Vereine fit machen für den neuen Datenschutz

Handout zum Seminar
zusammengestellt von Hans-Jürgen Fuchs

Die Herausforderungen der Europäischen Datenschutzverordnung meistern!

Die Einführung der Europäischen Datenschutzverordnung hat einigen Wirbel verursacht, nicht nur bei Firmen, sondern auch bei den Ehrenamtlichen im Land. Die Fortbildung „Vereine fit machen für den neuen Datenschutz" richtet sich an Verantwortliche in kleinen und mittleren Vereinen, die die Herausforderung der neuen europäischen Datenschutzverordnung annehmen wollen.

Der Referent, Hans-Jürgen Fuchs, ist seit vielen Jahren Datenschutzbeauftragter, u.a. an mehreren Volkshochschulen und Musikschulen
Er ist zudem Vorsitzender eines großen Vereins und deshalb mit den Notwendigkeiten und Zwängen in der Vereinsführung bestens vertraut.

Inhalt

Vorab ...

Ich bin kein Anwalt. Diese Ausführungen sind keine zivilrechtliche Beratung! Bitte beachten Sie, dass es Ihre Aufgabe als Nutzer des Handouts ist, die zivilrechtliche Bewertung dieser Ausführungen vorzunehmen.

Grundlegendes

Was ist die DSGVO?

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen, Vereine und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden. Im Gegensatz zur vorher geltenden Richtlinie, die von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden musste, gilt die Datenschutz-Grundverordnung unmittelbar in allen EU-Mitgliedstaaten. In Deutschland wird die DSGVO durch das BDSG (neu) 2017 umgesetzt, das das bisherige Bundesdatenschutzgesetz komplett ersetzt. Es gilt ab dem 25. Mai 2018

Was sind personenbezogene Daten?

„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind; (Art. 4 lit 1, DSGVO)

Besonders schützenswerte Daten

„Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

Absatz 1 gilt nicht in folgenden Fällen: ... (DSGVO Art. 9 lit 1)

„... es sei denn, die Verarbeitung ist in den in dieser Verordnung dargelegten besonderen Fällen zulässig, ... unter anderem bei ausdrücklicher Einwilligung der betroffenen Person oder bei bestimmten Notwendigkeiten, insbesondere wenn die Verarbeitung im Rahmen rechtmäßiger Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, die sich für die Ausübung von Grundfreiheiten einsetzen.” (DSGVO Erwägungsgrund 51).

Rechte der Betroffenen

Die Betroffenen sollen wissen, wer welche Daten zu welchem Zweck über sie erhebt und so in die Lage versetzt werden, die Datenerhebung, -verarbeitung bzw. -nutzung zu prüfen. Diese Anforderung kann nur dann erfüllt werden, wenn der Verantwortliche im Verein die Betroffenen ausreichend über die Datenverarbeitungsvorgänge informiert. Um die Betroffenen informieren zu können, müssen im Verein wiederum die Sachverhalte ermittelt werden, in welchen Informationspflichten bestehen (beispielsweise Anmeldung zum Newsletter, Weitergabe von Daten ...).

Die Betroffenen einer Datenverarbeitung haben folgende Rechte:

- Informationsrecht
- Auskunfts- und Widerspruchsrecht
- Recht auf Berichtigung, Löschung und Einschränkung
- Recht auf „Datenübertragbarkeit“. Dieses neue Instrument soll dem Einzelnen einen Anspruch bieten, seine personenbezogenen Daten von einer verantwortlichen Stelle auf die andere zu übertragen. Wie das geregelt werden soll ist noch unklar und umstritten.

Die wichtigsten Artikel der Europäischen Datenschutz Grundverordnung

Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a. auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
b. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
c. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
e. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
f. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
b. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
c. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
d. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
e. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
f. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

Informationspflichten des Vereins

Jeder Verein hat aus Gründen der Transparenz umfassend darüber zu informieren, wie personenbezogene Daten verarbeitet werden. Hierfür hat der Verein zum Zeitpunkt der Erhebung (z.B. im Mitgliedsantrag) sämtliche Informationspflichten des Art. 13 DSGVO mitzuteilen. Art. 13 DSGVO regelt die Informationspflicht bei der Erhebung von personenbezogenen Daten, der auch Vereine unterworfen sind. Hier reicht es nicht, die Informationen nur auf der Vereinswebsite zu veröffentlichen.

Bei Bestandsmitgliedern lässt sich die Pflicht durch eine Information in der Mitgliederzeitschrift oder als Anlage zu einem Jahresbrief/zur Einladung zur Jahreshauptversammlung erfüllen.

Bei Neumitgliedern sollte die Information mit dem Mitgliedsantrag erfolgen ... mit einer Bestätigung, dass das neue Mitglied davon Kenntnis genommen hat. Sinnvoll ist, dass Antrag und Info zusammen ausgegeben werden (z.B. Vorder-/Rückseite). Mehr dazu weiter unten unter „Mitgliedsantrag mit Datenschutzerklärung".

Vereinsorganisation

Wer ist der Verantwortliche?

Verantwortung des für die Verarbeitung Verantwortlichen (Art. 24 DSGVO)

1. Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.
2. Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

Die Erarbeitung von Strategien zum Datenschutz ist Aufgabe der/des Verantwortlichen im Verein, nicht die des Datenschutzbeauftragten.

Benötigt der Verein einen Datenschutzbeauftragten?

Mit der DSGVO gibt es erstmals eine europaweite Pflicht zur Bestellung eines Datenschutzbeauftragten (Art. 37 ff.). Diese ist verpflichtend

- sofern ein Verein einer Tätigkeit nachgeht, die aus Datenschutz-Sicht einer besonderen Kontrolle bedarf (Krankenhaus, strafrechtliche Dinge),
- wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.

Darüber hinaus kann jeder Verein einen Datenschutzbeauftragten freiwillig bestellen.

Laut §38 BDSG (neu) muss ein Datenschutzbeauftragter bestellt werden, wenn mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. „Ständig" beschäftigt ist eine Person, wenn sie für diese Aufgabe auf längere Zeit vorgesehen ist und sie entsprechend wahrnimmt. Irrelevant ist, ob die Person beim Verein beschäftigt oder ehrenamtlich tätig ist. Die Aufgabe braucht auch nicht Hauptaufgabe der Person zu sein. Das Tatbestandsmerkmal „ständig" ist daher auch erfüllt, wenn die Aufgabe selbst nur gelegentlich anfällt, die betreffende Person sie aber stets wahrzunehmen hat.

Das heißt aber auch, dass ein Übungsleiter, der Anwesenheiten, Leistungsdaten, Kontaktdaten von Vereinsmitgliedern etc. aufnimmt, als Person, die ständig mit der Verarbeitung personenbezogener Daten beschäftigt ist, gilt. Folglich wird es kaum einen Sportverein geben, der keinen Datenschutzbeauftragten braucht!

Die vorsätzliche oder fahrlässige Versäumnis, einen betrieblichen Datenschutzbeauftragten zu bestellen, diesen nicht in der vorgeschrieben Weise oder nicht rechtzeitig zu bestellen, stellt gemäß § 43 Abs. 1 Nr. 2 BDSG bereits heute eine Ordnungswidrigkeit dar, die mit einem Bußgeld belegt werden kann.

Der Datenschutzbeauftragte muss formell wirksam bestellt werden:

- Eine Bestellung muss schriftlich erfolgen.
- Die Bestellungsurkunde muss von beiden Parteien unterschrieben worden sein.
- Die Bestellung hat gesondert zu erfolgen, d.h. in einer eigenen Vereinbarung außerhalb eines beabsichtigten oder bestehenden Vertrages.
- Zudem muss die Bestellung eine Aufgabenbeschreibung enthalten, die Präzisierung der organisatorischen Stellung, sowie die Verpflichtung des Vereins, durch personelle und materielle Unterstützung die Arbeit des Datenschutzbeauftragten zu ermöglichen.

Der Verein muss die Kontaktdaten des Datenschutzbeauftragten veröffentlichen. Hierbei ist es ausreichend, wenn die E-Mail-Adresse des Datenschutzbeauftragten auf der Vereinshomepage frei zugänglich genannt wird. Nicht erforderlich ist die Kundgabe des Namens des Datenschutzbeauftragten.

Der Datenschutzbeauftragte ist der zuständigen Aufsichtsbehörde zu melden. Eine Meldung ist beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg online möglich: https://www.baden-wuerttemberg.datenschutz. de/dsb-online-melden.

Aufgaben und Pflichten des Datenschutzbeauftragten

Die Aufgaben und Pflichten des betrieblichen Datenschutzbeauftragten sind in Art. 39 DSGVO geregelt:

1. Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:
   a. Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften ...;
   b. Überwachung der Einhaltung dieser Verordnung, ... sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
   c. c. Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;
   d. Zusammenarbeit mit der Aufsichtsbehörde;
   e. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, ...

2. Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Um diesen Aufgaben und Pflichten nachkommen zu können, regelt die Datenschutz-Grundverordnung explizit, dass der Datenschutzbeauftragte „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen“ einzubinden ist (vgl. Art. 38 Abs. 1 DSGVO).

Fachliche Qualifikationen des Datenschutzbeauftragten

Näheres siehe ab S. 31 Punkt 7.1 der Orientierungshilfe „Datenschutz im Verein nach der DSGVO“ sowie in Kurzpapier Nr. 12 der Datenschutzkonferenz *(https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/01/DSK_KPNr_12_Datenschutzbeauftragter.pdf).*
Datenschutzbeauftragter sollte natürlich nicht der 1. Vorsitzende sein, um Interessenskonflikte zu vermeiden.

Datenschutzerklärungen für Ehrenamtliche

Ehrenamtliche, die mit Daten des Vereins in Kontakt kommen (Vorstand, Kassenführung, Angestellte oder Praktikanten ...) müssen eine Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO) unterschreiben.

Ein Muster finden Sie im Anhang.

Mitgliedsantrag mit Datenschutzerklärung

Wichtig ist, dass bereits der Mitgliedsantrag auf die spätere Verarbeitung der Daten hinweist. Was muss rein?

- Name/ Kontaktdaten des Verantwortlichen und ggf. seines Vertreters
- Kontaktdaten des Datenschutzbeauftragten, falls vorhanden
- Zwecke und Rechtsgrundlage der Verarbeitung
- Berechtigte Interessen i.S.d. Art. 6 Abs. 1 lit. f) DSGVO
- Empfänger oder Kategorien von Empfängern
- Absicht von Drittlandtransfer 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 der Datenschutz-Aufsichtsbehörde
- Pflicht zur Bereitstellung der Daten
- Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling (Schufa ...)

(Quelle: Datenschutz im Verein nach der DSGVO – Praxisratgeber, hrgg. durch den Landesbauftragten für den Datenschutz und Informationsfreiheit Baden-Württemberg)

Es ist nicht ausreichend, wenn der Verein die Datenschutzhinweise auf seine Webseite stellt und das Mitglied etwa bei Abschluss eines Mitgliedvertrages einfach darauf verwiesen wird, denn das widerspräche dem Gebot der leichten Zugänglichkeit (Art. 12 Abs. 1 S.1 DSGVO). Informationen sind so bereitzustellen, dass die betroffene Person sie im Zusammenhang mit der Datenerhebung ohne „Medienbruch" entgegen nehmen kann. Wird das Beitrittsformular also von Hand ausgefüllt, so sind dem Mitglied die Informationen in Schriftform vorzulegen. Dennoch ist es sinnvoll, die Informationen zusätzlich auf der Webseite zur Verfügung zu stellen, denn auf diese Weise können auch die Bestandsmitglieder Kenntnis hiervon erlangen.

Bei bereits erfolgten Datenerhebungen (von Altmitgliedern) nach dem BDSG sind die Informationspflichten des Art. 13 DSGVO nicht zu erfüllen bzw. nachzuholen. Hier ist eine Info in der Mitgliederzeitschrift oder als Anlage zu einem Jahresbrief/zur Einladung zur Jahreshauptversammlung sinnvoll.

Ein Muster für einen Mitgliedsantrag finden Sie im Anhang des Handouts.

Einwilligungserklärungen

(Basis: Datenschutz im Verein nach der DSGVO – Praxisratgeber, hrgg. durch den Landesbauftragten für den Datenschutz und Informationsfreiheit Baden-Württemberg)

Ein Verein darf auch ohne Einwilligung Daten erheben,

- wenn die für die Begründung und Durchführung des zwischen Mitglied und Verein durch den Beitritt zustande kommenden rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich sind (Art. 6 Abs. 1 lit. b) DSGVO) ... eine Vereinsmitgliedschaft ist ein Vertragsverhältnis.
- wenn er an der Datenverarbeitung ein überwiegendes berechtigtes Interesse hat (Art. 6 Abs. 1 lit. f) DSGVO).

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. Eine Einwilligung ist in diesem Fall nicht notwendig und auch nicht sinnvoll, denn sie könnte ja jederzeit widerrufen werden. Allerdings sind die Betroffenen in jedem Fall über die Datenerhebung zu informieren (siehe Informationspflicht).

In welchen Fällen ein Verein Daten aufgrund des Art. 6 Abs. 1 lit. b) DSGVO erheben darf, ist in der Orientierungshilfe „Datenschutz im Verein nach der DSGVO" *(https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf)* ausführlich dargelegt.

Nur für Datenverarbeitungen, die über die gesetzlich erlaubten Verarbeitungen hinausgehen, ist eine Einwilligung erforderlich. Dies sind Fälle, in denen die Verarbeitung der personenbezogenen Daten weder zur Durchführung des Mitgliedsvertrags noch aufgrund berechtigter Interessen des Vereins erforderlich sind.

In Betracht kommen insbesondere:

- Veröffentlichung von Fotos auf der Webseite des Vereins
- Veröffentlichung von Geburtsdaten/Jubiläen im Vereinsblatt/am schwarzen Brett
- Werbung von Dritten

Welche Form muss die Einwilligung haben?

Die DSGVO ermöglicht die Einwilligung schriftlich, elektronisch, mündlich oder sogar konkludent (ohne ausdrückliche Erklärung durch schlüssiges Verhalten abgegeben, d.h. die Willenserklärung wird aus den Handlungen des Erklärenden abgeleitet) abzugeben. Jedoch muss der Verein nachweisen können, dass die betroffene Person eingewilligt hat (Art. 7 Abs. 1 DSGVO). Deshalb sollten Einwilligungen schriftlich (d.h. mit eigenhändiger Unterschrift der betroffenen Person) eingeholt und aufbewahrt werden. Liegt von den der Bestandsmitgliedern bereits eine datenschutzkonforme Einwilligung vor, dann gilt diese weiter und muss nicht erneut eingeholt werden. Lediglich wenn es zu einer weitergehenden einwilligungspflichtigen Verarbeitung personenbezogener Daten kommen soll, ist eine neue Einwilligung notwendig.

Für jede Art der Datenverarbeitung ist eine gesonderte Einwilligung erforderlich. Daher sollte für jede ein gesondertes Formular verwendet werden. Auf jedem Formular ist genau anzugeben, welche Daten zu welchem Zweck verarbeitet werden.

> ***Ein Muster für die Einwilligung in der Veröffentlichung von Daten auf der Webseite des Vereins finden Sie im Anhang.***

Dokumentationspflicht

Der wesentliche Unterschied zwischen der neuen und der bisherigen Datenschutzordnung ist die Dokumentationspflicht. Auch Vereine müssen ihren Umgang mit dem Datenschutz schriftlich dokumentieren. Es nutzt also nichts, einer Aufsicht zu sagen: „aber das machen wir doch so!". **ACHTUNG: Was nicht dokumentiert ist, existiert für die Aufsichtsbehörden nicht!** Die erste zentrale Dokumentation ist das Verzeichnis der Verarbeitungstätigkeiten ...

Verzeichnis der Verarbeitungstätigkeiten

Aus dem früheren Verfahrensverzeichnis wurde in der DSGVO das Verzeichnis der Verarbeitungstätigkeiten (VVT), das der Verantwortliche für den Datenschutz führen muss. In diesem sind die wesentlichen Informationen zu Datenverarbeitungstätigkeiten zusammenzufassen. **Das Verzeichnis muss jederzeit und vollständig für die Aufsichtsbehörden vorgehalten werden, ansonsten droht ein Bußgeld.** Während das alte Verfahrensverzeichnis noch auf Antrag jedermann zugänglich zu machen war, besteht diese Pflicht bei Verzeichnissen von Verarbeitungstätigkeiten nur noch gegenüber den Aufsichtsbehörden. Unternehmen oder Einrichtungen mit weniger als 250 Mitarbeitern sind nach Art. 30 Abs. 5 DSGVO von der Führung eines Verzeichnisses befreit, außer

- die vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen (z.B. Scoring),
- **die Verarbeitung erfolgt nicht nur gelegentlich**
- oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 DSGVO (z.B. Gesundheitsdaten) bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 DSGVO.

In erster Linie die Ausnahme „die Verarbeitung erfolgt nicht nur gelegentlich", unterwirft eigentlich alle Vereine wieder der Pflicht, ein Verzeichnis zu führen, denn es genügt, wenn regelmäßig neue Mitglieder eingegeben oder ausgeschiedene gelöscht werden.

Im Verzeichnis müssen die wesentlichen Angaben zur Datenverarbeitung gemacht werden:

- Namen und die Kontaktdaten des für die Verarbeitung Verantwort-

lichen (ggf. auch Vertreter und Datenschutzbeauftragter)
- Zwecke der Verarbeitung
- Kategorien von betroffenen Personen und personenbezogenen Daten
- Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden (auch in Drittländern)
- Übermittlungen von Daten an ein Drittland oder an eine internationale Organisation
- Wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- Eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (TOMs, siehe unten).

Für kleinere Vereine kann eine tabellarische Form des Verzeichnis' völlig ausreichen. So empfiehlt der baden-württembergische Landesbeauftragte für den Datenschutz in seinem Praxisratgeber-für-Vereine Baden-Württemberg.pdf diese Form:

Beispiel für ein ausgefülltes Verzeichnis von Verarbeitungstätigkeiten:

Verarbeitungstätigkeit	Zwecke der Verarbeitung	Kategorien der betroffenen Personen	Kategorien von personenbezogenen Daten	Kategorien von Empfängern	Übermittlung an ein Drittland	Löschfristen
Mitgliederverwaltung	Mitglieder- verwaltung	Mitglieder	Name Adresse Geburtsdatum Abteilung/ Sportbereich	Keine	Nein	Nach Beendigung der Mitgliedschaft
Lohnabrechnung	Auszahlung von Gehalt, Abfuhr von Steuern und Sozialabgaben	Beschäftigte	Name Adresse Religionszugehörigkeit Steuernummer etc.	Ggf. externer Dienstleister	Nein	Gesetzl. Aufbewahrungsfrist von 10 Jahren
Veröffentlichung von Fotos auf der Vereinswebseite	Außerdarstellung, Anwerben neuer Mitglieder	Mitglieder, Besucher der Webseite	Fotos, IP-Adressen	Keine	Nein	Fotos bei Widerruf der Einwilligung, IP-Adressen nach 30 Tagen

Eine gute Unterstützung bei dieser Aufgabe, auch bei großen Vereinen bietet diese Broschüre (kostenloses PDF): GDD-Praxishilfe DSGVO V – Verzeichnis von Verarbeitungstätigkeiten. Herausgeber: Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.).
Sie erhalten es hier: www.gdd.de.

Ein Muster für ein solches Verzeichnis finden Sie auch im Anhang dieses Handouts.

Auftragsverarbeitung

Wenn Dienstleister Aufgaben für den Verantwortlichen erfüllen (z.B. Adressverwaltung, externe Lohnabrechnung, Wartung IT) und in diesem Zusammenhang mit personenbezogenen Daten umgehen bzw. Einblick in diese haben, so spricht man von einer Auftragsverarbeitung. Diese ist auch dann gegeben, wenn ein Verein seine Mitgliederdaten nicht auf einer eigenen EDV-Anlage speichert, sondern hierfür einen Datenbankserver nutzt, den ein Dienstleistungsunternehmen zu diesem Zweck zur Verfügung stellt.

Der Verein darf nur Auftragsverarbeiter einsetzen, die eine hinreichende Garantie für eine datenschutzkonforme Datenverarbeitung gewährleisten.

Die Auftragsverarbeitung darf nur auf der Grundlage eines bindenden Vertrages erfolgen. In diesem muss im Einzelnen 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 DSGVO vorgeschriebenen Rechte der betroffenen Personen
- Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei den in Art. 32 ff. DSGVO festgeschriebenen Verpflichtungen, insbesondere bei der Meldepflicht von Datenschutzverstößen
- Abwicklung nach Beendigung der Auftragsverarbeitung
- Kontrollrechte des Auftraggebers

Gemäß Art. 28 Abs. 9 DSGVO 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. Im Ergebnis muss der Vertragspartner in der Lage sein, das akzeptierte Dokument „bei sich“ zu speichern und auszudrucken.

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 DSGVO). Der Verantwortliche hat die Gewährleistung der in Kapitel III der DSGVO aufgeführten Betroffenenrechte (siehe unter Betroffenenrechte) sicherzustellen.

Weitere Informationen und ein Muster hier:
www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-3-ADV.pdf

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.

Die Weitergabe von personenbezogenen Daten an Auftragsverarbeiter in ein Land außerhalb der EU ist grundsätzlich zulässig. Zu beachten sind dann allerdings die zusätzlichen Anforderungen an die Sicherstellung des Datenschutzniveaus beim Auftragsverarbeiter nach Kapitel V der DSGVO. Auf der sicheren Seite sind Vereine nur bei Nutzung von Dienstleistern innerhalb Europas ... also z. B. nicht mit der dropbox.

Datenschutzfolgenabschätzung

Vereine sind in bestimmten Fällen verpflichtet, eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen. Diese ist nur erforderlich, **wenn die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten für die betroffene Person zur Folge hat**. Das ist insbesondere dann der Fall, wenn eine umfangreiche Verarbeitung besonderer Kategorie von Daten erfolgt (z. B. Verarbeitung von Gesundheitsdaten) oder wenn systematische und umfassende Bewertungen persönlicher Aspekte vorgenommen werden (z. B. Profiling). Hiervon ist bei Vereinen in aller Regel nicht auszugehen, kann jedoch bei Vereinen der Straffälligenhilfe oder bei Selbsthilfegruppen ausnahmsweise der Fall sein.

Die Aufsichtsbehörden für den Datenschutz sind gehalten, Positivlisten von Verarbeitungsvorgängen zu erstellen, bei denen typischerweise Folgenabschätzungen nach Art. 35 DSGVO vorgeschrieben sind. Ebenso erstellen die Datenschutz-Aufsichtsbehörden Negativlisten von Vorgängen, bei denen Folgenabschätzungen entbehrlich sind.

Technische und organisatorische Maßnahmen zur Datensicherung (TOMs)

In Art. 32 Abs. 1 b) DSGVO sind vier Schutzziele aufgelistet, die bei der Verarbeitung personenbezogener Daten sichergestellt werden müssen:

- **Vertraulichkeit**, d.h. Daten sind für unberechtigte Dritte nicht zugänglich.
- **Integrität**, d.h. Daten können nicht verfälscht werden.
- **Verfügbarkeit**, d.h. Daten stehen zur Verfügung, wenn sie gebraucht werden.
- **Belastbarkeit**

Unter den Begriff der „technischen und organisatorischen Maßnahmen“ fallen vor allem diejenigen Maßnahmen, die sicherstellen, dass Daten nur zweckgebunden verarbeitet werden und zur Kenntnis gelangen. Dies ist sowohl technisch (z.B. durch Verschlüsselung, Passwortschutz, Verriegelung von Räumen, Firewalls, Virenscanner, Backupkonzept) als auch organisatorisch (z.B. Zugriffsberechtigungen, regelmäßige Änderungen von Passwörtern, Sperren von EDV-Geräten, Schreddern von Dokumenten) zu gewährleisten.

Technische und organisatorische Maßnahmen zur Datensicherheit und ein Notfallmanagement, inkl. Notfallplänen sollten erarbeitet und durch den Verantwortliche im Verein schriftlich festgehalten werden. Die Wiederherstellbarkeit von Daten sollte regelmäßig getestet werden.

Natürlich muss das alles im Rahmen des technisch Machbaren sein und in einem angemessenen Verhältnis zu den personellen und finanziellen Möglichkeiten des Vereins stehen.

> ***Art. 32 DSGVO Sicherheit der Verarbeitung***
> Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten ...

Allerdings gibt es bei besonders schützenswerten Daten auch für kleine Institutionen keinen Sicherheitsrabatt.

Welche Vorgehensweise ist anzuraten?

- Bewertung von Risiken auf der Basis des Verzeichnisses der Verarbeitungstätigkeiten
- Besprechen der notwendigen TOMs
- Beschreiben des Managements für Datensicherheit
- Etablieren der notwendigen Maßnahmen
- Maßnahmen der Datensicherheit dokumentieren und fortlaufend aktualisieren
- regelmäßige Prüfung, ob die Datensicherungen zur Wiederherstellung verlorener Daten genutzt werden können.

Die große Gefahr: USB-Sticks und mobile Festplatten

USB-Sticks und mobile Festplatten sind mit das größte Sicherheitsrisiko für unsere Daten. Eigentlich müsste der Einsatz zumindest unverschlüsselter USB-Sticks grundsätzlich technisch verhindert werden. Denn Downloads auf die Sticks können nicht nachvollzogen werden, sodass Daten in falsche Hände kommen können außerdem können Wechselmedien Viren enthalten. Nach einer Untersuchung nutzen fast 95% aller Mitarbeiter in deutschen Unternehmen im Dienst USB-Sticks.In fast ¾ aller Unternehmen gingen bereits Sticks verloren und 80% davon waren unverschlüsselt …

Deshalb sollten niemals Wechselmedien verwendet werden, die nicht verschlüsselt sind!

Eine Verschlüsselung lässt sich auch von Laien mit der kostenlosen Software veracrypt recht einfach bewerkstelligen. Infos dazu finden Sie hier:

- Filmische Anleitung auf Youtube: *https://youtu.be/gUbqrow3Od0*
- Auf Lehrerfortbildung Baden-Württemberg: *https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/dossiers/sicherheit/stickcrypt/vc/*

Übermittlung von Daten

Quelle: http://www.vereinsknowhow.de/kurzinfos/datenschutz.htm

Teilweise muss der Verein Daten von Mitgliedern weitergeben. Ob das zulässig ist, hängt vom Einzelfall ab:

- Weitergabe **an andere Mitglieder**: i.d.R. nur im Sonderfall; das ist vor allem das Minderheitenbegehren nach § 37 BGB
- Weitergabe **an Verbände**: Die ist zulässig, wenn sie sich schon aus der Vereinstätigkeit ergibt (z.B. Wettkampfmeldungen). Geht die Datenweitergabe darüber hinaus, sollte das in der Satzung geregelt oder in der Einverständniserklärung benannt werden.
- **Veröffentlichung** von Daten: Die Veröffentlichung (Mitteilungsblatt, Schwarzes Brett) ist zulässig, wenn sie dem Vereinszweck dient, z.B. bei Mannschaftsaufstellungen oder Spielergebissen. Nicht zulässig ist die Veröffentlichung der Namen in Fällen mit „ehrenrührigem" Inhalt wie Hausverboten, Vereinsstrafen oder Spielersperren
- **Veröffentlichung im Internet**: Hier ist besondere Zurückhaltung geboten. Die Veröffentlichung personenbezogener Daten durch einen Verein im Internet ist grundsätzlich unzulässig, wenn sich der Betroffene nicht ausdrücklich damit einverstanden erklärt hat.

Informationen über Vereinsmitglieder (z.B. Spielergebnisse und persönliche Leistungen, Mannschaftsaufstellungen, Ranglisten, Torschützen usw.) oder Dritte (z.B. Ergebnisse externer Teilnehmer) können i.d.R. auch ohne Einwilligung **kurzzeitig** ins Internet gestellt werden, wenn die Betroffenen darüber informiert sind.

- Persönliche Nachrichten, wie z.B. zu Spenden, Geburtstagen und Jubiläen, sind in der Regel unproblematisch. Das Mitglied kann dem aber widersprechen.
- Die Weitergabe zu Werbezwecken (etwa an Sponsoren) darf nur mit Zustimmung des jeweiligen Mitglieds erfolgen.
- Ein besonderes Schutzinteresse ergibt sich oft aus dem Vereinszweck (z.B. bei Selbsthilfevereinen zu Erkrankungen). Hier dürfen die Daten nicht ohne Zustimmung weitergegeben oder veröffentlicht werden.

Risiko =

Eintrittwahrscheinlichkeit x Schadenshöhe

Prozess bei Widersprüchen oder Datenschutzverletzungen

Meldung von Datenschutzverstößen (Data Breach)

Ein Data Breach (=Datenpanne) ist ein Verstoß gegen die Datensicherheit und den Datenschutz, bei denen personenbezogene Daten Unberechtigten vermutlich oder erwiesenermaßen bekannt werden. Ursachen dafür sind vielfältig und können

- z.B. in einem Hackerangriff,
- dem Verlust eines USB-Sticks,
- dem Diebstahl eines Smartphones
- oder in einem unbefugten Weitergeben durch Mitarbeiter liegen – gleichgültig, ob dies bewusst oder unbewusst erfolgte.

Formale Anforderungen an die Data Breach

Die DSGVO sieht eine deutlich verschärftere Meldepflicht bei Data Breaches vor. Für die formalen Anforderungen werden in den Art. 33, 34 DSGVO jeweils Mindestanforderungen geregelt.

Notwendig ist bei der Meldung an die Aufsichtsbehörde:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, möglichst mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- der Name und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Datenschutzes
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Die letzten drei Punkte sind auch bei der Benachrichtigung der Betroffenen zu berücksichtigen. Zudem ist in diesen Fällen die Meldung in einer klaren und einfachen Sprache zu verfassen.

Meldefristen

Sowohl die Data Breach Notification an die Aufsichtsbehörde als auch die Benachrichtigung der Betroffenen haben unverzüglich nach Kenntniserlangung zu erfolgen. In Art. 33 Abs. 1 DSGVO wird für die Meldung an die Aufsichtsbehörde ein gesetzlicher Richtwert von 72 Stunden für den Ablauf der Unverzüglichkeit angenommen. Erfolgen Data-Breach Notifications erst nach Ablauf dieser Frist, muss die Verzögerung gesondert begründet werden.

Dokumentationspflichten

DSGVO-typisch werden dem Verantwortlichen nach Art. 33 Abs. 5 DSGVO außerdem Dokumentationspflichten hinsichtlich aller Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen auferlegt.

Um diesen Melde- bzw. Informationspflichten nachkommen zu können, muss im Verein ein Prozess verankert sein, mit dem die Verletzung des Schutzes personenbezogenen Daten erkannt, der Sachverhalt an den Datenschutzbeauftragten – wenn vorhanden – weitergeleitet und anschließend bewertet wird. Der Datenschutzbeauftragte hat dabei zu prüfen, ob ein normales oder ein hohes Risiko für die Rechte und Freiheiten von Betroffenen vorliegt (bzw. ob überhaupt ein Risiko vorliegt).

Kein Verwertungsverbot

Im alten Datenschutzgesetz durften Informationen aus der Meldung einer Datenpanne in einem Straf- oder Ordnungswidrigkeitsverfahren nur mit Zustimmung des Verantwortlichen verwendet werden. Eine solche Einschränkung ist in der DSGVO nicht mehr vorhanden. Es besteht daher grundsätzlich die Möglichkeit, dass Verantwortliche durch Erfüllung der Meldepflicht selbst die Grundlage für ein Bußgeldverfahren gegen sich schaffen.

> ***Ein Musterformular zur Aufnahme und Dokumentation von Datenschutzverstößen finden Sie im Anhang.***

Datenschutz auf der Vereinswebsite

Die Website eines Vereins ist das Einfallstor für Abmahner. Sie ist problemlos von außen überprüfbar, sicher auch durch automatische Programme. Deshalb hat die Absicherung der Website höchste Priorität.

add-ons, cookies, tracker

Viele Websites checken im Hintergrund die Aktivitäten ihrer Nutzer … ohne das offen zu sagen. Jeder kennt das: da hat man sich einmal in einem Online-shop etwas angesehen – sagen wir mal: rote Schuhe – und plötzlich erscheinen auf anderen Websites und bei facebook überall Angebote für rote Schuhe. Das ist folge des Einsatzes kleiner Programme auf den Webseiten, die wir besuchen. Und es ist legal … wenn man vor dem Einsatz der Programme darauf hingewiesen wird. Was aber so gut wie nie passiert.

Was hat das mit Vereinswebsites zu tun? Nun, viele nutzen ebenfalls cookies, tracker etc. Und nicht selten ist es den Verantwortlichen gar nicht bewusst. Vor Jahren hat ein wohlmeinendes Vereinsmitglied die Website gestaltet und gleich z.B. mit google analytics ausgestattet. Die Hoffnung war, dass man so einiges über die Besucher der Site erfährt, wo sie leben, welche Hobbies sie sonst haben etc. Genutzt wurde das Ganze nur selten. Wenn überhaupt. Und dann geriet es in Vergessenheit. Vielleicht weiß schon lange niemand mehr, dass der tracker läuft. Aber der schaltet sich nicht selbstständig ab. Und er sendet weiter munter Daten an google, facebook und wie sie alle heißen.

Aber die Robotprogramme der Abmahner können jede Seite in Sekundenbruchteilen checken … und finden alle die add-ons. Und wenn dann in der Datenschutzerklärung der Seite nicht auf diese hingewiesen wird, hat man ein Problem.

Es gilt also, die Website abzusichern. Hier sinnvolle Schritte, um eine datenschutzkonforme Lösung für die Vereinswebsite zu erreichen:

1. Schritt: Analyse

Fragen Sie denjenigen, der Ihre Website erstellt hat, beziehungsweise diese pflegt. Bitten Sie ihn, Ihnen genau zu sagen, welche Erweiterung, cookies, add-ons etc., eure Website verwendet. Der Möglichkeiten sind viele:

- Google Analytics
- Facebook-Plugins (Like-Button)
- Twitter
- Google+
- Instagram
- LinkedIn
- Pinterest
- SoundCloud
- Spotify
- XING
- Tumblr
- YouTube
- Matomo (früher Piwik)
- SSL-Verschlüsselung …

… um nur die wichtigsten zu nennen.

Sie können Ihre Site auch selbst testen: cookies finden Sie, indem Sie hier: *http://www.cookie-checker.com* Ihre URL eingeben. Tracker etc. findet die **Browsererweiterung „Ghostery"**, die sich in den meisten Browsern installieren lässt und fortan mit einem kleinen Geistsymbol diese Unholde anzeigt.

Überlegen Sie sich schließlich genau, welche add-ons oder Cookies die Website wirklich benötigt. Eigentlich braucht sie, wenn man ehrlich ist, wahrscheinlich keines davon. Ich habe Websites gecheckt, die über drei Aktivitäten-Tracker verfügten und niemand von den Websitebetreibern, wusste davon.
Also weg mit allem, was Sie nicht brauchen!

2. Schritt: SSL-Verschlüsselung

Die DSGVO fordert, dass personenbezogene Daten nicht unverschlüsselt übertragen werden dürfen. Das heißt aber auch, dass eigentlich alle Websites über dieses Feature verfügen müssen. Sie erreichen das über den Hoster Ihrer Site, also über strato, 1&1 etc. Meistens lässt sich das leicht online durchführen und ist für eine Site auch kostenlos. Bei strato loggen Sie sich mit Ihrer Kundennummer ein und gehen über den Menüpunkt „Sicherheit", bei den anderen Providern dürfte das ähnlich sein. Zur Not hilft die Hotline. Dass die SSL-Verschlüsselung aktiv ist, erkennen Sie an einem Schlosssymbol vor Ihrer URL oder an dem „s" in https::://

3. Schritt: Direkter Weg zur Datenschutzerklärung

Lassen Sie auf Ihrer Website unbedingt einen eigenen Menüpunkt Datenschutz erstellen. Bitte nicht ins Impressum mischen! Dieser muss auf jeder Seite direkt (One-click) erreichbar sein.

4. Schritt: Die Datenschutzerklärung

Das ist der aufwändigste Teil. Denn neben allgemeinen Aussagen müssen Sie für jedes add-on eine eigene Formulierung in der Erklärung haben. Zum Glück gibt es im Internet einige kostenlose Generatoren, z.B. unter *https://www.wbs-law.de*. Dort kann man sich die passende Erklärung „zusammenklicken". Leider schalten einige Anbieter die kostenlosen Versionen langsam ab. Deshalb sollten Sie das bald erledigen.

Aber bitte: gehen Sie nicht nach dem Motto vor: „eher zu viel als zu wenig Plugins/APIs auflisten – ein Websitebesucher liest sich das sowieso nicht durch – dann sind wir auf der sicheren Seite. Hier ist „mehr" nicht „besser". Add-ons zu benennen, die man nicht verwendet, widerspricht Geist und Wortlaut der DSGVO. Diese schreibt nämlich vor (Art. 5 DSGVO, lit c), dass grundsätzlich nur die Daten gesammelt und gespeichert werden dürfen, die zur Erfüllung eines bestimmten, genau definierten Zwecks notwendig sind. D.h. wenn wir Daten sammeln, und die Erweiterungen auf der Website sind Instrumente der Datensammlung und Weitergabe (an google), dann dürfen wir das nur, wenn wir vorher festlegen, zu welchem Zweck wir diese sammeln. Und wenn wir außerdem den Betroffenen, also den Nutzern der Website, **in transparenten, klaren und gut verständlichen Worten** sagen, was wir tun und warum wir das tun.

5. Schritt: Weitere Datensammelstellen

Schauen Sie auf Ihrer Webseite nach, ob dort Kontaktformulare oder elektronische Anmeldemöglichkeiten, zum Beispiel für Mitgliedschaften, bestehen. Bei all diesen Formularen benötigen Sie unbedingt eine Schaltfläche, die angeklickt werden muss, bevor das Formular abgeschickt werden kann. Die Formulierung neben der Schaltfläche könnte lauten: „Die Datenschutzerklärung des XYZ-Vereins habe ich zur Kenntnis genommen." Und natürlich muss das Wort „Datenschutzerklärung" dann auf Ihre Datenschutzerklärung verlinkt sein.

Wenn Sie diese Punkte umsetzen, ist Ihre Website gegen die wesentlichen Angriffe der Abmahnfirmen gefeit.

Fotos, Namen und Adressen von Ehrenamtlichen auf der Website

Auch für Portraits von Ehrenamtlichen, z. B. auf der Website, benötigt der Verein eine schriftliche Einwilligung. Dabei muss deutlich werden:

- Wie groß das Bild wiedergegeben wird,
- wo es erscheint,
- wie lange es erscheint,
- wann es entfernt werden muss
  (z. B. vier Wochen nach dem Ausscheiden aus dem Vorstand).

Es muss zudem auf die Freiwilligkeit der Veröffentlichung hingewiesen werden und darauf, dass die Einwilligung jederzeit widerrufen werden kann.

Ein Muster für diese Einwilligung finden Sie im Anhang.

Die Problematik von Fotos auf der Website und in Vereinspublikationen

Hier gibt es viele Gerüchte, bis zu dem, dass gar keine Fotos mehr machbar seien. Das trifft sicher nicht zu. Der Rahmen, in dem wir hier arbeiten können, wird gut beschrieben in einer Broschüre des Landesamts für den Datenschutz Brandenburg. In diesem heißt es:

3.4 Fotografien im Rahmen ehrenamtlicher Tätigkeit (z. B. Vereine)

Große Unsicherheit herrscht derzeit insbesondere bei Privatpersonen, die im Rahmen ehrenamtlicher Tätigkeit auch Fotografien anfertigen oder auf Webseiten oder Broschüren benutzen (möchten). ... grundsätzlich haben z. B. Vereine ein Interesse daran, Fotos zu veröffentlichen, um u. a. auf der Vereinshomepage über Aktivitäten zu berichten und über den Verein zu informieren. In der Regel werden sich hieraus keine Beeinträchtigungen für den Betroffenen ergeben. Dennoch ist auch in diesem Kontext bei besonderer Motivlage (Kinder, Partyfotos etc. ...) immer im Einzelfall zu prüfen, ob gerade der Veröffentlichung bestimmter Fotos z. B. auf einer Webseite schutzwürdige Interessen des Betroffenen entgegenstehen. Bei Unklarheiten empfiehlt sich, eine Einwilligung des Betroffenen einzuholen, die wie bereits erläutert nicht zwingend schriftlich eingeholt werden muss. Auch mündliche Erklärungen sind wirksam, müssen jedoch im Zweifel nachgewiesen werden."

https://www.lda.brandenburg.de/media_fast/4055/DSGVOFotografienfinal.pdf (S. 9)

Bei Veranstaltungen ist es ggf. sinnvoll, am Eingang zu informieren:

„Bei einer öffentlichen bzw. größeren Veranstaltung auf Einladung dürfte die Erwartungshaltung der Gäste und der an der Durchführung Beteiligten regelmäßig dahingehen, dass eine Dokumentation in Form von Fotografien stattfinden wird. Bitte beachten Sie, dass ... bestimmte Informationspflichten bestehen ... . Wir empfehlen daher einen deutlichen Hinweis auf die Datenverarbeitung, an wen sich Betroffene für Datenschutzfragen wenden können sowie Art und Zweck der weiteren Verarbeitung (z. B. Verwendung auf der Webseite oder in sozialen Medien), etwa in Form eines nicht übersehbaren Aufstellers im Eingangsbereich einer Veranstaltung. Sollten einzelne Personen eine Ablichtung nicht wünschen, stünde es ihnen so frei, den Kontakt mit dem Fotografen zu suchen ..."

https://www.lda.brandenburg.de/media_fast/4055/DSGVOFotografienfinal.pdf (S. 5)

Eine Alternative wäre eine mündliche Information vor Beginn der Veranstaltung.

Fotos von großen Menschenmengen, z. B. bei Sportveranstaltungen, Versammlungen oder Straßenzügen sind in der Regel im berechtigten Interesse des Veranstalters. Das ändert aber nichts an der Informationspflicht. Allerdings kann diese eingeschränkt sein: nach Art. 14 DSGVO, Abs. 5 lit. d) besteht keine Pflicht zur Information, wenn die Erteilung der Informationen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde. Es kommt also auf den tatsächlichen Aufwand an und dieser Aufwand ist im Lichte des Informationsinteresses des Betroffenen zu betrachten und abzuwägen. Letztlich ist das also eine Einzelfallabwägung, bei der die individuellen Gegebenheiten zu berücksichtigen sind. Das Landesamt für den Datenschutz Brandenburg schließt: „Auch in dieser Hinsicht wäre eine ausdrückliche gesetzliche Regelung für die Besonderheiten der Fotografie wünschenswert. Bis zu einer rechtssicheren Klärung sollte der Maßstab in dieser Hinsicht sicher nicht zu streng gehandhabt werden."

Dem schließen sich die Vereine sicher gerne an.

Vorsicht bei Fotos von Kindern!

Besondere Vorsicht ist geboten, wenn Minderjährige im Mittelpunkt von Fotos, auch von Manschaftsfotos stehen. Bei ihnen werden oft berechtigte Interessen vorliegen, die eine Veröffentlichung von Fotos ohne Einwilligung ausschließen.

- Spielszenen bei Mannschaftsspielen sollten in der Regel nicht ohne Einwilligung der Sorgeberechtigten im Internet veröffentlicht werden.
- Dasselbe gilt für Gruppenfotos aller Art vom Training.
- Kein Problem stellt es dagegen normalerweise dar, wenn Kinder beim Besuch einer Person der Zeitgeschichte mit abgebildet sind.

Quelle: Erste Hilfe zur Datenschutzgrundverordnung für Unternehmen und Vereine, C.H.Beck, 2018, Seite 56.

Mannschaftsfotos

„Bei Mannschaftsfotos von Erwachsenen kann man von einer stillschweigenden Einwilligung in das Foto an sich ausgehen, weil die einzelnen Personen bewusst daran mitwirken und sich auch bewusst entsprechend auf dem Foto positionieren lassen. Daraus lässt sich allerdings noch nicht ableiten, dass die Betroffenen mit einer Veröffentlichung des Fotos im Internet einverstanden sind. ... Deshalb ist zu empfehlen, in Form einer Unterschriftliste die Zustimmung zur Veröffentlichung im Internet einzuholen. Damit es beim Einholen der Unterschrift nicht zu unliebsamen Überraschungen kommt, sollte dieses Vorgehen schon vor Anfertigung des Mannschaftsfotos besprochen und angekündigt werden. Sollte die Mannschaft in einer Teambesprechung gemeinsam entscheiden, dass es ohne eine solche Unterschriftenliste geht, ist das in Ordnung. Dann haben alle Teammitglieder zugestimmt. Das Gesetz schreibt nicht vor, dass dies schriftlich geschehen muss. Doch Vorsicht: Wenn einzelne Teammitglieder einfach nichts sagen, liegt darin keine Zustimmung. ...

Quelle: Erste Hilfe zur Datenschutzgrundverordnung für Unternehmen und Vereine, C.H.Beck, 2018, Seite 56.

Vereinschronik

Im Gegensatz zum Internet, hat ein gedrucktes Werk nur einen begrenzten Verbreitungsbereich.

- Fotos von Veranstaltungen können häufig abgebildet werden, ohne dass eine Einwilligung der Personen erforderlich ist, die darauf zu sehen sind.
- Fotos, auf denen Personen individuell abgebildet werden, dürfen nur mit Einwilligung dieser Personen veröffentlicht werden. Das gilt auch, wenn beispielsweise jemand früher Vereinsvorsitzender war.
- Bei historischen Fotos kommt es öfter vor, dass die Abgebildeten teilweise oder sogar bereits alle verstorben sind. Falls abgebildete Personen schon länger als zehn Jahre tot sind, dürfen die Fotos problemlos veröffentlicht werden. Eine Einwilligung von Angehörigen ist jedenfalls rein rechtlich gesehen nicht mehr erforderlich. Anders sieht es aus, falls der Tod noch weniger als zehn Jahre zurückliegt und nach dem, was oben geschildert wurde, eine Einwilligung erforderlich ist. Dann tritt an die Stelle der Einwilligung des Verstorbenen die Einwilligung der Angehörigen (siehe § 22 Sätze 3 und 4 KUG).

Quelle: Erste Hilfe zur Datenschutzgrundverordnung für Unternehmen und Vereine, C.H.Beck, 2018, Seite 56.

Mitgliederbriefe und Mailings

Völlig unproblematisch ist das Versenden von Informationen per Post. Allerdings müssen auch diese dem Zweck entsprechen, für den die Daten einmal erhoben wurden. Es dürfen also keine Werbungen anderer (z.B. Sponsoren) verschickt werden, es sei denn, die Mitglieder haben das vorab ausdrücklich erlaubt. **Das Datenschutzrecht erlaubt unter bestimmten Voraussetzungen, Mitgliedern und anderen Betroffenen ohne gesonderte Erlaubnis auch E-Mails zuzusenden.** Dabei sind vier Voraussetzungen zu beachten:

- Der Verein muss die E-Mail-Adresse im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erhalten haben. Es dürfen also nur Bestandskunden beworben werden.
- Es dürfen nur eigene Produkte und Dienstleistungen beworben werden, die dem bereits „verkauften" ähnlich sind. Ergänzungsangebote (Up-Selling) sind grundsätzlich auch zulässig.
- Die Mitglieder und andere Betroffene müssen bereits bei der Übergabe seiner E-Mail-Adresse und in jedem Mailing darauf hingewiesen werden, dass der Verwendung jederzeit widersprochen werden kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen. Ihm ist also jedes Mal eine Kontaktadresse anzubieten, an die er sich wenden kann, um den weitere Infos abzubestellen. Ein entsprechender Hinweis muss auch bereits bei Erhebung der E-Mail-Adresse erfolgen.

- Hat das Mitglied/der Betroffene von seinem Widerspruchsrecht Gebrauch gemacht, muss seine Adresse unverzüglich aus dem Verteiler genommen werden.

(Quelle: www.datenschutzbeauftragter-info.de/fachbeitraege/newsletterund-datenschutz)

Wichtig: Mailadressen bei Verteilern dürfen nur unter BCC: versandt werden um zu verhindern, dass alle Empfänger die Mailadressen lesen können!

Newsletterabo: Nur mit double-opt-in

Rigider ist das Recht allerdings bei Newslettern. Das ist aber keine Frage der DSGVO, sondern basiert auf der Tatsache, dass hier zusätzlich das Wettbewerbsrecht greift. Im Gesetz gegen den unlauteren Wettbewerb (UWG) heißt es:

§ 7 Unzumutbare Belästigungen

Eine geschäftliche Handlung, durch die ein Marktteilnehmer in unzumutbarer Weise belästigt wird, ist unzulässig. Dies gilt insbesondere für Werbung, obwohl erkennbar ist, dass der angesprochene Marktteilnehmer diese Werbung nicht wünscht.

Das Problem ist, dass Newsletter regelmäßig erscheinen und unspezifisch werben. Deshalb sind zwar spezielle direct-Mailings an bestimmte Zielgruppen ohne vorherige Einwilligung möglich, nicht aber der Versand eines Newsletters, der einer dezidierte Zustimmung bedarf, z.B. über ein „Double-Opt-in“:

„Beim „Double-Opt-in“ ... muss der Eintrag in die Abonnentenliste in einem zweiten Schritt bestätigt werden. Meist wird hierzu eine E-Mail-Nachricht mit Bitte um Bestätigung an die eingetragene Kontaktadresse gesendet. ... Eine Registrierung beim „Double-Opt-in“ wird erst dann wirksam, wenn sie bestätigt wird. ... Dieses Verfahren wird für seriöses E-Mail-Marketing von verschiedenen Organisationen, wie zum Beispiel dem Deutschen Dialogmarketing Verband (DDV), empfohlen. Der BGH erklärte, das Double-opt-in-Verfahren ist geeignet, Darlegung und Nachweis einer Einwilligung in den Empfang von Werbemails zu erleichtern.[1]”

(Quelle: https://de.wikipedia.org/wiki/Opt-in)

Das Problem der WhatsApp-Gruppen

Für viele von uns gehört Whatsapp zum Alltag. Der Messenger, der zu Facebook gehört, hat hierzulande etwa 40 Millionen aktive Nutzer. Viele verwenden Whatsapp nicht nur auf ihrem privaten Smartphone, sondern auch auf Dienstgeräten – und sorgen damit für Kopfzerbrechen in den Unternehmen.

Neulich machte der erste große Konzern in Deutschland einen Schnitt: Der Continental verbot die Nutzung von Whatsapp auf allen Dienstgeräten. Gleiches gilt für das soziale Netzwerk Snapchat, über das Nutzer vor allem Fotos und Videos verschicken.

Was ist an Whatsapp und Co. bedenklich? Nun, beide Dienste verlangen Zugriff auf die Kontaktdaten im Adressbuch und übertragen die darin gespeicherten Informationen auf ihre eigenen Server. Wer dies ablehnt, kann die Apps nur sehr eingeschränkt nutzen.

Aus Sicht von Conti ergibt sich dadurch ein Risiko, denn laut der DSGVO müssten Mitarbeiter eigentlich jeden auf ihrem Gerät gespeicherten Kontakt vorher ausdrücklich um Erlaubnis fragen, bevor seine Daten weitergereicht werden. Dies sei im Alltag aber „nicht ausreichend zuverlässig und damit praktisch untauglich“, sagt Conti.

Wenn das geschafft ist ...

- Verzeichnis zur Datenverarbeitung jährlich auf Aktualität und Anpassungsbedarf prüfen.
- Stete Sensibilisierung von Vorstand, Mitarbeiter/-innen und Ehrenamtlichen im Verein für die Wichtigkeit des Datenschutzes.
- Schnell und ehrlich auf mögliche Datenpannen reagieren.

Weitere Hilfen

Den Wortlaut der DSGVO finden Sie gut aufgearbeitet hier:
https://dsgvo-gesetz.de

„Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine“, Hrsg: Bayerisches Landesamt für Datenschutzaufsicht, bearb. von Thomas Kranig, 12/2017, ISBN 978-3-406-71662-1; 5,50 €

Datenschutz im Verein nach der DSGVO – Praxisratgeber,
Broschüre hrgg. durch den Landesbauftragten für den Datenschutz und Informationsfreiheit Baden-Württemberg
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-für-Vereine.pdf

Datenschutz im Verein nach der Datenschutzgrundverordnung (DSGVO) Informationen über die datenschutzrechtlichen Rahmenbedingungen beim Umgang mit personenbezogenen Daten in der Vereinsarbeit
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf

GDD Praxishilfe DSGVO V – Verzeichnis von Verarbeitungstätigkeiten
Herausgeber: Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.), *www.gdd.de*

Orientierungshilfe „Datenschutz im Verein nach der DSGVO“
Kurzpapier Nr. 12 der Datenschutzkonferenz
(https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/01/DSK_KPNr_12_Datenschutzbeauftragter.pdf).

Verarbeitung personenbezogener Daten bei Fotografien
Broschüre des Landesamts für Datenschutz Brandenburg:
www.lda.brandenburg.de/media_fast/4055/DSGVOFotografienfinal.pdf

Websites auf cookies checken
http://www.cookie-checker.com

Datenschutzerklärung für Websites: Generator
https://datenschutz-generator.de

Landesamt für Datenschutz und Informationsfreiheit Baden-Württemberg
https://www.baden-wuerttemberg.datenschutz.de

Bayerisches Landesamt für Datenschutzaufsicht Bayern
https://www.lda.bayern.de/de/datenschutz_eu.html

Anhang

ToDo-Liste Datenschutz-Implementierung

Benennen des Verantwortlichen ..... ☐

Entscheidung: Brauchen wir einen Datenschutzbeauftragten? ..... ☐
- Falls ja: Benennung des Datenschutzbeauftragten ..... ☐
- Meldung des Datenschutzbeauftragten an die Aufsichtsstelle ..... ☐
- Richtlinie zur Einbindung des Datenschutzbeauftragten erstellen ..... ☐

Datenschutzerklärung Ehrenamtliche ..... ☐

Mitgliedsanträge datenschutzkonform machen ..... ☐

Verzeichnis der Verarbeitungstätigkeiten erstellen ..... ☐

Klären, ob eine Datenschutzfolgenabschätzung erforderlich ist ..... ☐
- Falls ja: Sie benötigen professionelle Hilfe!

Beschreibung der Technisch-organisatorischen Maßnahmen (TOMs), Datensicherheitskonzept ..... ☐

Prozess der Wahrnehmung von Betroffenenrechten fixieren ..... ☐

Prozess bei Widersprüchen und Datenschutzverletzungen festlegen ..... ☐

Website datenschutzkonform machen ..... ☐

Newsletter datenschutzkonform machen ..... ☐

Fortbildung der Mitarbeiter/innen ..... ☐

Überprüfung und Dokumentieren der Änderungen, mindestens jährlich ..... ☐

Formulierungshilfe:

Info Mitglieder, Mitgliedsantrag

Art. 13 DSGVO regelt die Informationspflicht bei der Erhebung von personenbezogenen Daten, der auch Vereine unterworfen sind.

Bei **Bestandsmitgliedern** kann das durch eine Information in der Mitgliederzeitschrift oder als Anlage zu einem Jahresbrief/zur Einladung zur Jahreshauptversammlung erfolgen.

Bei **Neumitgliedern** sollte die Information mit dem Mitgliedsantrag erfolgen ... mit einer Bestätigung, dass das neue Mitglied davon Kenntnis genommen hat. Sinnvoll ist, dass Antrag und Info zusammen ausgegeben werden (z.B. Vorder-/Rückseite).

Inhalte der Mitgliederinformation zur Erhebung von personenbezogenen Daten gemäß Art. 13 DSGVO

Quelle: LfDI BW - Datenschutz im Verein nach der DSGVO, S. 13f

1. **Name und Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters**
   Verantwortlicher im Sinne des Art. 13 Abs. 1 lit. a) DSGVO ist

   Name Verein: _____

   Straße: _____

   PLZ, Ort: _____

   Tel.: _____

   E-Mail: _____

   Vorstand: _____

2. **Kontaktdaten des Datenschutzbeauftragten**
   Die Kontaktdaten des Datenschutzbeauftragten müssen nur dann angegeben werden, wenn ein solcher benannt ist. Ausreichend ist hierbei die Angabe eines Funktionspostfachs.

   Formulierungsbeispiel:
   Unseren Datenschutzbeauftragten erreichen Sie unter folgender E-Mail-Adresse: Datenschutzbeauftragter@Musterverein.de

3. **Zwecke und Rechtsgrundlage der Verarbeitung**
   Bei einem Verein können je nach Ausrichtung ganz verschiedene Zwecke anfallen, für die personenbezogene Daten verarbeitet werden. Jeder Zweck ist gesondert aufzunehmen und die Rechtsgrundlage der Verarbeitung anzugeben.

   Jeder Verein sollte sich daher zunächst einen Überblick darüber verschaffen, welche Daten zu welchem Zweck verarbeitet werden und sodann prüfen, auf welcher Grundlage die Verarbeitung erfolgt. Als Rechtsgrundlage kommen in Betracht:

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

   Formulierungsbeispiele
   (die im Folgenden genannten Zwecke sind nur beispielhaft und nicht abschließend):

   Der Musterverein verarbeitet folgende personenbezogene Daten:

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

4. **Berechtigte Interessen des Vereins**
   Berechtigte Interessen nach Art. 6 Abs. lit. f) DSGVO eines Vereins spielen immer dann eine Rolle, wenn der Verein bestimmte Daten verarbeiten möchte, diese Daten jedoch weder für die Erfüllung des Mitgliedsvertrags/Satzung benötigt werden noch eine Einwilligung der Vereinsmitglieder in die entsprechende Datenverarbeitung vorliegt. Die berechtigten Interessen können daher von Verein zu Verein ganz verschieden sein.

   Formulierungsbeispiele für berechtigte Interessen
   (nicht abschließend):

   - Der Musterverein übermittelt ohne vertragliche oder sonstige Verpflichtung auf freiwilliger Basis Mitgliederlisten an den Dachverband ... (konkret benennen), um (Grund für das Interesse der Datenübermittlung nennen).
   - Der Musterverein hat als Gegenleistung für das Sponsoring ein berechtigtes Interesse daran, an den Sponsor X (konkret benennen) den Namen, die Adressen sowie die E-Mail-Adresse der Mitglieder zum Zwecke der Werbung zu übermitteln. Das Vereinsmitglied kann dieser Übermittlung jederzeit widersprechen; im Falle eines Widerspruches werden seine personenbezogenen Daten auf der zu übermittelnden Liste geschwärzt.
   - Der Musterverein hat ein berechtigtes Interesse daran, personenbezogene Daten Dritter, die dem Verein bekannt sind (etwa von Personen, die regelmäßig Eintrittskarten für Spiele beziehen), zum Zwecke der Eigenwerbung zu verarbeiten.
   - Der Musterverein hat ein berechtigtes Interesse daran, bei dem Verkauf von Eintrittskarten für Fußballspiele Name, Vorname, Anschrift und Geburtsdatum von unbekannten Personen zu erheben, um zu überprüfen, ob gegen diese ein Stadionverbot ausgesprochen worden ist oder ob sie als gewaltbereit anzusehen sind.

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

   Formulierungsbeispiele (nicht abschließend):

   - Als Mitglied des Muster-Kreisverbandes ... (Verband konkret benennen) ist der Verein verpflichtet, seine Mitglieder an den Verband zu melden. Übermittelt werden dabei Name, LfDI BW - Datenschutz im Verein nach der DSGVO, Adresse, ... (Daten bitte konkret nennen). Bei Mitgliedern mit besonderen Aufgaben (z.B. Vorstandsmitglieder) wird zusätzlich die Bezeichnung ihrer Funktion im Verein übermittelt.
   - Der Musterverein hat einen Kooperationsvertrag mit ... (Name des kooperierenden Unternehmens) abgeschlossen. Hierfür übermittelt er einmal im Jahr eine vollständige Liste der Mitglieder an ... (Name des kooperierenden Unternehmens), die den Namen, die Adresse und das Geburtsjahr enthält.
   - Im Rahmen der Cloud-Mitgliederverwaltung werden die personenbezogenen Daten unserer Mitglieder bei ... (Name des Cloud-Anbieters) gespeichert.

6. **Drittlandstransfer**
   Besteht die Absicht des Vereins, personenbezogene Daten der Mitglieder an ein Drittland zu übermitteln (z.B. im Rahmen der Cloud-Mitgliederverwaltung erfolgt die Speicherung in den USA), so ist hierauf hinzuweisen.

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

   Formulierungsbeispiele (nicht abschließend):

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

8. **Betroffenenrechte**

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

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

   Dem Vereinsmitglied steht ferner ein Beschwerderecht bei einer Datenschutz-Aufsichtsbehörde zu.

9. **Pflicht zur Bereitstellung der Daten**

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

10. **Automatisierte Entscheidungsfindung einschließlich Profiling**

    Ein Hinweis hierauf ist nur dann erforderlich, wenn eine automatisierte Entscheidungsfindung (einschließlich Profiling) gemäß Art. 22 Abs. 1 und Abs. 4 DSGVO durch den Verein erfolgt. Art. 22 DSGVO findet jedoch nur dann Anwendung, wenn die die betroffene Person beschwerende Entscheidung auf eine automatisierte Verarbeitung zurückgeht (z.B. Profiling, Ablehnung Online-Kreditantrag). Eine automatisierte Entscheidungsfindung ist bei Vereinen allerdings kaum denkbar, sodass ein Hinweis hierauf nicht erfolgen muss.

Formulierungshilfe: ***Verpflichtung Ehrenamtlicher***

zur Einhaltung der Anforderungen der DSGVO

Frau/Herr _____
wurde darauf verpflichtet, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DSGVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DSGVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

- auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung");
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. *[Nur für Angestellte: Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen.]* Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. *[Nur für Angestellte: Ihre sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen ergebenden Pflichten, wie die Vertraulichkeitsverpflichtung, wird durch diese Erklärung nicht berührt. Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.]*

Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung habe ich erhalten. Ort, Datum/Unterschrift des Verpflichteten

Formulierungshilfe:
Nutzung von Namen und Fotos auf der Website

Die [Verein e.V.] möchte auf seiner Website Namen, Kontaktdaten und Porträtfotos seiner [Funktionsträger benennen „Vorstand, Beirat, Abteilungsleiter ...] veröffentlichen. Aus Datenschutzgründen ist dazu Ihre Zustimmung notwendig. Der Vereinsvorstand bittet Sie um diese Zustimmung und weist darauf hin, dass diese freiwillig erfolgt.

Einwilligung zur Nutzung von Namen, Kontaktdaten und Fotos

Ich gestatte hiermit dem [Verein e.V.] die Veröffentlichung

☐ meines Namens

☐ meiner Mailadresse

☐ meiner Telefonnummer

☐ meines Portraitfotos auf der Website [Website URL] in einer Größe von maximal 600 px (längere Seite).

Namen, Kontaktdaten und Porträtfoto verbleiben auf der Seite, bis ich meine Zustimmung widerrufe oder aus dem [Funktion benennen „Vorstand, Beirat, Abteilungsleiter ...] ausscheide. In letzterem Fall ist der [Verein e.V.] verpflichtet, Name, Kontaktdaten und Porträtfoto spätestens vier Wochen nach meinem Ausscheiden aus der Funktion zu entfernen.

Ort, Datum/Unterschrift des Einwilligenden

Formulierungshilfe: ***Verzeichnis der Verarbeitungstätigkeiten***

Große Vereine sollten ein umfangreicheres Verzeichnis führen. Hier ein Vorschlag auf der Basis der „GDDPraxishilfe DSGVO V – Verzeichnis von Verarbeitungstätigkeiten", hgg. von der Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.), www.gdd.de, Stand: Version 1.0 (April 2017).

Vorblatt

Verzeichnis von Verarbeitungstätigkeiten
Verantwortlicher gem. Artikel 30 Abs. 1 DSGVO

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name .....

Straße.....

Postleitzahl.....

Ort .....

Telefon.....

E-Mail-Adresse .....

Internet-Adresse.....

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name .....

Straße.....

Postleitzahl.....

Ort .....

Telefon.....

E-Mail-Adresse .....

Angaben zum Datenschutzbeauftragten

Name .....

Straße.....

Postleitzahl.....

Ort .....

Telefon.....

E-Mail-Adresse .....

Zuständige Aufsichtsstelle: Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg (www.baden-wuerttemberg.datenschutz.de)

Meldung des/der Datenschutzbeauftragten an die zuständige Aufsichtsstelle ist erfolgt:
☐ Ja ☐ Nein

Bezeichnung der Verarbeitungstätigkeit

Datum der Anlegung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse	
Bezeichnung der Verarbeitungstätigkeit [1]	
Zwecke und Rechtsgrundlage der Verarbeitung [1]	
Beschreibung der Kategorien betroffener Personen	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ Sonstige:
Beschreibung der Datenkategorien [2]	☐ ☐ ☐ ☐ Besondere Arten personenbezogener Daten:
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch werden [3]	☐ intern Abteilung/ Funktion ☐ extern Empfängerkategorie
Datenübermittlung Nennung der konkreten Datenempfänger	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt: ☐ Drittland [4], Name: ☐ internationale Organisation, Bezeichnung:

	Empfängerkategorie: Dokumentation geeigneter Garantien (Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt)
Fristen für die Löschung der verschiedenen Datenkategorien [5]	
Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO Bemerkungen: siehe TOM-Beschreibung	

[1] **Beispiele für Verarbeitungstätigkeiten**

„Allgemeine Kundenverwaltung“
verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso“
„Customer-Relationship-Management“
verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Kundenbeziehungen, Marketing, Neukundenakquise, Kundenbindungsmaßnahmen, Kundenberatung

[2] **Beispiele für Datenkategorien**

Kunden
Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax-und E-Mail-Daten), Geburtsdatum, Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließl. Kundenentwicklung, Produkt- bzw. Vertragsinteresse, Statistikdaten, Abrechnungs- und Leistungsdaten, Bankverbindung

Beschäftigtendaten (Lohn und Gehalt)
Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, etc.

[3] **Beispiele für Empfängerkategorien**

Empfängerkategorien sind insbesondere am Prozess beteiligte weitere Stellen des Vereins oder andere Gruppen von Personen oder Stellen, die Daten – ggf. über Schnittstellen – erhalten z.B. in den Prozess eingebundene weitere Fachabteilungen, Vertragspartner, Kunden, Behörden, Versicherungen, Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.

[4] **Drittländer**

sind solche außerhalb der EU/des EWR Beispiele für internationale Organisationen: Institutionen der UNO, EU.

[5] Anzugeben sind hier die konkreten **Aufbewahrungs-/Löschfristen**, die in Verarbeitungstätigkeiten implementiert sind, bezogen auf einzelne Verarbeitungsschritte, falls unterschiedlich. Soweit diese in einem Löschkonzept dokumentiert sind, reicht der konkrete Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.

Formulierungshilfe: ***Formular zur Aufnahme und Dokumentation von Datenschutzverstößen***

Das Formular ist vom Verantwortlichen für die Datenverarbeitung zu führen.

Zeitpunkt der Meldung (Datum, Uhrzeit):
Name und Kontaktdaten der-/desjenigen, die/der einen potenziellen Datenschutzverstoß meldet:
Beschreibung des potenziellen Verstoßes (z.B. Hackerangriff, Verlust eines USB-Sticks, Diebstahl eines Smartphones) und der Anzahl und Art der möglicherweise betroffenen Daten:
Information des Datenschutzbeauftragten durch: am:
Wahrscheinliche Folgen der Datenschutzverletzung:
Maßnahmen zur Behebung der Datenschutzverletzung oder zur Abmilderung ihrer möglichen nachteiligen Auswirkungen:
Empfehlung des Datenschutzbeauftragten Die Aufsichtsbehörde ☐ ist einzuschalten ☐ muss nicht eingeschaltet werden

Zeitpunkt der Meldung an die Aufsichtsbehörde (Datum, Uhrzeit) (mit Beschreibung der Art der Datenschutzverletzung, möglichst mit Angabe der Kategorien der Daten und der ungefähren Zahl der betroffenen personenbezogenen Datensätze und Personen, Name und Kontaktdaten des Datenschutzbeauftragten, Beschreibung der wahrscheinlichen Folgen und der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung oder zur Abmilderung ihrer möglichen nachteiligen Auswirkungen:
Zeitpunkt der Benachrichtigung der Betroffenen (Datum, Uhrzeit, Benachrichtigungsweg, Ablageort der Benachrichtigung) (mit Name und Kontaktdaten des Datenschutzbeauftragten, Beschreibung der wahrscheinlichen Folgen und der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung oder zur Abmilderung ihrer möglichen nachteiligen Auswirkungen:
Ergriffene Maßnahmen zur Verhinderung einer Wiederholung der erfolgten Datenschutzverletzung

Vereine fit machen für den neuen Datenschutz

Handout zum Seminar

zusammengestellt von Hans-Jürgen Fuchs