpflichtung zur Führung eines solchen Verzeichnisses befreit sind. Diese Vorschrift hat in der Praxis aber so gut wie keine Bedeutung, weil diese Ausnahme nur dann gilt, wenn die Verarbeitung nur gelegentlich erfolgt und auch keine besonderen Datenkategorien wie Gesundheits- oder Religionsdaten verarbeitet werden. Jeder Verein, der für seine Beschäftigten zum Beispiel Lohnabrechnungen durchführt, verarbeitet jedoch grundsätzlich auch Religionsdaten zur Abführung der Kirchensteuer oder Gesundheitsdaten zur Feststellung der Krankheitstage. Jeder Verein

pflegt zusätzlich die Daten seiner Mitglieder - z. B. in Mitgliederlisten - und arbeitet somit ständig mit diesen Daten, so dass eine Verarbeitung von personenbezogenen Daten nicht mehr nur gelegentlich erfolgt und die Ausnahmevorschrift somit für Vereine nicht greift.

Das Verzeichnis von Verarbeitungstätigkeiten dient zunächst nur der eigenen Kontrolle und dafür, auf Anfrage der Aufsichtsbehörde nachzuweisen, mit welchen personenbezogenen Daten im Verein wie umgegangen wird. Das Verzeichnis ist somit nicht öffentlich und muss insbesondere gegenüber betroffenen Personen, von denen personenbezogene Daten erhoben werden, nicht offen gelegt werden.

Das Verzeichnis kann in elektronischer Form oder schriftlich erstellt werden und muss immer auf dem aktuellen Stand gehalten werden.

Der Inhalt des Verzeichnisses muss mindestens die in Art. 30 Abs. 1 DSGVO genannten Bestandteile haben. Das sind

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters;
- Zwecke der Verarbeitung der personenbezogenen Daten;
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- Kategorien von Empfängern von Daten einschließlich Empfänger in Drittstaaten (etwaige Übermittlung von Daten außerhalb der EU);
- Wenn möglich Aufbewahrungsfristen zur Löschung von personenbezogener Daten.

3. Verzeichnis technisch-organisatorische Maßnahmen

Sofern ein Verein – was wie dargelegt stets der Fall ist – zur Führung eines Verzeichnisses über Verarbeitungstätigkeiten verpflichtet ist, muss er ebenfalls ein Verzeichnis über die technisch-organisatorischen Maßnahmen zum Datenschutz im Verein schriftlich oder in elektronischer Form führen.

Das Verzeichnis über die technisch-organisatorischen Maßnahmen beinhaltet Informationen darüber, inwiefern personenbezogene Daten im Verein technisch geschützt sind und somit der Zugriff unbefugter Dritter möglichst vermieden wird. Dieses Verzeichnis muss zum Beispiel zum Inhalt haben, welche Virenschutzprogramme oder Firewalls eingesetzt werden, wo die Daten gespeichert werden (PC, Laptop, interne /

externe Server oder in der Cloud), wie Serverräume gesichert sind oder ob und wie Datensicherungen regelmäßig durchgeführt werden.

4. Datenschutz-Folgeabschätzung

Sofern die Form der Verarbeitung aufgrund ihrer 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 DSGVO), so muss der Verein eine Datenschutz-Folgeabschätzung vornehmen. Das ist jedoch nur ausnahmsweise für Vereine der Fall, die besondere Kategorien von personenbezogenen Daten (Art 9 DSGVO – z. B. Gesundheitsdaten) umfangreich als eigentlichen Vereinszweck (Kerntätigkeit) verarbeiten. Eine Datenschutz-Folgeabschätzung ist daher für Vereine in den seltensten Fällen erforderlich.

Die Datenschutz-Folgeabschätzung muss 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 enthalten (Art. 37 Abs. 7 DSGVO).

5. Grundsätze der Verarbeitung personenbezogener Daten

Im Datenschutzrecht und insbesondere nach der DSGVO gilt stets das Prinzip des „Verbots mit Erlaubnisvorbehalt“. Das bedeutet, dass niemand mit personenbezogenen Daten von anderen umgehen darf, wenn er nicht über eine ausdrückliche Einwilligung der betroffenen Person verfügt oder aber die Verarbeitung personenbezogener Daten auf einer Rechtsgrundlage beruht, die erlaubt oder sogar anordnet, mit personenbezogenen Daten Dritter umzugehen. Wichtig ist also, dass jeder, der mit personenbezogenen Daten umgehen möchte, vorher prüft, ob er eine Einwilligung zur Verarbeitung hat oder eine andere Rechtsgrundlage hierfür besteht.

a. Einwilligung

Eine Einwilligung ist nur dann wirksam, wenn sie

- freiwillig abgegeben wird;
- sie für einen bestimmten Zweck abgegeben wird;
- die Einwilligung auf einer klaren und verständlichen Information beruht, die den betroffenen deutlich macht, für welchen konkreten Zweck die Daten verarbeitet werden sollen;

- die betroffene Person darüber informiert wurde, dass die Einwilligung jederzeit widerrufen werden kann und
- die Einwilligung durch eine bestätigende Handlung der betroffenen Person erfolgt (dieses ist z. B. nicht der Fall, wenn im Internet ein bereits vorangehaktes Kästchen im Zusammenhang mit einer Einwilligungserklärung besteht. Der Nutzer muss vielmehr das Kästchen mit dem Häkchen immer aktiv ankreuzen).

Grundsätzlich ist die ordnungsgemäße Einwilligung des Betroffenen immer die sicherste Variante im Sinne des Datenschutzes. Zu beachten ist jedoch, dass jede Einwilligung auch widerrufen werden kann. Aus diesem Grunde sollte stets geprüft werden, ob die Verarbeitung personenbezogener Daten nicht auch auf einer anderen Rechtsgrundlage als der Einwilligung gestützt werden kann.

b. Verarbeitung zur Vertragserfüllung

Personenbezogene Daten, die zur Erfüllung eines Vertrages notwendig sind, können verarbeitet werden, ohne dass es einer ausdrücklichen Einwilligung des Betroffenen bedarf. Wenn also z. B. jemand Mitglied in einem Verein werden will, darf der Verein z. B. Namen, Kontaktdaten und Bankverbindung (im Falle einer Einzugsermächtigung) der antragstellenden Person erhalten, weil diese Daten dann zur Vertragserfüllung (Mitgliederverwaltung) erforderlich sind.

c. Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen

Personenbezogene Daten dürfen darüber hinaus auch zur „Wahrung berechtigter Interessen des Verantwortlichen verarbeitet werden, sofern nicht die Interessen der betroffenen Person überwiegen“. In diesem Fall ist somit immer eine Interessenabwägung vorzunehmen. So könnte man zum Beispiel diese Ermächtigungsgrundlage heranziehen, wenn der Verein personenbezogene Daten seiner Mitglieder dazu nutzt, dem Mitglied (über den Zweck der eigentlichen Mitgliedschaft heraus) zusätzlichen Informationen über geplante Termine und Veranstaltungen per E-Mail oder Post zukommen zu lassen. Hiermit wird ein Vereinsmitglied in der Regel rechnen müssen und es dürften keine Interessen des Mitglieds überwiegen, solchen Informationen nicht zu erhalten.

Zu beachten ist jedoch, dass die Wahrung der berechtigten Interessen des Verantwortlichen die „schwammigste“ Rechtsgrundlage darstellt. Denn eine Interessenabwägung könnte im Zweifelsfall die Interessen der betroffenen Person

über die Interessen der Verantwortlichen stellen und somit die Datenverarbeitung, sofern keine Einwilligung vorliegt, rechtswidrig machen.

d. Konkreter Zweck der Verarbeitung

Zu beachten ist in jedem Fall, dass eine Verarbeitung personenbezogener Daten, egal ob diese auf der Basis einer Einwilligung, eines Vertrages oder einer Interessenabwägung erfolgt, nur für einen vorab konkret festgelegten Zweck erfolgen darf. Es ist also erforderlich, dass sich der Verein damit befasst, zu welchem Zweck die Datenverarbeitung jeweils erfolgt und sichergestellt ist, dass die Daten auch nur für diesen Zweck verwendet werden. Beruht die Einwilligung auf einem genannten Zweck und sollen die Daten später zu einem anderen Zweck verarbeitet werden, so ist es zwingend erforderlich, eine Einwilligung des betroffenen auch für den neuen Zweck einzuholen.

Der Verein als Verantwortlicher für die Datenverarbeitung muss sich somit immer vor Augen führen, dass er nicht nur die datenschutzrechtlichen Grundsätze einhält, sondern deren Einhaltung (z. B. gegenüber der Aufsichtsbehörde) auch nachweisen muss. Die Aufsichtsbehörde kann nämlich von dem Verantwortlichen verlangen, dass er mittels geeigneter Dokumentationen nachweisen kann, welche personenbezogener Daten von Mitarbeitern, Mitgliedern, Lieferanten etc. er verarbeitet, auf welcher Rechtsgrundlage er dies konkret macht, für welchen Zweck er die Daten verwendet und wie lange er diese Daten speichert.

6. Auftragsverarbeitung

Häufig werden Dienstleister zur Erledigung der Aufgaben des Vereins eingeschaltet, die für den Verein z. B. die EDV-Anlagen pflegen und warten, die Buchhaltung erledigen oder Veranstaltungen für den Verein durchführen. Wenn externe Dienstleister solche Aufgaben für den Verein übernehmen und bei der Erfüllung dieser Arbeiten mit personenbezogenen Daten des Vereins umgehen, so liegt grundsätzlich eine sogenannte „Auftragsverarbeitung“ vor.

Eine Auftragsverarbeitung liegt also immer dann gegeben, sobald der Verein als verantwortliche Stelle personenbezogene Daten an jemand außerhalb des Vereins weitergibt oder dem externen Dienstleister ermöglicht, einen Einblick auf die eigene Datenverarbeitung und / oder personenbezogene Daten (z. B. im Rahmen der Pflege der Vereins-IT) ermöglicht.

Sofern der Verein einen Auftragsverarbeiter einschalten möchte, muss vorher geprüft werden, ob dieser Auftragsverarbeiter hinreichend gewährleisten kann, dass die Verarbeitung bei ihm im Einklang mit den datenschutzrechtlichen Vorschriften erfolgt. Aus diesem Grunde ist auch ein Vertrag zwischen dem Verein als Verantwortlichen und dem externen Dienstleister als Auftragsverarbeiter zu schließen. Dieser Vertrag hat insbesondere das Weisungsrecht des Verantwortlichen gegenüber dem Auftragsverarbeiter zum Inhalt und schreibt fest, welche Tätigkeiten der Auftragsverarbeiter durchführen soll, inwiefern der Auftragsverarbeiter zur Vertraulichkeit und Einhaltung der Sicherheit der Verarbeitung personenbezogener Daten verpflichtet ist und was mit den Daten zum Beispiel nach Abschluss der Auftragsverarbeitung geschehen soll.

Wichtig ist ebenfalls, dass der Verein sich von dem Auftragsverarbeiter umfangreiche Kontrollrechte einräumen lässt. So muss es dem Auftraggeber beispielsweise möglich sein, dass er Kontrollen vor Ort bei dem Auftragsverarbeiter durchführt. Die Kontrollrechte stehen dem Verein selbst dann zu, wenn der Auftragsverarbeiter seine Arbeiten in Heimarbeit durchführen sollte. In diesem Fall hätte der Auftraggeber selbst das Recht, seine Kontrollrechte mittels Zutrittsrechts in der Privatwohnung des Auftragsverarbeiters durchzuführen.

7. Datenschutz und IT-Sicherheit

Für die Sicherheit seiner eigenen IT ist jeder Verein selbst verantwortlich. Neben der Vergabe von einzelnen Zugriffsberechtigungen und z. B.l der Verschlüsselungen von Backups auf externe Datenträgern (Festplatten, USB-Sticks, Server) ist auch darauf zu achten, dass Zugangsdaten und Passwörter nicht an Dritte weitergegeben oder gar auf einem Zettel am Monitor befestigt werden. Bevor eine E-Mail versendet wird, ist unbedingt darauf zu achten, ob der richtige Empfänger im Adressfeld steht. Denn durch entsprechende Verwechslungen können vertrauliche Informationen unbefugten dritten Personen zur Kenntnis gelangen.

8. Datenschutzbeauftragter

a. Allgemeines

Der Datenschutzbeauftrage im Unternehmen oder Verein darf nicht mit dem / der Landesbeauftragten für den Datenschutz (Behörde) verwechselt werden. Bei den / der Landesbeauftragen für den Datenschutz handelt es sich um staatliche Aufsichtsbehörden.

Strickt davon zu trennen ist der Datenschutzbeauftragte des Vereins, der den Verein bei der internen Kontrolle zu allen Fragen des Datenschutzes unterstützt.

Zu den Aufgaben des internen Datenschutzbeauftragten gehören nach den Bestimmungen der DSGVO insbesondere folgende Tätigkeiten:

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten hinsichtlich ihrer Pflichten nach datenschutzrechtlichen Vorschriften;
- Überwachung der Einhaltung der gesetzlichen Datenschutzvorschriften;
- Zusammenarbeit mit der Aufsichtsbehörde und deren Ansprechpartner;
- Beratung betroffener Personen.

Der Verantwortliche hat die Kontaktdaten des Datenschutzbeauftragten der Aufsichtsbehörde mitzuteilen. Die meisten Aufsichtsbehörden stellen für diese Meldung ein Online-Formular zur Verfügung. Soweit dieses noch nicht der Fall sein sollte, sind die Kontaktdaten des Datenschutzbeauftragten der Behörde zum Beispiel per E-Mail mitzuteilen.

b. Pflicht zur Bestellung eines Datenschutzbeauftragten

Für jeden Verein stellte sich die Frage, ob überhaupt die Verpflichtung besteht, einen eigenen Datenschutzbeauftragten zu benennen. Die Verpflichtung zu Benennung eines internen Datenschutzbeauftragten besteht grundsätzlich dann,

- wenn in dem Verein mindestens 10 Personen damit beschäftigt sind, personenbezogene Daten automatisiert zu verarbeiten oder
- wenn die Kerntätigkeit des Vereins in der Verarbeitung von Gesundheitsdaten, genetischen Daten, Daten über politische Meinungen, religiöse Daten, Daten der Gewerkschaftszugehörigkeit oder Daten über strafrechtliche Verurteilungen oder Straftaten besteht.

Bei der Frage, ob mindestens 10 Personen beschäftigt sind, die personenbezogene Daten automatisiert verarbeiten, werden die Personen nach Köpfen gezählt. Es werden also auch Teilzeitkräfte oder Praktikanten sowie ehrenamtliche Mitarbeiter genauso wie Vollzeitbeschäftigte als jeweils eine Person berechnet. Sollte die Summe aller entsprechenden Personen also unter 10 liegen, so ist der Verein zur Benennung eines Datenschutzbeauftragten nicht verpflichtet.

Eine Ausnahme hiervon wird nur dann gemacht, wenn die Kerntätigkeit des Vereins in der Verarbeitung der oben beschriebenen personenbezogenen Daten zum Inhalt hat. In diesem Falle müsste also ein Datenschutzbeauftragter unabhängig von der Anzahl der Personen benannt werden. Die Zahl der Beschäftigten spielt in diesem Falle keine Rolle. Diese Ausnahme trifft jedoch auf die meisten Vereine nicht zu. Denn die Ausnahme gilt zum Beispiel dann nicht, wenn der Verein für alle Beschäftigten Religionsdaten speichert, um festzustellen, ob sie der Kirchensteuerpflicht unterliegen. Diese Daten sind nämlich für die eigentliche Tätigkeit des Vereins nicht erforderlich und somit keine Kerntätigkeit im Sinne des Gesetzes.

Sofern der Verein einen Datenschutzbeauftragten benennen muss, so ist es ihm freigestellt, ob er einen internen (Mitarbeiter) oder externen Datenschutzbeauftragten benennt. Wichtig ist, dass zum Beispiel der Vorstand eines Vereins oder der IT-Beauftragte nicht Datenschutzbeauftragter werden kann, da hier Interessenkonflikte vorprogrammiert sind und sich die entsprechenden Personen im Endeffekt selbst kontrollieren müssten.

Besteht die Verpflichtung zur Benennung eines Datenschutzbeauftragten, so ist es nicht zwingend aber stets zu empfehlen, dass sowohl der interne als auch der externe Datenschutzbeauftragte mit schriftlichem Vertrag bestellt wird.

9. Rechte der betroffenen Personen

Wie bereits dargelegt, schützt die DSGVO die Rechte und Freiheiten der betroffenen Personen und deren Recht auf Schutz ihrer personenbezogenen Daten. Die DSGVO sieht zum Zwecke der Erreichung dieses Schutzes zahlreiche Betroffenenrechte vor, die diese in die Lage versetzen sollen, die Informationen zu erhalten, zu welchem Zwecke der Verantwortliche welche personenbezogenen Daten des Betroffenen gespeichert hat und wie er sie nutzt bzw. verarbeitet.

Wichtig ist zu wissen, dass – egal ob die Datenverarbeitung auf einer Einwilligung oder sonstigen gesetzlichen Grundlage beruht – der Betroffene im Vorfeld oder zum Zeitpunkt der (ersten) Datenerhebung über die Zwecke der Verarbeitung seiner personenbezogener Daten informiert werden und er auch während der Datenverarbeitung diverse Informationen auf Anfrage unentgeltlich erhalten muss.

Aus diesem Grunde ist somit stets erforderlich, dass die Homepage eines Vereins eine Datenschutzerklärung vorhält und auch im Rahmen eines Mitgliedsantrags in Papierform der Betroffene umfangreiche Informationen über die Verarbeitung seiner personenbezogenen Daten und seiner diesbezüglichen Rechte erhält.

Deshalb liegt es auch bereits im eigenen Interesse des Vereins, dass er ein vollständiges und aktuelles Verzeichnis über Verarbeitungstätigkeiten (siehe oben) erstellt und regelmäßig pflegt. Denn daraus kann der Verein ersehen, welche Daten in welchem Bereich innerhalb des Vereins verarbeitet werden. Der Verein ist dadurch in der Lage, diese Daten schnell und vollständig zusammen zu führen, um dem Betroffenen dann eine vollständige Auskunft zeitnah erteilen zu können. Sollte sich ein Betroffener bei der Aufsichtsbehörde beschweren, weil der Verein seinem Auskunftsverlangen nicht oder nicht vollständig (Frist grundsätzlich innerhalb eines Monats) nachgekommen ist, so bliebe der Aufsichtsbehörde letztendlich auch nichts anderes übrig, den Verein zur Einhaltung der gesetzlichen Verpflichtungen anzuhalten und gegebenenfalls Sanktionen (Bußgeld) gegen den Verein zu verhängen. Jeder Verein sollte sich somit mit den Rechten der Betroffenen beschäftigen, damit er auf etwaige Auskunftsersuche vorbereitet ist und somit relativ leicht etwaige Sanktionen der Aufsichtsbehörde vermieden werden können.

Zu den wichtigsten betroffenen Rechten gehören:

a. Recht auf (vorherige) Information

Sofern die Datenerhebung direkt bei der betroffenen Person erfolgt, so muss der Verein wegen des Transparenzgebots im Rahmen jeder Datenverarbeitung zum Zeitpunkt der Datenerhebung eine entsprechende datenschutzrechtliche Unterrichtung gegenüber dem Betroffenen vornehmen. Der Verein muss also z. B. bei der Verwendung jedes Formulars, mit welchem er personenbezogene Daten erhebt (offline wie online), eine entsprechende Information bereitstellen und insbesondere auf folgende Punkte hinweisen:

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters (Vorstand des Vereins);
- Kontaktdaten des Datenschutzbeauftragten (sofern bestellt);

- Zwecke der Verarbeitung (möglichst einzelne Aufzählung);
- Rechtsgrundlage der einzelnen Verarbeitungsvorgänge;
- Empfänger oder Kategorien von Empfängern (z.B. Weitergabe personenbezogener Daten an eine Versicherung, an den Dachverband, an alle Vereinsmitglieder);
- Transfer der Daten in Drittländer (außerhalb der EU, z.B. bei Mitgliederverwaltung in der Cloud);
- Speicherdauer der personenbezogenen Daten / Löschfristen;
- Belehrung über Betroffenenrechte (z. B. Auskunft, Berichtigung, Löschung, Widerspruchsrecht gegen Verarbeitung – siehe unten);
- Hinweis auf jederzeitiges Widerrufsrecht einer Einwilligung;
- Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde.

Erhebt der Verein personenbezogene Daten auf andere Weise, also nicht bei der betroffenen Person selbst sondern über Dritte, so muss der Verein zusätzlich zu den zuvor genannten Punkten über die Quelle der Daten und die Kategorie der von dort übermittelten Daten informieren.

b. das Recht auf Berichtigung und Löschung

Der Anspruch auf Berichtigung ist selbstverständlich und bezieht sich auf die Korrektur falscher Daten (zum Beispiel die Korrektur einer neuen Adresse des Mitglieds).

Der Anspruch auf Löschung besteht dann, wenn eine weitere Speicherung der personenbezogenen Daten zur Erfüllung des ursprünglichen Zwecks nicht mehr erforderlich ist, der Betroffene seine Einwilligung zur Datenverarbeitung widerrufen hat oder es keine andere Rechtsgrundlage für die weitere Speicherung der Daten gibt. Zu beachten ist jedoch, dass das Recht zur Löschung personenbezogener Daten nicht per se besteht. Es können nämlich zum Beispiel gesetzliche Aufbewahrungspflichten der sofortigen Löschung entgegenstehen. So gibt es diverse Aufbewahrungspflichten nach steuerrechtlichen, handelsrechtlichen oder satzungsrechtlichen Vorschriften. Es ist somit unabdingbar, dass der Verein auch die diversen Aufbewahrungs- und Löschungsfristen einzelner Daten kennt, denen er unterworfen ist.

c. Recht auf Auskunft

Das Recht auf Auskunft soll den Betroffenen ermöglichen, überhaupt zu erfahren, welche personenbezogenen Daten bei dem Verantwortlichen gespeichert sind. Eine Auskunft ist nicht automatisch zu erteilen, sondern nur dann, wenn der Betroffene einen Antrag bei dem Verein stellt. Zu beachten ist in diesem Zusammenhang, dass sich der Verantwortliche stets darüber zu vergewissern hat, dass der Antragsteller auch derjenige ist, für den er sich vorgibt zu sein. Ansonsten bestünde die Gefahr, dass personenbezogene Daten an unbefugte Dritte weitergegeben werden.

Das Recht auf Auskunft beinhaltet insbesondere folgende Informationen: den Zweck der Verarbeitung, die Kategorien der personenbezogenen Daten, die (Dritt-) Empfänger der Daten, die geplante Speicherdauer, den Hinweis auf sonstige Betroffenen-Rechte und die Beschwerdemöglichkeit bei einer Aufsichtsbehörde.

Im kleineren Vereinen, in denen die elektronische Speicherung der Daten auf einem PC oder einem kleinen Netzwerk erfolgt, ist es in der Regel relativ leicht, den Anspruch auf Auskunft zu erfüllen. Die Auskunft muss jedoch - egal wie groß der Aufwand sein sollte - stets kostenlos zur Verfügung gestellt werden.

d. Recht der Datenübertragbarkeit.

Das Recht auf Datenübertragbarkeit regelt den Anspruch, dass die betroffene Person ihre personenbezogenen Daten, die sie einem Verantwortlichen mitgeteilt hat, in einem gängigen Format zur Verfügung gestellt bekommt oder auch an einen anderen Verantwortlichen (zum Beispiel einen anderen Verein) weitergeben lassen kann. Wichtig ist, dass das Recht der Datenübertragbarkeit nur solche Daten betrifft, die die betroffene Person selbst übermittelt hat und nicht etwaige Erkenntnisse daraus umfasst, die ein Verantwortlicher im Zusammenhang mit diesen Daten erhalten hat. So ist ein Verein zum Beispiel auf Verlangen des Betroffenen verpflichtet, seine Daten (Name, Anschrift, E-Mail Adresse etc.) an einen anderen Verein in einem elektronischen Format zu übermitteln. Das beinhaltet jedoch nicht die Verpflichtung, weitere Daten des Betroffenen (zum Beispiel an welchen Veranstaltungen er teilgenommen hat) dem anderen Verein zu übermitteln.

e. Widerspruch gegen die Verarbeitung

Neben dem Recht auf jederzeitigen Widerruf seiner Einwilligung in die Verarbeitung personenbezogener Daten hat der Betroffene auch das Recht, wenn

der Verein sich als Rechtfertigung für seine Verarbeitung auf sein berechtigtes Interesse (Interessenabwägung) beruft, dieser Verarbeitung mit Wirkung für die Zukunft zu widersprechen. Die betroffene Person muss hierfür jedoch plausible Gründe nennen. Der Verantwortliche darf dann in Kenntnis dieser Gründe eine Verarbeitung der personenbezogenen Daten nur fortsetzen, wenn der Verein zwingende schutzwürdige eigene Gründe nachweisen kann, die die Interessen des Betroffenen an seinen Widerspruch überwiegen.

Bezieht sich der Widerspruch dagegen nur auf Werbemaßnahmen (zum Beispiel die Übermittlung eines Newsletters), muss die betroffene Person keine Gründe vortragen. Der Verantwortliche ist in diesem Fall stets verpflichtet, in Zukunft auf die Werbemaßnahmen gegenüber der betroffenen Person zu verzichten.

10. Sanktionen und Haftung bei Datenschutzverstößen

Die DSGVO sieht bei Verstößen gegen datenschutzrechtliche Bestimmungen recht hohe Bußgelder vor, die von den Aufsichtsbehörden verhängt werden können. Außerdem sieht die DSGVO Schadensersatzansprüche der betroffenen Personen gegenüber dem Verantwortlichen im Falle von Datenschutzverstößen vor.

11. Einzelheiten im Umgang mit personenbezogenen Daten im Verein

a. Nutzung von Mitgliederdaten

Innerhalb des Vereins sind die Aufgaben oft abgegrenzt und bestimmten Funktionsträgern zugewiesen. Die Satzung oder die Geschäftsordnung kann beispielsweise bestimmen, welche Person für welchen Bereich im Verein zuständig ist. Für den Umgang mit Mitgliederdaten gilt, dass jeder Funktionsträger grundsätzlich nur die für die Erfüllung seiner Aufgaben erforderlichen Mitgliederdaten verarbeiten, nutzen und kennen darf. Der Vorstand darf auf alle Mitgliederdaten zugreifen, wenn er diese zur Aufgabenerledigung benötigt. Auch müssen der Geschäftsstelle alle Mitgliederdaten in der Regel für die Mitgliederverwaltung und -betreuung zur Verfügung stehen. Für den Schatzmeister reicht es indessen grundsätzlich aus, wenn er die für den Einzug der Mitgliedsbeiträge relevanten Angaben (Name, Anschrift und Bankverbindung) und die Zahlungseingänge hinsichtlich einzelner Mitglieder kennt. Dabei dürfen die Daten wie bereits dargelegt grundsätzlich nur zur Verfolgung des Vereinszwecks bzw. zur Betreuung und Verwaltung von Mitgliedern genutzt werden. Nur ausnahmsweise ist es möglich, diese Daten für sonstige berechtige Interessen

des Vereins oder Dritter zu nutzen, vorausgesetzt, dem stehen keine schutzwürdigen Interessen der Vereinsmitglieder entgegen.

b. Nutzung von Daten Dritter

Daten Dritter, etwa Ansprechpartner von Lieferanten und Veranstaltern oder Daten von Besuchern und Gästen, dürfen gespeichert und genutzt werden, wenn diese in die Verarbeitung eingewilligt haben oder die Verarbeitung für die Begründung / Durchführung eines Vertrags mit diesen Personen erforderlich ist oder der Verein ein berechtigtes Interesse daran hat und nicht erkennbar ist, dass dem schutzwürdigen Interessen des Betroffenen entgegenstehen (z. B. bei der Versendung von Einladungen an externe Gäste). 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 Verarbeitung zulässig. Denn jeder Betroffene darf sich in der Regel darauf verlassen, dass der Verein seine Daten nur im Rahmen seiner Einwilligung bzw. der Zwecke des Vertragsverhältnisses oder berechtigten Interesses (z. B. Einladung zu Veranstaltungen) nutzt.

c. Nutzung der Daten für Werbung und Spendenaufrufe

Der Verein darf Daten seiner Vereinsmitglieder für eigene Spendenaufrufe und für eigene Werbung zur Erreichung der Ziele und Zwecke des Vereins nutzen. Die Nutzung von Mitgliederdaten für die Werbung Dritter ist ohne die vorherige Einwilligung des einzelnen Mitglieds grundsätzlich allerdings nicht zulässig.

Daten Dritter, die dem Verein bekannt sind, etwa von Personen, die regelmäßig an Veranstaltungen als Gäste teilnehmen, darf der Verein für Werbezwecke nutzen, wenn diese entweder darin eingewilligt haben oder der Verein berechtigte Interessen an der Nutzung zu Werbezwecken hat und keine entgegenstehende Interessen des Dritten überwiegen. Informiert der Verein transparent und umfassend über eine vorgesehene Nutzung der Daten, erwartet die betroffene Person auch grundsätzlich, dass ihre Daten entsprechend genutzt werden.

Wichtig ist, dass die von der Werbung betroffene Person ein jederzeitiges Widerspruchsrecht hinsichtlich der Nutzung ihrer Daten zu Werbezwecken hat. Sollte also ein Betroffener von seinem Widerspruchsrecht Gebrauch machen, darf der Verein die Daten zukünftig nicht mehr für Werbezwecke - egal in welcher Form - verwenden.

Achtung: Telefonische Werbung und Werbung per E-Mail gegenüber Dritten (keine Vereinsmitglieder) ist ohne ausdrückliche vorherige Einwilligung des Betroffenen nicht zulässig!!!

Sollte der Verein einen externen Dienstleister damit beauftragen, für den Verein die Werbemaßnahmen durchzuführen (z. B. Druckereien, Werbeagentur etc.) so muss ein Auftragsverarbeitungsvertrag (siehe oben) mit diesen Unterhemen abgeschlossen werden.

d. Nutzung der Daten für Vereinsmitteilungen, -blätter und Aushänge

Das „Schwarze Brett“ eines Vereins und die Vereinszeitung sind in erster Linie für Vereinsmitglieder bestimmt. Es kann jedoch nicht ausgeschlossen werden und ist zum Teil auch beabsichtigt, dass auch Fremde die Anschlagtafeln oder das Mitteilungsblatt des Vereins lesen (können).

Personenbezogene Daten dürfen in diesem Zusammenhängen zunächst auch nur offenbart werden, wenn es für die Erreichung des Vereinszwecks erforderlich ist. Persönliche Nachrichten über einzelne Mitglieder mit einem konkreten Bezug zum Verein wie Eintritte, Austritte, oder runde monatliche Geburtstage (nicht aber das Geburtsdatum) und Jubiläen können veröffentlicht werden, wenn dem Verein keine schutzwürdigen Belange des Betroffenen bekannt sind, die dem entgegenstehen. Es ist aber zu empfehlen, dass Vereinsmitgliedern beim Eintritt in den Verein mitgeteilt wird, welche Daten entsprechend veröffentlicht werden sollen.

Informationen aus dem persönlichen Lebensbereich eines Vereinsmitglieds (z.B. Eheschließungen, Geburt von Kindern, Abschluss von Schul- und Berufsausbildungen) dürfen allerdings nur dann veröffentlicht werden, wenn das einzelne Mitglied ausdrücklich sein Einverständnis hierfür erklärt hat.

Das gilt auch für die Bekanntgabe der Höhe der Spende eines Vereinsmitgliedes. Spender außerhalb des Vereins dürfen nur mit deren Einverständnis öffentlich bekannt gegeben werden, weil ihr Interesse an vertraulicher Behandlung das Vereinsinteresse an einer Veröffentlichung in der Regel überwiegt.

Die Funktionsträger eines Vereins dürfen auch ohne ausdrückliche Einwilligung mit ihren funktionsbezogenen Kontaktdaten in das Internet auf der Homepage des

Vereins eingestellt werden. Der Verein sollte daher für diese Zwecke entsprechende eigene Kommunikationsdaten einrichten. Die privaten Adressen (E-Mail, postalisch, Telefon) der Funktionsträger dürfen hingegen nur mit deren Einverständnis veröffentlicht werden.

Veröffentlichungen über Jahreshauptversammlungen oder Ergebnisse von Vorstandswahlen sind aufgrund des berechtigten Interesses des Vereins wegen der Wichtigkeit dieser Ereignisse für das Vereinsleben ebenfalls zulässig.

Komplette Listen von Vereinsmitgliedern sollten nur den Vereinsmitgliedern gesondert (z. B. in einer extra gedruckten Liste oder einem passwort-geschützten Mitgliederbereich der Internetseite des Vereins) zur Kenntnis gebracht und nicht für beliebige Dritte zur Einsicht veröffentlicht werden. Letzteres wäre grundsätzlich nur mit der Einwilligung jedes einzelnen Vereinsmitglieds in die Veröffentlichung seiner Daten erlaubt.

e. Nutzung Daten von Minderjährigen

Die Erhebung und Verarbeitung von personenbezogenen Daten Minderjähriger unterliegen aufgrund eines erhöhten schutzwürdigen Interesses dieser Personen stets erhöhten datenschutzrechtlichen Anforderungen.

Minderjährige können wirksame Einwilligungen in die Datenverarbeitung selbst immer erst dann erteilen, wenn sie auch in der Lage sind, die Konsequenzen der Verwendung ihrer Daten vollständig zu übersehen und zu verstehen. Die DSGVO sieht in Art 8 Abs. 1 vor, dass die datenschutzrechtliche Einwilligung von Minderjährigen unter 16 Jahren generell nur dann wirksam ist, wenn diese Einwilligung durch den Träger der elternlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.

Kann die Einsichtsfähigkeit eines Minderjährigen über 16 Jahre indessen im konkreten Fall nichts zweifelsfrei festgestellt werden, ist die Verarbeitung personenbezogener Daten ebenfalls nur mit einer Einwilligung der gesetzlichen Vertreter zulässig. Es ist daher zu empfehlen, bei Personen, die das 18. Lebensjahr noch nicht vollendet haben, zur Sicherheit stets eine Einwilligung der gesetzlichen Vertreter hinsichtlich der Erhebung und Verarbeitung von personenbezogenen Daten einzuholen (das gilt insbesondere dann, wenn der Verein Fotos von Minderjährigen im Internet veröffentlichen möchte).

f. Veröffentlichung von Fotos im Internet

Vereine wollen häufig Fotos von Vereinsfeiern, anderen Veranstaltungen oder auch von Mitgliedern oder Mitarbeitern, auf denen diese abgebildet sind, in das Internet stellen.

Hierbei stellt sich stets die Frage, ob dieses ohne konkrete Einwilligung der betroffenen Person(en) zulässig ist.

Achtung: Ein freundliches Lächeln oder Winken in die Kamera während einer Vereinsfeier kann zwar eine stillschweigende bzw. schlüssige Einwilligung in die Aufnahme des Fotos als solches darstellen. Zu beachten ist jedoch, dass dieses in der Regel noch keine wirksame Einwilligung in die freie Veröffentlichung des Fotos im Internet darstellen muss.

Rechtsgrundlage für die Veröffentlichung von Fotos im Internet bildet zum Beispiel das Kunsturhebergesetz (KUG), welches das Recht am eigenen Bild regelt (presserechtliche Besonderheiten sollen hier nicht näher behandelt werden). Auch nach dem KUG dürfen Bildnisse nur mit Einwilligung des Abgebildeten öffentlich verbreitet werden. Ausnahmen von der Einwilligung nach dem KUG gelten jedoch bei

- Bildnissen aus dem Bereich der Zeitgeschichte;
- Bildern, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen oder
- Bildern von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben.

Personen der Zeitgeschichte sind Personen, die aufgrund ihrer Stellung, Taten oder Leistungen außergewöhnlich herausragen (z. B. Politiker oder Spitzensportler), sowie Menschen, die in Zusammenhang mit einem zeitgeschichtlichen Ereignis in den Blick der Öffentlichkeit geraten. Zudem müssen diese Personen im Zusammenhang mit ihrer „öffentlichen“ Tätigkeit abgebildet werden. Sofern diese Personen im privaten Bereich fotografiert werden, bedarf die Veröffentlichung derartiger Aufnahmen auch von diesen Personen deren Einwilligung.

Eine weitere Ausnahme bilden Aufnahmen von nur beiläufig abgebildeten Personen als „Beiwerk“, z.B. neben einem Denkmal, Gebäude oder einer Naturlandschaft.

Außerdem ist bei Veranstaltungen in öffentlichen Räumen grundsätzlich für die fotografische Abbildung der Teilnehmer und Zuschauer keine Einwilligung erforderlich (z. B. bei Vereinsumzügen). Bei Fotos und Filmaufnahmen von öffentlichen Vorgängen muss es sich jedoch um Aufnahmen handeln, bei denen grundsätzlich die Ansammlung von Menschen und nicht die einzelne Person im Vordergrund steht.

Gibt es keinen Vertrag mit der abgebildeten Person oder sonstige Ermächtigungsgrundlage, kann das Erfordernis einer Einwilligung in die Veröffentlichung eines Fotos oder Filmaufnahme z. B. auch dann entfallen, wenn die Verarbeitung gem. der DSGVO zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist und die Interessen der abgebildeten Person diesem Interesse nicht überwiegen. Das bedeutet, sofern die betroffene Person zum Zeitpunkt der Anfertigung der Aufnahmen und angesichts deren Umstände vernünftigerweise absehen kann, dass die Aufnahmen und deren Verarbeitung zu bestimmten Zwecken erfolgen wird (z. B. Berichterstattung im Vereinsblatt oder auf der Homepage des Vereins), dürfte den Interessen des Vereins als Verantwortlichen in der Regel der Vorrang einzuräumen sein. Wobei zu erwähnen ist, dass es hier auch Stimmen gibt, die wegen der weltweiten Abrufmöglichkeit eines Fotos im Internet die Interessen des Betroffenen stets überwiegen lassen und somit eine entsprechende Einwilligung in die jeweilige Veröffentlichung unabdingbar sein soll.

Leider ist im Zuge des Inkrafttretens der DSGVO hier vieles noch ungeklärt bzw. auslegungsbedürftig. Ob die Rechtsprechung zur alten Rechtslage uneingeschränkt herangezogen werden kann, ist ebenfalls noch nicht vollständig geklärt.

Es ist somit derzeit grundsätzlich zu empfehlen, möglichst von jeder Person, die auf einem Foto abgebildet ist und dieses Foto z. B. im Internet veröffentlicht werden soll, eine entsprechende Einwilligung einzuholen.

Das ist jedoch in der Praxis nicht immer umsetzbar. Es kann in der Regel auf Vereinsfeiern oder sonstigen Veranstaltungen, zu denen eine Vielzahl von Personen eingeladen oder die sogar der allgemeinen Öffentlichkeit zugänglich sind, eine Einwilligungserklärung von jeder einzelnen Person gar nicht, sehr schwer oder nur überaus umständlich eingeholt werden. In diesem Falle sollte in jedem Fall am Eingang zu der Veranstaltung im gut sichtbaren Bereich ein Hinweisschild mit beispielsweise folgendem Mindestinhalt angebracht werden:

Beispiel:

Foto- und Filmaufnahmen

Während unserer Veranstaltungen werden von uns zu Zwecken der Öffentlichkeits- und Vereinsarbeit Foto- und Filmaufnahmen gemacht.

Name, Kontaktdaten des Vereins