Bundesarbeitsgemeinschaft Selbsthilfe von Menschen mit Behinderung, chronischer Erkrankung und ihren Angehörigen e.V.

Dachverband von Selbsthilfe-verbänden

BAG SELBSTHILFE
Kirchfeldstraße 149
40215 Düsseldorf

Telefon 0211.31 00 6-0
Telefax 0211.31 00 6-48
info@bag-selbsthilfe.de
www.bag-selbsthilfe.de

DATENSCHUTZ IM VEREIN

Was haben Selbsthilfeorganisationen beim Datenschutz nach der EU-Datenschutzgrundverordnung (DSGVO) zu beachten?*

Spätestens seit Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) im Mai 2018 und der damit verbundenen Berichterstattung ist vielen Vereinen klar geworden, dass auch sie die gesetzlichen Vorgaben des Datenschutzes zu beachten haben. Diese Verpflichtung bestand zwar auch schon zuvor, allerdings war festzustellen, dass der Datenschutz vielfach gar nicht oder nur in unzureichendem Maße beachtet und umgesetzt wurde. Teilweise ist das auch jetzt noch der Fall.

Ein Grund hierfür mag ein mangelndes Bewusstsein dafür sein, dass auch personenbezogene Daten ein schützenswertes Rechtsgut darstellen. Sie betreffen unmittelbar die Privatsphäre und damit die Autonomie und Selbstbestimmung des Einzelnen. Umgekehrt sind Daten und ihre Erfassung in wirtschaftlicher Hinsicht und darüber hinaus auch zur Überwachung und Lenkung von Personengruppen immer bedeutsamer geworden. Es verwundert daher nicht, dass der weltweite Datenhandel in den letzten Jahren enorm zugenommen hat. Umso wichtiger ist es deshalb, mit Daten sorgsam und zurückhaltend umzugehen, natürlich auch aus Haftungsgründen.

* Trotz größter Sorgfalt bei der Erstellung der vorliegenden Übersicht kann keine Gewähr für die inhaltliche Richtigkeit und Vollständigkeit übernommen werden. Die Zusammenfassung orientiert sich an der Informationsschrift „Datenschutz im Verein nach der Datenschutzgrundverordnung (DS-DVO)“ des Landesbeauftragten für den Datenschutz Baden-Württemberg.

- Stand Juni 2019 -

In Vereinen ist die Beachtung des Datenschutzes schon deshalb besonders geboten, da die Erfassung der im Rahmen des Vereinsbeitritts abgefragten Mitgliederdaten in der Regel zu einem hohen Datenaufkommen insgesamt führt. Gleichzeitig hat meist eine größere Zahl an Mitarbeitern im Verein die Möglichkeit hat, auf diese Daten zuzugreifen. Darüber hinaus speichern viele Selbsthilfeorganisationen neben den üblichen Kontaktdaten und Angaben zur Bankverbindung auch sensible Gesundheitsdaten ihrer Mitglieder ab.

Vor diesem Hintergrund sollte Datenschutz im Verein stets ernst genommen und als Qualitätsmerkmal einer guten Vereinsarbeit gesehen werden. Denn je mehr Gewissheit die Mitglieder haben können, dass das Thema Datenschutz ernst genommen wird und die entsprechenden Regelungen auch eingehalten werden, desto größer ist auch das Vertrauen in den Verein, seine Organe und Aktivitäten insgesamt.

Die vorliegende Übersicht beinhaltet die wesentlichen Aspekte, die in einem Verein datenschutzrechtliche Relevanz entfalten. Sie ist nicht abschließend und kann vor allem nicht auf alle Detailfragen, die sich in diesem Zusammenhang ergeben können, eingehen. Das ist schon deshalb nicht der Fall, weil die Mitgliedsorganisationen der BAG SELBSTHILFE in ihrer Größe, Struktur und inhaltlichen Ausprägung durchaus verschieden sind. Nicht-destotrotz soll sie Vorständen, Geschäftsführern, Mitgliederverwaltungen, Datenschutzbeauftragen und allen anderen, die im Verein mit der Erfassung und Verarbeitung von Daten zu tun haben (oder auch nur Spaß und Interesse an dem Thema haben), als Grundlage und Nachschlagewerk in Sachen Datenschutz dienen und vor allem zu einem sorgsamen Umgang mit personenbezogenen Daten sensibilisieren.

In diesem Sinne wünschen wir allen Lesern eine informative und anregende Lektüre!

Ihre

INHALT:

Rechtsgrundlage

Die meisten datenschutzrechtlichen Vorgaben ergeben sich aus der EU-Datenschutzgrundverordnung (DSGVO) und - hierauf basierend – auf dem überarbeiteten Bundesdatenschutzgesetz (BDSG). Daneben können die Landesdatenschutzgesetze, das Telekommunikationsgesetz und andere Regelungen zur Anwendung kommen. Die genannten Normen gelten übrigens für alle Vereine, egal ob es sich um eingetragene Vereine (e.V.) handelt oder nicht. Wichtig ist es, neben den gesetzlichen Regelungen nicht die verbandseigenen Regelungen zu vergessen (etwa Datenschutz-Richtlinien oder Vorstandsbeschlüsse zum Umgang mit Daten), soweit ein Verband solche ergänzend beschlossen hat. Diese verbandsinternen Regelungen müssen natürlich im Einklang mit den gesetzlichen Vorgaben stehen.

Begriffe

Wer einen Blick in die DSGVO und das BDSG wirft, wird einer Reihe an Fachbegriffen und Definitionen begegnen, die zwar erforderlich sind, um zu verstehen, was das Gesetz im Einzelnen meint und bezweckt. Das bedeutet aber nicht, dass es notwendig ist, stur sämtliche Begriffe und Rechtsnormen auswendig zu lernen. Viel wichtiger ist es, erst einmal das notwendige Verständnis für den Datenschutz und einen entsprechenden Automatismus im Umgang mit Daten zu entwickeln. Dafür ist es aber wiederum sinnvoll, wenn gerade die Verantwortlichen im Verein (also insbesondere der Vorstand und der Geschäftsführer) wissen, welche datenschutzrechtlichen Grundsätze bestehen und wo sie im Gesetz Definitionen und Erläuterungen hierzu finden. Von Bedeutung sind insoweit folgende Begriffe:

Personenbezogene Daten:

Geschützt werden personenbezogene Daten. Das sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (vgl. Art. 4 Nr. 1 DSGVO). Hierzu zählen neben Name, Anschrift und Geburtsdatum etwa auch der Familienstand, die Religionszugehörigkeit, das Vorliegen von Krankheiten oder Behinderungen, die berufliche Tätigkeit, Hobbies und nicht zuletzt auch bestehende Vereinsmitgliedschaften einschließlich des Zeitpunkts des Beitritts (und ggf. des Austritts).

Der Datenschutz bezieht sich übrigens nicht nur auf digital erfasste Angaben, sondern für alle Informationen in schriftlicher Form (also egal, ob auf dem Bildschirm oder auf Papier), in Bild-Form (Fotos, Videomitschnitte) oder auch in akustischer Weise (Tonaufnahmen).

Selbsthilfeorganisationen, die von ihren Mitgliedern Angaben über das Bestehen der betreffenden Behinderungs-/Erkrankungsart speichern, sollten unbedingt beachten, dass die DSGVO in Art. 9 an die Verarbeitung bestimmter Daten besondere Anforderungen stellt: Grundsätzlich ist nämlich die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse und 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 untersagt. Nur unter den engen Voraussetzungen des Art. 9 Abs. 2 – 4 ist eine Erfassung und Verarbeitung dieser Daten zulässig. Selbsthilfevereine sollten also im Umgang mit ihnen eine besonders große Sorgfalt an den Tag legen (*hierzu Näheres in den nachfolgenden Abschnitten*).

Verarbeitung von personenbezogenen Daten:

Während in der Vergangenheit noch zwischen Datenerhebung, -verarbeitung, -nutzung und -übermittlung unterschieden wurde, verwendet die DSGVO nur noch allgemein den Begriff der Verarbeitung. Er umfasst jeden Vorgang im Zusammenhang mit personenbezogenen Daten (vgl. Art. 4 Nr. 2 DSGVO). Das bedeutet, dass der Datenschutz nach wie vor mit der Erhebung oder Erfassung beginnt (das ist zum Beispiel die Entgegennahme eines ausgefüllten Beitrittsformulars eines Neumitglieds) und über die Verwahrung dieser Daten (in Form einer elektronischen Speicherung, aber auch die Aufbewahrung von Papierakten, die personenbezogene Daten enthalten) und deren Verwendung innerhalb der Organisation (z.B. um ein Mitglied anzuschreiben) sowie die Weitergabe an Dritte (auch in der Weise, dass dem Dritten eine Einsichtnahme gewährt wird) bis hin zum Löschen oder Vernichten dieser Daten reicht.

Verantwortlicher:

Als Verantwortlicher wird in der DSGVO (vgl. Art. 4 Nr. 7) die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle bezeichnet, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Bei Selbsthilfe-organisationen ist also regelmäßig der Verein (als juristische Person) der „Verantwortliche" im Sinne der DSGVO. Ihm sind insoweit auch seine unselbstständigen Untergliederungen (Abteilungen, Ortsvereine etc.) sowie seine Funktionsträger und Mitarbeiter zuzurechnen, nicht dagegen die Vereinsmitglieder und Dachverbände, in denen der Verein selbst Mitglied ist. Sie sind regelmäßig „Dritter" im Sinne der DSGVO (s.u.).

Dritter:

Gemäß Art. 4 Nr. 10 DSGVO ist „Dritter" im Sinne des Regelungswerks eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftrags-verarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten. Diese Definition ist gerade für Vereine wichtig, denn hier ist oft nicht ohne weiteres erkennbar, ob sich die Weitergabe von Daten noch innerhalb der Organisationseinheit des Verantwortlichen abspielt (z.B. innerhalb der Geschäftsstelle des Verbandes) oder bereits eine Weitergabe an Dritte bedeutet, für die in der Regel eine gesonderte Einwilligung erforderlich ist (*siehe hierzu die weiteren Ausführungen*).

Auftragsverarbeiter:

Manchmal lagern Unternehmen (und auch Vereine) aus Effizienzgründen ihre Datenverarbeitung an eine Fremdfirma aus. Das ist rechtlich zulässig. Nach Art. 4 Nr. 8 DSGVO ist als ein solcher „Auftragsverarbeiter" (das kann eine natürliche oder juristische Person, eine Behörde oder eine Einrichtung sein) derjenige anzusehen, der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Wie zuvor ausgeführt, ist der Auftrags-verarbeiter nicht Dritter gem. Art. 4 Nr. 10 DSGVO.

Grundprinzipen des Datenschutzrechts

Angesichts der Vielzahl an Vorschriften, Begrifflichkeiten, Hinweisen und Warnungen im Zusammenhang mit dem Datenschutz mag sich manch einer überfordert fühlen und vielleicht sogar Sorgen haben, wichtige Vorgaben zu übersehen. Es ist aber auch gar nicht erforderlich, jede Norm und jede Definition auswendig zu lernen. Hilfreich ist es vielmehr, sich zunächst immer wieder klar zu machen, dass es sich bei personenbezogenen Daten um ein schützenswertes Rechtsgut handelt. Ist man sich dessen bewusst, wird man automatisch vorsichtiger im Umgang mit eigenen wie auch mit fremden Daten. Das funktioniert bei anderen Wertgegenständen immerhin genauso: Wohl niemand lässt auf seinem Sitz im Zug seine Brieftasche oder sein Smartphone zurück, wenn er die Toilette oder das Bordbistro aufsucht, und genauso wenig wird man einem Unbekannten auf der Straße auf seine Bitte, ihm 100 Euro zu borgen, leichtfertig den erbetenen Betrag in die Hand drücken mit der Erwartung, derjenige wird das Geld schon irgendwann wieder zurückgeben.

Hilfreich ist es zudem, die folgenden Prinzipien der DSGVO zu verinnerlichen, auf denen die einzelnen Regelungen der DSGVO sowie des BDSG im Grunde genommen aufbauen. An dieser Stelle sollen die Grundsätze nur kurz skizziert werden. Ausführliche Darstellungen zu den einzelnen Punkten finden sich in den nachfolgenden Kapiteln.

1. Verbot mit Erlaubnisvorbehalt

Die DSGVO geht nicht davon aus, dass die Datenerhebung und –verarbeitung grundsätzlich erlaubt ist und nur durch einzelne Regelungen in bestimmten Punkten eingeschränkt wird. Vielmehr besteht umgekehrt das Prinzip, dass eine Datenverarbeitung eigentlich nicht erlaubt ist und nur unter bestimmten Voraussetzungen gestattet ist: das ist der Fall, wenn der Betroffene in die Verarbeitung seiner Daten ausdrücklich eingewilligt hat oder wenn eine gesetzliche Grundlage eine Datenverarbeitung gestattet.

2. Datenvermeidung und Datensparsamkeit

Es gilt das Prinzip, so wenige Daten wie möglich zu erheben und zu speichern. Denn je größer der Datenumfang ist, desto größer ist auch das Risiko einer Datenpanne oder eines Datenmissbrauchs. Das beinhaltet vor allem, nur diejenigen Daten zu erfassen, die zur Zweckerreichung wirklich erforderlich sind und zum anderen Daten, die nicht mehr benötigt werden, unverzüglich zu löschen.

3. Zweckbindung

Erforderlich ist, dass eine Datenverarbeitung nur zu einem konkreten Zweck durchgeführt werden darf. Der Zweck muss festgelegt, eindeutig und rechtmäßig sein. Anlasslos dürfen Daten nicht erhoben und gespeichert werden.

4. Transparenz und Informiertheit

Es muss insbesondere für den Betroffenen erkennbar sein, welche seiner Daten erhoben und verarbeitet werden, was mit ihnen passiert, zu welchem Zweck, für wie lange etc. Demzufolge ist der Verantwortliche verpflichtet, umfangreiche und verständliche Informationen bereitzustellen und auf Wunsch Auskünfte über die Datenverarbeitung zu erteilen. Zudem trifft ihn eine Dokumentationspflicht.

Im Falle einer unzulässigen Datenerhebung steht dem Betroffenen ein Recht auf Berichtigung, Einschränkung der Verarbeitung oder auf Löschung („Recht auf Vergessenwerden“) zu. Erteilte Einwilligungen kann er grundsätzlich jederzeit widerrufen.

5. Datensicherheit

Schließlich verpflichtet die DSGVO den Verantwortlichen zu weitreichenden Sicherungsmaßnahmen, insbesondere im Hinblick auf digitale Verarbeitung. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, der Umstände und Zweck der Datenverarbeitung, aber auch der Eintrittswahrscheinlichkeit und der Schwere des Risikos hat der Verantwortliche geeignete technische und organisatorische Maßnahmen umzusetzen.

Rechtmäßigkeit der Datenverarbeitung

Die eingangs genannten Rechtsgrundlagen beinhalten konkrete Zulässigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten. Zentrale Norm ist dabei Art. 6 Abs. 1 DSGVO. Danach ist die Verarbeitung nur rechtmäßig, wenn eine der in dieser Vorschrift aufgeführten Bedingungen erfüllt ist. Kurz gesagt bedeutet das:

Eine Verarbeitung ist nur dann zulässig, wenn

- die betroffene Person in die Verarbeitung eingewilligt hat

  oder

- eine konkrete Rechtsgrundlage nach der DSGVO, sonstigem Unionsrecht oder auch nach dem Recht der Mitgliedsstaaten eine Verarbeitung erlaubt.

Eine Verarbeitung ist nicht schon deshalb zulässig, weil eine entsprechende gesetzliche Regelung fehlt bzw. weil etwas nicht ausdrücklich verboten ist. Auch reicht es nicht aus, wenn die betroffene Person nicht ausdrücklich widersprochen hat.

Ein Verein braucht nicht für jede einzelne Aktivität, die mit einer Datenverarbeitung verbunden ist, eine individuelle Einwilligung einholen. Das würde die Vereinsarbeit gerade im Bereich der Mitgliederverwaltung schnell zum Erliegen bringen. Deshalb sieht die DSGVO unter anderem vor, dass eine Datenverarbeitung zulässig ist, soweit sie zur Erfüllung eines Vertrages erforderlich ist. Da die Mitgliedschaft in einem Verein regelmäßig auf einem Vertragsverhältnis zwischen dem einzelnen Mitglied und dem Verein beruht (dabei bestimmt in erster Linie die Vereinssatzung den Vertragsinhalt), ist es folglich zulässig, wenn der Verein die notwendigen Daten seiner Mitglieder erfasst und speichert. Dazu gehören vor allem der Name und die Kontaktdaten, da das Mitglied ja beispielsweise zur Mitgliederversammlung eingeladen werden muss. Auch können weitere Daten erhoben werden, wenn dies zur Erfüllung des mitgliedschaftlichen Rechtsverhältnisses, d.h. insbesondere zur Erfüllung des Vereinszwecks, erforderlich ist. Allein die Tatsache, dass die Erfassung bestimmter Daten

hilfreich oder zweckmäßig wäre, genügt indessen nicht. Insoweit müsste vielmehr regelmäßig eine entsprechende Einwilligung eingeholt werden.

Da nach Art. 5 Abs. 1 b) DSGVO die Zwecke, für welche die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen sind, sollte darauf geachtet werden, dass insoweit die Satzung hinreichend klar formuliert ist. Es dürfen vor allem keine überraschenden Regelungen, die zu einer Datenverarbeitung berechtigen, enthalten sein, mit denen das Mitglied bei seinem Vereinsbeitritt nicht rechnen musste.

Bei Selbsthilfeorganisationen stellt sich zuweilen die Frage, ob der Satzungszweck *Selbsthilfe* dazu berechtigt, bei den Mitgliedern auch das Vorliegen der betreffenden Behinderungs- oder Erkrankungsart abzufragen. Da es sich hierbei aber um Gesundheitsdaten handelt, die – wie bereits oben erwähnt – nur unter engen Voraussetzungen verarbeitet werden dürfen, empfiehlt es sich, hier im Zweifel eine entsprechende Einwilligung einzuholen. Art. 9 Abs. 2 d) DSGVO sieht zwar vor, dass eine Verarbeitung zulässig ist durch „Organisationen ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder (…) bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden“. Das bedeutet aber letztlich, dass die Gesundheitsdaten dann auch nur intern, etwa zu reinen statistischen Zwecken erfasst werden dürfen oder um zu prüfen, ob das Mitglied die Voraussetzungen für eine Mitgliedschaft erfüllt - soweit das Vorliegen der betreffenden Behinderung / Erkrankung zwingende Voraussetzung hierfür ist.

Informationspflicht

Der Betroffene ist gem. Art. 13 DSGVO bei der Erhebung seiner Daten datenschutzrechtlich zu unterrichten, damit sich dieser ein umfassendes Bild über den Umfang und den Zweck der Datenverarbeitung machen kann, aber auch weiß, welche Schutzrechte er hat und an wen er sich im Bedarfsfall wenden kann. Im Einzelnen ist anzugeben:

- Name und Kontaktdaten des Verantwortlichen (d.h. hier des Vereins und seines vertretungsberechtigten Vorstands)
- Name und Kontaktdaten des Datenschutzbeauftragten (soweit vorhanden)
- Zweck der Verarbeitung
- Rechtsgrundlage der Verarbeitung
- Berechtigtes Interesse i.S.d. Art. 6 Abs. 1 f DSGVO
- Empfänger der weitergegebenen Daten (bzw. Kategorien von Empfängern), soweit Datenweitergabe stattfindet
- Info, wenn beabsichtigt ist, die Daten in ein Drittland zu transferieren (für Selbsthilfeorganisationen kann das dann relevant werden, wenn eine im Drittland befindliche Cloud für die Mitgliederverwaltung genutzt wird)
- Speicherdauer
- Information über Betroffenenrechte (Auskunftsrecht, Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung, Widerspruchsrecht)
- Hinweis auf Widerrufsmöglichkeit bei Einwilligung
- Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde

Die Zusammenstellung dieser Punkte ist weniger aufwendig als die Liste auf den ersten Blick erscheint. Gerade für den Bereich der Mitgliedschaft ergeben sich letztlich wohl immer dieselben Pflichtangaben, so dass man sie sicherlich in den meisten Fällen bequem wiederverwenden kann. Hinzu kommt, dass auf diejenigen Punkte gar nicht weiter eingegangen werden muss, die nicht relevant sind.

Sollte der Verein die Daten nicht bei der betroffenen Person erhoben, sondern auf andere Weise erhalten haben, ist er genauso zur Information über die oben aufgeführten Punkte verpflichtet und muss darüber hinaus die

Quelle der erhobenen Daten angeben, ferner die Kategorie der verarbeiteten Daten.

Einwilligung

Wie gesehen, ist ein Verein aufgrund des mitgliedschaftlichen Rechtsverhältnisses berechtigt, die erforderlichen Kontaktdaten sowie – wenn der Satzungszweck dies erfordert - weitere Daten des einzelnen Mitglieds zu verarbeiten, ohne dass das Mitglied hierin nochmals ausdrücklich einwilligen müsste. Eine gesonderte Einwilligung ist jedoch dann erforderlich, wenn die entsprechende Datenverarbeitung über die sich aus dem reinen Mitgliedschaftsverhältnis ergebenden Befugnisse hinausgeht.

Ob das der Fall ist, kann im Einzelfall durchaus schwer zu beurteilen sein. Während jedem Mitglied klar ist, dass der Verein seine Kontaktdaten abspeichern muss, um die typischen Vereinsaufgaben, insbesondere auch die Pflichten gegenüber dem Mitglied (z.B. Einladung zur Mitgliederversammlung) zu erfüllen, und deshalb eine Berechtigung sich schon aus dem Vertragsverhältnis ergibt, ist das beispielsweise nicht ohne Weiteres klar, wenn der Verband die Kontaktdaten an ein Verlagshaus weitergibt, damit dieses die dort im Auftrag des Vereins gedruckte Vereinszeitung direkt an die Mitglieder versenden kann. Streng genommen ist nämlich das Verlagshaus Dritter im Sinne von Art. 4 Nr. 10 DSGVO (*vgl. oben*), und eine Weitergabe an diesen Dritten erfordert dann grundsätzlich eine ausdrückliche Einwilligung. Bedient sich der Verein des Verlagshauses jedoch quasi als Gehilfen und geht dies aus der Satzung klar hervor, so dass das Mitglied bei seinem Beitritt (d.h. bei Vertragsabschluss) weiß, dass die Herausgabe seiner Daten erfolgt, um ihm die Vereinszeitung zuzusenden, wird auch diese Datenverarbeitung von dem Vertragsverhältnis erfasst. In diesem Fall ist eine gesonderte Einwilligung also nicht erforderlich. Verschiedene Fallbeispiele werden später noch näher vorgestellt.

Ist nicht klar, ob eine ausdrückliche Einwilligung erforderlich ist, sollte im Zweifel eine solche eingeholt werden. Dies sollte den Verein aber nicht dazu veranlassen, stets eine zusätzliche Einwilligung einzuholen, „um auf Nummer sicher zu gehen“. Denn bei einer Einwilligung kann das Mitglied davon ausgehen, dass es auch ein entsprechendes Widerrufsrecht hat, was im Falle

einer Datenverarbeitung zur Erfüllung eines Vertrages (oder eines anderen Grundes nach Art. 6 Abs. 1 c) – f) DSGVO) aber regelmäßig nicht zutrifft.

Zu beachten ist, dass die Einwilligung auch wirksam sein muss. Und das wiederum erfordert, dass der Einwilligung eine freie Entscheidung des Betroffenen zugrunde liegt und dass er zuvor ausreichend und verständlich darüber informiert worden ist, welche Daten für welchen Zweck verarbeitet werden sollen.

Im Zusammenhang mit der Einholung einer Einwilligung ist darüber zu informieren,

- welche konkreten Verarbeitungsvorgänge geplant sind
- unter welchen Voraussetzungen die Daten an Dritte weitergegeben werden (soweit das beabsichtigt ist)
- dass die Erklärung freiwillig ist
- wie lange die Speicherung der Daten vorgesehen ist
- welche rechtlichen Konsequenzen die Einwilligung nach sich zieht (im Vereinsbereich ist dieser Hinweis wohl in vielen Fällen hinfällig bzw. sehr kurz zu fassen)
- welche Folgen eine Verweigerung der Einwilligung nach sich zieht (nur erforderlich, wenn im Einzelfall erforderlich)
- dass die Einwilligung stets widerrufen werden kann

Diese Auflistung mag bürokratisch und aufwendig erscheinen, sie bedeutet aber nicht, dass zu den einzelnen Punkten seitenweise detaillierte Angaben gemacht werden müssten. Häufig lassen sich die erforderlichen Informationen in zwei oder drei Sätzen zusammenfassen, weil der Verarbeitungszweck klar ist und keine langen Erklärungen erforderlich sind.

Im Übrigen müssen diese Hinweise auch nicht zwingend dokumentiert werden. Es kann aber im Einzelfall sinnvoll sein, die Belehrung schriftlich zu fixieren, weil der Verein insoweit beweispflichtig ist.

Das ist auch im Hinblick darauf von Bedeutung, dass eine Einwilligung nicht zwingend schriftlich erfolgen muss, sondern auch auf elektronische,

mündliche oder konkludente (also durch nicht ausdrücklich, sondern durch schlüssiges Verhalten) Weise abgegeben werden kann. Aus diesem Grunde ist einem Verein aus Gründen der Nachweisbarkeit anzuraten, in der Regel eine schriftliche Einwilligung einzuholen.

Wichtig ist zudem, dass für den Betroffenen die Abgabe seiner Einwilligung sowie die diesbezüglichen Informationen klar erkennbar sind. Lediglich eine Erwähnung im „Kleingedruckten“ reicht nicht; die Erklärung darf dem Betroffenen keinesfalls „untergeschoben“ werden. Wenn also etwa im Zusammenhang mit der Abfrage der Kontaktdaten auf einem Beitrittsformular auch die Einwilligung für eine bestimmte Gegebenheit eingeholt werden soll, für die ein gesondertes Einverständnis erforderlich ist, dann ist dieser Teil des Textes optisch hervorzuheben bzw. vom übrigen Text klar zu trennen.

Ist eine ausdrückliche Einwilligung nach datenschutzrechtlichen Vorgaben erforderlich, kann diese nicht durch einen Vorstands- oder einen Mehrheitsbeschluss in der Mitgliederversammlung ersetzt werden. Auch stellt die alleinige Möglichkeit, einer bestimmten Datenverarbeitung zu widersprechen (etwa in Form eines Ankreuzens der Erklärung „Ich bin mit der Weitergabe meiner Kontakt- und Gesundheitsdaten an die Firma XY nicht einverstanden.“), keine wirksame Einwilligung dar.

Auch Jugendliche können wirksame Einwilligungen abgeben, soweit sie in der Lage sind, die Konsequenzen der Verarbeitung ihrer Daten zu übersehen. Bei Kindern unter 13 Jahren wird man das aber wohl regelmäßig verneinen müssen, so dass hier grundsätzlich die Einwilligung des Sorgeberechtigten erforderlich ist.

Mitgliederdaten

Der Beitritt einer Person zu einem Verein begründet, wie bereits erwähnt, zwischen diesen beiden ein mitgliedschaftliches Vertragsverhältnis. Das bedeutet, dass der Verein diejenigen personenbezogenen Daten des Mitglieds

verarbeiten darf, die zur Verfolgung der Vereinsziele und für die Betreuung und Verwaltung der Mitglieder erforderlich sind. Hierunter fallen regelmäßig Name, Anschrift, Geburtsdatum und Bankverbindung. Das bedeutet im Umkehrschluss, dass darüber hinausgehende Daten grundsätzlich nur mit ausdrücklicher Einwilligung erfasst und gespeichert werden dürfen.

Soweit Selbsthilfeorganisationen bei Neumitgliedern abfragen, ob diese von der betreffenden Behinderungsart oder chronische Erkrankung, mit der sich der Verband befasst, betroffen sind, sollte - wie bereits eingangs hingewiesen – eine gewisse Vorsicht und Zurückhaltung an den Tag gelegt werden. Denn zum einen handelt es sich bei diesen Gesundheitsangaben um besonders sensible Daten, deren Verarbeitung grundsätzlich mit erheblichen Risiken für die Grundrechte und Grundfreiheiten des Betroffenen verbunden ist. Vor allem kann die Kenntnis eines Dritten über das Vorliegen der Behinderung / Erkrankung zu Nachteilen im Alltag führen, etwa wenn sich der Betroffene aufgrund einer Stellenausschreibung bewirbt oder eine Versicherung abschließen will.

Zum anderen ist eine Verarbeitung von Gesundheitsdaten nur eingeschränkt zulässig. Ob allein die Tatsache, dass es sich um eine Selbsthilfeorganisation handelt (und dies auch durch den in der Satzung enthaltenen Vereinszweck zum Ausdruck kommt), zu einer Verarbeitung der betreffenden Gesundheitsdaten der Mitglieder befugt, ist – wie bereits gesagt - nicht ganz zweifelsfrei. Zumindest wenn es sich um Daten handelt, die über die über eine reine statistische und anonymisierte Erfassung hinausgehen bzw. weitere Gesundheitsdaten wie Diagnosen, Begleiterkrankungen, Medikamenteneinnahmen o.a. beinhalten, sollte auf jeden Fall eine ausdrückliche (und aus Gründen der Nachweisbarkeit) schriftliche Einwilligung eingeholt werden. Wichtig ist jedoch: Aus dem grundsätzlichen Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO und dem Gebot zur Datensparsamkeit folgt, dass nur diejenigen Gesundheitsdaten abgefragt werden dürfen, die für die Arbeit als Selbsthilfeorganisation wirklich erforderlich sind.

Im Falle einer Doppelmitgliedschaft, etwa im rechtlich selbständigen Landesverband und im übergeordneten Bundesverband, ist es erforderlich, dass das Neumitglied über diesen Umstand hinreichend informiert wird und

Beitrittserklärungen gegenüber beiden Vereinen abgibt. Da es sich trotz der gemeinsamen Vereinsstruktur datenschutzrechtlich in der Regel um zwei Verantwortliche handelt, berechtigt die Doppelmitgliedschaft auch nicht ohne weiteres zur Weiterleitung von Daten, es sei denn dies ist geht aus den Vereinssatzungen hinreichend hervor oder es ist eine entsprechende Einwilligung des Mitglieds eingeholt worden. Das ist vor allem zu beachten, wenn ein selbständiger Landes- oder Regionalverband dazu verpflichtet ist, regelmäßig Mitgliederlisten an den Bundesverband zu senden. Das gilt vor allem, wenn es sich bei beiden um rechtlich eigenständige Vereine handelt. Bei unselbständigen Untergliederungen ist eine gemeinsame Verwaltung und damit auch die Weitergabe innerhalb der Organisation (als einziger Verantwortlicher) zulässig, ohne dass hierfür eine zusätzliche Einwilligung erforderlich wäre. Auch eine Satzungsregelung über die Weiterleitung ist in einem solchen Fall nicht erforderlich, allerdings sollte im Rahmen der Informationen an das Mitglied über die erfolgende Datenverarbeitung auch dargelegt werden, in welcher Form eine Nutzung stattfindet (z.B. durch einen Hinweis, dass die im Landesverband erfassten Mitgliedsdaten beim Bundesverband verwaltet werden).

Datenverarbeitung aufgrund eines berechtigten Interesses

Die DSGVO lässt in Art. 6 Abs. 1 f) eine Datenverarbeitung ausnahmsweise auch dann zu, wenn der Verantwortliche ein berechtigtes Interesse hieran hat. Das ermöglicht es einem Verein, Daten in einem bestimmten Umfang auch zu anderen Zwecken als zur Verfolgung der Vereinsziele oder zur Mitgliederverwaltung zu erheben und zu nutzen. Wegen des besonderen Vertrauensverhältnisses zwischen dem Verein und seinen Mitgliedern ist eine solche Datenverarbeitung aber nur in Ausnahmefällen zulässig. Vor allem dürfen insoweit nicht die Interessen und Grundrechte der betroffenen Person (in datenschutzrechtlicher Hinsicht) überwiegen. Das dürfte in der Praxis aber sehr häufig der Fall sein, zum Beispiel bei wirtschaftlichen oder beruflichen Gründen und vor allem wenn es um die Privat- und Intimsphäre des Betroffenen geht, etwa gesundheitliche Aspekte. Übrigens geht die DSGVO bei Kindern unter 16 Jahren davon aus, dass hier die schutzwürdigen Interessen des Kindes regelmäßig überwiegen.

Datenerhebung bei Nichtmitgliedern

Der Verein kann grundsätzlich auch von Nichtmitgliedern personenbezogene Daten erheben, soweit dies zur Wahrnehmung berechtigter Interessen des Vereins erforderlich ist und keine schutzwürdigen Belange der Betroffenen entgegenstehen. Können beispielsweise neben Mitgliedern auch Nicht-mitglieder an Vereinsveranstaltungen teilnehmen, ist in der Regel auch die Erfassung von notwendigen Daten (etwa Name, Anschrift und ggf. auch das Geburtsdatum) dieser Personengruppe zulässig. Das gilt gerade auch für Treffen von Selbsthilfegruppen, an denen auch Nichtmitglieder teilnehmen dürfen und der Verein zwecks Kontaktierung der Betreffenden oder aus anderen wichtigen Gründen auch von ihnen personenbezogene Daten erfassen muss. Ermächtigungsgrundlage ist hierfür in der Regel auch der zuvor erwähnte Art. 6 Abs. 1 f) DSGVO, unter Umständen auch Art. 6 Abs. 1 b), soweit man in der regelmäßigen Teilnahme eine vertragliche Beziehung zwischen dem Gruppenteilnehmer und dem Verein (als Veranstalter der Gruppentreffen) sieht. Werden von Nichtmitgliedern Daten erfasst, die über die reinen Kontaktdaten hinausgehen, ist hierfür in der Regel eine ausdrückliche Einwilligung notwendig.

Datenschutz in der Selbsthilfegruppe

Das Thema Datenschutz sollte auch in einer Selbsthilfegruppe angesprochen werden. In der Regel ist eine Selbsthilfegruppe eine Gliederung bzw. Bestandteil des Verbandes, so dass der Verein auch hier „Verantwortlicher“ im Sinne der DSGVO bleibt. Hier kommen also die gleichen datenschutz-rechtlichen Regelungen zur Anwendung wie an allen anderen Bereichen des Vereins. Das gilt vor allem bezüglich derjenigen personenbezogenen Daten, die der Verein möglicherweise bewusst abfragt und erfasst (etwa durch den vom Verein bestellten Gruppenleiter).

Persönliche Informationen, die die Teilnehmer im Verlauf des Gesprächs von sich aus machen, gehen regelmäßig mit der (konkludenten) Einwilligung einher, dass die betreffenden personenbezogenen Daten von den anderen auch zur Kenntnis genommen werden. Da die anderen Teilnehmer keine „Verantwortlichen“ im Sinne der DSGVO sind, bestehen für diese insoweit auch keine datenschutzrechtlichen Pflichten. Nichtsdestotrotz ist es jedoch

wichtig, alle Beteiligten für den Datenschutz zu sensibilisieren. Vor dem Hintergrund, dass in einem Gruppengespräch regelmäßig höchstpersönliche Dinge zur Sprache kommen, sollte allen Teilnehmern immer wieder klar gemacht werden, dass es sich bei solchen personenbezogenen Daten um ein wertvolles Rechtsgut handelt, das das Persönlichkeitsrecht des Einzelnen unmittelbar betrifft. Aus diesem Grunde sind alle Informationen und Angaben, die in der Gruppe zur Sprache kommen, vertraulich zu behandeln und nicht nach außen zu tragen. Dies sollte nicht nur einem neuen Teilnehmer zu Beginn seines ersten Besuchs mitgeteilt werden, sondern in regelmäßigen Abständen immer wieder in der Gruppe zur Sprache kommen.

Da der Verein in der Regel als „Veranstalter“ der Gruppentreffen auftritt, ist zu empfehlen, dass er auch aus eigenem Interesse das Thema Datenschutz hervorhebt und die erforderlichen datenschutzrechtlichen Hinweise erteilt und zugleich erklärt, dass er die im Gespräch preisgegebenen Daten nicht erfasst und verarbeitet.

Personaldaten

Beschäftigt der Verein hauptamtliche Mitarbeiter, ist er gem. Art. 88 DSGVO und § 26 BDSG dazu berechtigt, deren personenbezogenen Daten für Zwecke des Beschäftigungsverhältnisses zu verarbeiten, wenn dies für die Entscheidung über die Begründung des Beschäftigungsverhältnisses, für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung ergebenden Rechte und Pflichten der Interessen-vertretung der Beschäftigten erforderlich ist.

Auch hier gilt die Hinweispflicht nach Art. 13 DSGVO, d.h. wenn die Daten des Mitarbeiters erhoben werden, ist er über den Verarbeitungszweck, den Rechtsgrund, die Dauer der Speicherung etc. zu informieren.

Wichtig ist es auch, die Personalakten der Mitarbeiter sorgfältig zu führen und möglichst nur einem kleinen Kreis von Berechtigten hierauf Zugriff zu gewähren. Ist beispielsweise ein Vorstandsmitglied für Personalangelegen-heiten zuständig, darf er ohne Einwilligung des betreffenden Arbeitnehmers grundsätzlich keine Personaldaten an ein anderes Vorstandsmitglied weiterleiten.

Speicherung und Sicherung personenbezogener Daten

Eine Speicherung der Daten kann erfolgen

- mittels herkömmlicher Karteien oder Akten
- automatisiert, d.h. EDV-gestützt
- im Wege einer Auftragsdatenverarbeitung durch ein externes Service-unternehmen

Zu beachten ist, dass bei der Speicherung unterschiedliche Datengruppen voneinander zu trennen sind, also z.B. die Mitgliederdaten von den Personaldaten.

Zudem sind regelmäßig besondere Sicherungsmaßnahmen erforderlich: So sind nach Art. 32 DSGVO bei der Verarbeitung personenbezogener Daten geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das sind zunächst die in der erwähnten Rechtsnorm enthaltenen Mindestanforderungen (Verschlüsselung, Pseudonymisierung, technische und organisatorische Maßnahmen, regelmäßige Überprüfungen der Wirksamkeit der Sicherungs-maßnahmen etc.). Sicherzustellen ist vor allem, dass Unbefugte keinen Zugriff auf die gespeicherten Daten nehmen können. Dies kann u.a. durch die Einrichtung passwortgeschützter Nutzer-Accounts und eines Firewall-Systems geschehen, in der Regel ist zudem – wie auch Art. 32 vorgibt - die Verschlüsselung der Mitgliederdaten anzuraten. Wichtig sind natürlich nicht zuletzt auch regelmäßige Sicherheits-Updates.

Entsprechende Vorsichtsmaßnahmen sind natürlich auch dann erforderlich, wenn die Datenverarbeitung für den Verein durch einen Ehrenamtlichen zuhause an seinem Privat-Computer erledigt wird. Dabei muss das eigene Wohnzimmer natürlich nicht in einen IT-Hochsicherheitstrakt umfunktioniert werden. Es sind aber auch hier die zum Schutz vor einem unbefugten Zugriff erforderlichen Maßnahmen zu ergreifen, also etwa die Sperrung des PC bei Verlassen des Arbeitsplatzes, die Einrichtung eines Passwort-Schutzes sowie eines auf aktuellem Stand befindlichen Computer- und Internet-Schutzes. Es sollte übrigens auch daran gedacht werden, dass der eigene Ehepartner und andere Familienangehörige regelmäßig unbefugte Dritte sind, wenn es um Mitglieder- oder andere personenbezogene Daten geht, die für den Verein zuhause gespeichert und verwaltet werden.

Natürlich sind auch Daten, die auf Papier festgehalten sind und bei einem Verein verwahrt werden – etwa die Akten einer Rechtsberatung, Personalakten oder aber auch ausgedruckte Mitgliederlisten -, vor der Einsichtnahme und dem Zugriff unbefugter Dritter zu sichern. Sie sollten daher auch bei einem nur kurzzeitigen Verlassen des Arbeitsplatzes vor dem Blick anderer geschützt werden und erst recht nach Beendigung einer Bearbeitung in einem Aktenschrank o.a. verschlossen werden. Das gilt erst recht, wenn die Unterlagen sensible Gesundheitsdaten enthalten.

Auftragsverarbeitung

Eine Auslagerung der Datenverarbeitung an Externe ist zulässig, wenn sich der Verein jegliche Entscheidungsbefugnis über die Verwendung der Daten vorbehält und dem anderen auch grundsätzlich keinen eigenen inhaltlichen Bewertungs- und Ermessensspielraum einräumt; der Auftragsverarbeiter handelt also weisungsabhängig. Verglichen mit der alten Rechtslage ist neben dem Verantwortlichen nunmehr aber auch der Auftragsverarbeiter stärker in Pflicht und kann im Falle einer Datenpanne zur Verantwortung gezogen werden.

Der Verein als Verantwortlicher muss indessen dafür Sorge tragen, dass er einen Auftragsverarbeiter beauftragt, der eine hinreichende Garantie für eine datenschutzgerechte Datenverarbeitung gewährleistet; am einfachsten ist es insoweit, sich eines Unternehmens zu bedienen, das über eine entsprechende Zertifizierung i.S. des Art. 42 DSGVO und anerkannte Verhaltensregeln gem. Art. 40 DSGVO verfügt.

Wichtig ist, dass die Datenverarbeitung auf der Grundlage eines bindenden Vertrages erfolgt. Dieser muss nach Art. 28 Abs. 3 DSGVO bestimmte Anforderungen erfüllen (u.a. Bezeichnung des Gegenstands und der Dauer der Auftragsdatenvereinbarung, Angaben zu Umfang, Art und Zweck der Datenerhebung, Nennung der Pflichten und Rechte des Verantwortlichen, Angabe des Umfangs der Weisungen - die zu dokumentieren sind -, Verpflichtung des vom Auftragsverarbeiter eingesetzten Personals auf das Datengeheimnis, Regelung der technischen und organisatorischen Maßnahmen etc.)

In der Vergangenheit hatten der Verein und die extern beauftragte Adressverwaltung eine Einheit gebildet; nach der DSGVO ist das nicht mehr der Fall, weshalb die Daten vom Verein an den Auftragsverarbeiter *übermittelt* werden. Hierfür ist aber regelmäßig keine entsprechende Einwilligung des einzelnen Mitglieds erforderlich, weil sich der Verein im Rahmen seiner autonomen und eigenverantwortlichen Organisation durchaus einer externen Auftragsverarbeitung bedienen kann. Deshalb ist im Falle der Beauftragung eines Auftragsverarbeiters von einer Datenverarbeitung aufgrund eines berechtigten Interesses auszugehen, Art. 6 Abs. 1 f) DSGVO.

Trotz der neuen Verantwortlichkeit des Auftragsverarbeiters bleibt der Verein als Verantwortlicher dazu verpflichtet, die Rechte der Betroffenen (z.B. Informationspflichten, Auskunftsansprüche, Widerspruchsrecht, Recht auf Löschung) sicherzustellen. Um seinen eigenen Pflichten nachzukommen, ist er natürlich in der Pflicht, den Auftragsverarbeiter stets darauf zu kontrollieren, ob dieser die datenschutzrechtlichen Vorgaben einhält. Natürlich hat der Verein umgekehrt den Betroffenen auch darüber zu informieren, dass er sich eines Auftragsverarbeiters bedient und ob insoweit die Daten ggf. sogar in Drittländern verarbeitet werden.

Als Auftragsverarbeiter sind übrigens auch solche Firmen anzusehen, deren Datenbankserver der Kunde – hier also der Verein – über das Internet nutzt, wo die Daten anstelle auf einer eigenen EDV-Anlage des Vereins gespeichert werden. Immer häufiger bedient man sich auch einer sog. Cloud. Auch bei deren Nutzung liegt eine Auftragsdatenverarbeitung vor. Zu berücksichtigen ist hier jedoch, dass die Verarbeitung häufig in einem Land außerhalb der EU stattfindet, was nach der DSGVO aber zulässig ist. Die DSGVO bleibt insoweit auch regelmäßig weiter anwendbar, soweit der Verantwortliche oder der Auftragsverarbeiter mit Hauptsitz oder einer Niederlassung in der EU ansässig ist. Werden die Daten an einen Auftragsverarbeiter außerhalb der EU weitergegeben, sind jedoch die besonderen Vorgaben zur Sicherstellung des Datenschutzniveaus nach der DSGVO zu beachten.

Nutzung personenbezogener Daten

Ein Vorstandsmitglied oder auch ein hauptamtlicher Mitarbeiter eines Vereins darf grundsätzlich nur die zur Erfüllung ihrer Aufgaben erforderlichen Mitgliederdaten kennen und entsprechend verarbeiten. Der Aufgabenbereich ergibt sich in der Regel durch die Satzung und durch andere Geschäfts- bzw. Vereinsordnungen. So ist es beispielsweise regelmäßig ausreichend, wenn der Kassierer nur die für den Einzug der Mitgliedsbeiträge relevanten Daten (Name, Anschrift, Bankverbindung) kennt und entsprechend nutzt. Muss allerdings der gesamte Vorstand auf die Mitgliederdaten zugreifen um seine Aufgaben zu erfüllen, steht ihm dieses Zugriffsrecht selbstverständlich zu.

Neben Mitgliedsdaten fallen bei einem Verein auch regelmäßig Daten von Dritten (Lieferanten, Besuchern etc.) an. Deren Speicherung und Nutzung ist zulässig, wenn dies zur Begründung oder Durchführung eines Schuldverhältnisses (Vertrages) erforderlich ist. Eine darüber hinausgehende Nutzung zu einem anderen Zweck setzt ein entsprechendes berechtigtes Interesse des Vereins voraus, dem kein schutzwürdiges Interesse des Betroffenen entgegenstehen darf (*vgl. hierzu die obigen Ausführungen zu Art. 6 Abs. 1 f) DSGVO*). Eine solche Nutzung wird in der Praxis also nur in Ausnahmefällen in Betracht kommen.

Spendenaufrufe und Werbung

Die Nutzung von Daten für Spendenaufrufe und Werbung ist grundsätzlich nur zur Erreichung der eigenen Ziele des Vereins zulässig. Insoweit können also die eigenen Mitglieder problemlos angeschrieben und etwa um Spenden für den eigenen Verein gebeten werden. Geschieht dies regelmäßig, ist zu empfehlen, eine entsprechende Regelung in der Datenschutzordnung des Vereins zu treffen. Nicht zulässig ist indessen die Verwendung der Mitgliederdaten, um für andere Organisationen oder Aktionen zu werben; insoweit ist die vorherige Einwilligung des einzelnen Mitglieds erforderlich.

Gleiches gilt, wenn Nichtmitglieder zwecks Werbung für den Verein angeschrieben werden sollen. Auch sie müssen dann grundsätzlich vorab in die entsprechende Nutzung ihrer Daten eingewilligt haben. In bestimmten Fällen wird man eine Nutzung auch unter dem Gesichtspunkt des

berechtigten Interesses (Art. 6 Abs. 1 f) DSGVO) zulassen können, etwa wenn ein Nichtmitglied wiederholt Veranstaltungen des Vereins besucht und seine Beziehungen und Erwartungen an den Verein daher anders zu bewerten sind als bei einer Person, die bisher keinerlei Interesse am Verein gezeigt hat bzw. mit ihm noch nicht in Kontakt getreten ist.

Sendet der Verein oder ggf. auch eine von ihm beauftragte Firma einem Adressaten eine Werbesendung zu, muss für den Empfänger erkennbar sein, woher der Verein seine Daten hat. Wichtig ist in diesem Zusammenhang, dass der Verein seiner Hinweis- und Informationspflicht hinreichend nachkommt und den Betroffenen auch stets deutlich auf sein Widerspruchsrecht hinweist.

Übermittlung personenbezogener Daten

Daten von Mitgliedern dürfen an Dritte grundsätzlich nur weitergegeben werden, wenn dies zur Erreichung des Vereinszwecks bzw. zur Verwaltung und zur Betreuung der Mitglieder erforderlich ist. Anderenfalls ist auch hier eine ausdrückliche Einwilligung erforderlich.

Dritte sind auch die einzelnen Vereinsmitglieder. Diese haben nur unter ganz bestimmten Voraussetzungen ein Anrecht auf Erhalt der Mitgliederliste, so z.B. wenn laut Satzung der Vereinszweck darin besteht, die persönlichen Kontakte zu pflegen. Manche sehen hierin ein berechtigtes Interesse gem. Art. 6 Abs. 1 f) DSGVO, das zu einer Weitergabe berechtigt. In diesem Fall ist der Empfänger der Daten aber unbedingt darauf hinzuweisen, dass die erhaltenen Daten nur für die Kontaktherstellung verwendet werden dürfen und vor allem eine Weitergabe an Dritte nicht zulässig ist.

Dessen ungeachtet ist grundsätzlich zu empfehlen, sich im Hinblick auf die Herausgabe ohne Einwilligung äußerst restriktiv zu verhalten:

Angesichts der Tatsache, dass Mitglieder von Selbsthilfeorganisationen meist Betroffene der jeweiligen Erkrankung oder Behinderungsart oder Angehörige solcher Betroffenen sind und damit zumindest indirekt sensible Gesundheitsdaten von Mitgliedern bekannt werden, sollten Daten allenfalls dann herausgegeben werden, wenn aus der Satzung hinreichend deutlich hervorgeht, dass die Kontaktpflege untereinander Inhalt des Vereinszwecks

ist, so dass die Herausgabe für das Mitglied nicht überraschend ist. Letzteres ist aber auch bei Selbsthilfeverbänden nicht immer zwingend anzunehmen. Aus diesem Grunde wird empfohlen, vor der Herausgabe von Mitgliedsdaten an ein anderes Mitglied stets eine entsprechende Einwilligung einzuholen.

Auch im Falle eines ausdrücklichen Einverständnisses mit der Herausgabe ist zu beachten, dass dann nur die wirklich notwendigen Daten weitergegeben werden. Das sind im Zweifel nur Name und Telefonnummer, damit die betreffenden Mitglieder untereinander in Kontakt treten können. Alternativ besteht die Möglichkeit, dass der Verein einem Mitglied lediglich mitteilt, dass bei einem anderen Mitglied das Interesse an einem Kontakt besteht, und sollte das Interesse auf Gegenseitigkeit beruhen, könnte der andere beim Verein die entsprechenden Daten des Anfragenden abrufen.

Sollten sich Teilnehmer einer Selbsthilfegruppe außerhalb der Treffen austauschen wollen, steht es ihnen selbstverständlich frei, gegenseitig ihre Kontaktdaten auszutauschen. Das ist dann kein Grund für den Verein, datenschutzrechtlich aktiv zu werden. Werden aber von Teilnehmern entsprechende Bitten um Herausgabe von Daten anderer Teilnehmer an den Verein gerichtet (etwa an den vom Verein bestellten Gruppenleiter), gilt hier das zuvor Gesagte: es sollte zunächst eine ausdrückliche Einwilligung zur Herausgabe vom Betroffenen eingeholt werden, da auch im Rahmen einer Selbsthilfegruppe nicht zwingend davon auszugehen ist, dass ein Teilnehmer neben dem verbalen Austausch innerhalb der Gruppe einen Kontakt mit anderen bzw. eine Bekanntgabe seiner personenbezogenen Daten wünscht. Dabei spielt es keine Rolle, ob der Teilnehmer Mitglied des Vereins oder Nichtmitglied ist.

Vereinsrechtlich kann die Herausgabe der Mitgliederliste an einzelne Mitglieder auch aus anderem Grunde erforderlich und geboten sein. Das ist insbesondere der Fall, wenn die Einberufung einer außerordentlichen Mitgliederversammlung begehrt wird und hierfür eine bestimmte Mitgliederquote laut Satzung erreicht werden muss, damit eine solche Versammlung stattfinden kann. Auch in einem solchen Fall sollte unbedingt der Hinweis ergehen, dass die Liste nicht zu anderen (z.B. kommerziellen) Zwecken verwendet oder an Dritte herausgegeben werden darf; dies sollte man sich möglichst schriftlich zusichern lassen.

Allerdings sollte immer auch geprüft werden, ob nicht andere Mittel zur Erreichung des Ziels zur Verfügung stehen, z.B. ein entsprechender Aufruf in der Verbandszeitung. Auch ist zu überlegen, einen Treuhänder einzuschalten, der die Kontaktdaten erhält, um die Mitglieder dann von seiner Seite entsprechend zu informieren. Dieser darf die Mitgliederliste dann natürlich nicht seinerseits an einzelne Mitglieder oder an Dritte außerhalb des Vereins weitergeben.

Mitgliedschaft in einem Dachverband

Ein Dachverband, bei dem nur der Verein, nicht aber auch seine Einzelmitglieder Mitglied sind, ist Dritter im Sinne der DSGVO, wenn die Daten der Einzelmitglieder an diesen weitergegeben werden sollen. Daher ist grundsätzlich vorab eine Einwilligung einzuholen, es sei denn die Weitergabe dient der Erfüllung des Vereinszwecks und es überwiegen keine Interessen oder Grundrechte oder Grundfreiheiten der betroffenen Person. Wenn beispielsweise ein Mitgliedsverband dazu verpflichtet ist, regelmäßig eine Mitgliederliste an den Dachverband zu übermitteln, ist es hilfreich, dies in der Satzung zu verankern, damit für das Einzelmitglied von vornherein klar ist, dass seine Daten im Vereinsinteresse an den Dachverband weitergeleitet werden. Fehlt es an einer solchen Satzungsregelung, empfiehlt es sich dringend, die Mitglieder über die Weitergabe zu informieren und ihnen damit Gelegenheit zu Einwendungen zu geben.

Gegenüber dem Dachverband muss aber auch klargestellt werden, dass dieser die Daten nicht zu anderen als den eigenen Vereinszwecken verwenden darf. Wenn er also die Mitgliederliste benötigt, um die Vereinsmitgliedschaft der entsendeten Delegierten zu prüfen, darf sie auch nur hierzu genutzt werden (wobei auch dem Dachverband klar sein dürfte, dass er die Liste dann beispielsweise nicht an eine Werbefirma verkaufen darf).

Das Gesagte gilt natürlich auch im Verhältnis zwischen einer rechtsfähigen Untergliederung (z.B. ein eingetragener Landesverband) und seinem ebenfalls eingetragenen Bundesverband.

Datenweitergabe an Förderstelle

Führt ein Verein eine von einem Träger geförderte Veranstaltung durch – etwa im Rahmen einer Projektförderung durch eine Krankenkasse -, verlangt die betreffende Förderstelle manchmal zum Nachweis und zur Kontrolle ihrer eigenen Mittelvergabe eine Teilnehmerliste mit Namen, Anschrift und Unterschrift der Teilnehmer der Veranstaltung. Grundsätzlich wird man wohl davon ausgehen können, dass für die Weitergabe ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 f) DSGVO besteht, und zwar auch dann, wenn an der Veranstaltung neben Mitgliedern auch Nichtmitglieder teilgenommen haben.

Da die Teilnehmer im Zusammenhang mit der Datenerhebung ohnehin gem. Art. 13 DSGVO zu informieren sind, werden sie in diesem Zusammenhang über die Weitergabe der Daten informiert und können entscheiden, ob sie dennoch an der Veranstaltung teilnehmen oder nicht. Deshalb sollte man den Hinweis auf die Weiterleitung auch optisch hervorheben. Nichtdestotrotz ist es hilfreich, im Vorfeld auch noch einmal mit der betreffenden Förderstelle die datenschutzrechtliche Problematik zu erörtern. In vielen Fällen rücken die Träger inzwischen von dem Erfordernis einer Teilnehmerliste mit personenbezogenen Daten ab.

Datenweitergabe an Unternehmen

Die Weitergabe von Mitgliederdaten an Sponsoren und Firmen zu Werbezwecken ist grundsätzlich unzulässig, weil die Weitergabe in der Regel nicht vom Vereinszweck gedeckt ist. Insoweit ist also regelmäßig eine entsprechende ausdrückliche Einwilligung der Betroffenen erforderlich, erst recht wenn besonders schutzwürdige Daten betroffen sind (z.B. Gesundheitsdaten). Wichtig ist dabei, neben den weiteren erforderlichen Informationen über die Datenverarbeitung deutlich auf das jederzeitige Widerspruchsrecht hinzuweisen.

Liegt ein Einverständnis zur Übermittlung der Mitgliederdaten zu Werbe- oder anderen Zwecken vor, ist dringend zu empfehlen, die entsprechende Liste vor ihrer Herausgabe immer nochmals auf ihre Aktualität und vor allem auf mögliche, zwischenzeitlich ergangene Widersprüche einzelner Mitglieder

zu überprüfen. Bitten von Firmen auf Herausgabe von Adresslisten sollten aber ohnehin immer äußerst zurückhaltend behandelt werden; vor allem darf ein Mitglied niemals dazu gedrängt werden, sein Einverständnis zur Herausgabe zu erteilen.

Vor dem Hintergrund, dass gerade Pharmakonzerne oder auch Hilfsmittelhersteller oft ein großes Interesse an Informationen über die gesundheitliche Situation und den entsprechenden Bedarf von Betroffenen haben, ist bei Selbsthilfeorganisationen durchaus Vorsicht geboten im Umgang mit den personenbezogenen Daten ihrer Mitglieder. Das bedeutet zwar nicht, dass allgemeine Informationen oder Erfahrungswerte ohne Bezugnahme auf konkrete Personen nicht weitergegeben werden dürften. In diesem Fall stellt sich aber für Selbsthilfeverbände schnell die Frage, ob ein zu enger Austausch und eine zu intensive Zusammenarbeit mit Wirtschaftsunternehmen die erforderliche Neutralität und Unabhängigkeit der Selbsthilfe untergräbt (*vgl. insoweit die veröffentlichten Leitsätze für die Zusammenarbeit mit Wirtschaftsunternehmen der BAG SELBSTHILFE und des FORUMs im PARITÄTISCHEN*).

Das Erfordernis einer schriftlichen Einwilligung besteht natürlich auch im Zusammenhang mit dem Abschluss eines Gruppenversicherungsvertrages, aufgrund dessen die Vereinsmitglieder dann Einzelverträge zu günstigeren Konditionen abschließen können. Selbstverständlich dürfen auch hier die Kontaktdaten nicht ohne schriftliche Einwilligung herausgegeben werden - auch wenn den Mitgliedern ein wirtschaftlicher Vorteil entstehen könnte.

Soweit manche Versicherungsunternehmen behaupten, es seien in diesem Falle geringere Anforderungen an den Datenschutz zu stellen, sollte auf die Richtigkeit dieser Aussage nicht vertraut werden. Zumindest die Datenschutzaufsichtsbehörden der Länder teilen diese Rechtsauffassung nicht; sie verlangen sogar vielmehr, dass der Verein dem Versicherungsunternehmen die Mitgliedsdaten nur dann übermitteln darf, wenn das betreffende Mitglied eine ausdrückliche und informierte schriftliche Einwilligung erteilt hat.

Bekanntgaben in der Vereinszeitung und am „Schwarzen Brett“

Personenbezogene Informationen in Vereinspublikationen sind nur begrenzt zulässig, nicht zuletzt deshalb, weil hier der tatsächliche Adressatenkreis nicht feststellbar ist. So kann ein Mitglied die an ihn versandte Vereinszeitung immerhin problemlos an einen Dritten weiterreichen. Eine Bekanntgabe ist deshalb nur zulässig, wenn es für die Erreichung des Vereinszwecks unbedingt erforderlich ist. Dabei dürfen aber keine schutzwürdigen Interessen des Betroffenen entgegenstehen, was zum Beispiel regelmäßig dann der Fall ist, wenn es sich um Mitteilungen mit ehrenrührigem Inhalt (Verhängung einer Vereinsstrafe, Planung eines Vereinsausschlusses o.a.) handelt. Aber auch schon die Tatsache, dass jemand Mitglied eines Selbsthilfeverbandes ist und dementsprechend vermutet werden kann, dass diese Person von der jeweiligen Erkrankung oder Behinderung, mit der sich die Organisation befasst, selbst betroffen ist, verpflichtet den Verband zu einer deutlichen Zurückhaltung.

Bei typischen Mitteilungen wie Vereinsbeitritten, Geburtstagen oder Jubiläen ist auf jeden Fall anzuraten, vorab abzuklären, ob das Mitglied mit einer entsprechenden Veröffentlichung einverstanden ist. Das gilt natürlich erst recht, wenn zugleich ein Foto des Betroffenen mit veröffentlicht werden soll oder wenn weitere Informationen aus dem persönliche Lebensbereich des Mitglieds veröffentlicht werden sollen, durch die womöglich sogar personenbezogene Daten weiterer Personen bekannt werden (z.B. im Falle einer Eheschließung oder bei der Geburt eines Kindes). Selbst wenn eine Bekanntgabe (z.B. eines runden Geburtstages) in der Vereinspublikation üblich ist und dem auch bisher niemand widersprochen hat, heißt das nicht, dass ein anderes Mitglied einer Bekanntgabe seiner Daten auch automatisch zustimmt.

Übrigens ist auch die Nachricht, dass eine bestimmte Person eine Spende an den Verein gerichtet hat, nur nach vorheriger Einwilligung des Spenders zulässig, zumindest dann wenn es sich um ein Nichtmitglied handelt. Aber auch bei der Spende seitens eines Mitglieds wird man nicht ohne weiteres ein überwiegendes Interesse des Vereins gegenüber den Interessen des Betroffenen bejahen können, weshalb man auch hier im Zweifel eine vorherige Einwilligung einholen sollte.

Etwas anderes ist hingegen der Fall, wenn die Namen des Vorstandes oder anderer in der Vereinsführung tätigen Personen sowie deren dienstliche Kontaktdaten bekannt gegeben werden. Diese Informationen liegen grundsätzlich im Vereinsinteresse, weshalb hier die Einholung einer zusätzlichen Einwilligung nicht erforderlich ist. Wichtig ist es aber auch hier, sich auf die notwendigen Daten zu beschränken; Privatadressen von ehren- wie hauptamtlichen Mitarbeitern und erst recht Angaben über das Vorliegen einer Erkrankung bzw. Behinderung dürfen nicht ohne deren Einverständnis veröffentlicht werden bzw. sollten möglichst gar nicht erst eingeholt werden.

Ähnliches gilt auch für Veröffentlichungen am „Schwarzen Brett“. Auch für Aushänge in der eigenen Geschäftsstelle bzw. im Vereinshaus gilt, dass personenbezogene Daten grundsätzlich nur nach vorheriger Zustimmung veröffentlicht werden dürfen. Die Tatsache, dass diese Informationen in erster Linie nur von den eigenen Mitgliedern des Vereins gelesen werden und deshalb der potentielle Adressatenkreis kleiner ist als bei einer Veröffentlichung in der verbandseigenen Zeitung, ändert nichts daran, dass auch hier die Kenntnisnahme durch Dritte (also Nichtmitglieder) nicht auszuschließen ist.

Veröffentlichung in der Presse

Die Veröffentlichung von personenbezogenen Informationen in der Presse setzt zunächst voraus, dass diese Informationen von öffentlichem Interesse sind und dass die schutzwürdigen Belange des oder der Betroffenen gewahrt werden. Wird beispielsweise über eine Veranstaltung berichtet, ist von Bedeutung, ob diese öffentlich war, ob der Betroffene selbst Erklärungen gegenüber der Presse abgegeben hat und was die Presse von sich aus in Erfahrung bringen konnte. Insoweit ist bei Mitgliederversammlungen und Vorstandssitzungen zu berücksichtigen, dass diese grundsätzlich nicht öffentlich sind. Ein Bericht über dort geführte verbandspolitische Debatten und ergangene Beschlüsse verbietet sich also in der Regel. Ungeachtet dieser Aspekte darf der Verein ohnehin nur die unbedingt notwendigen persönlichen Angaben machen; Informationen zu privaten Angelegenheiten, die keinen Bezug zum Verein haben, kommen hingegen von vornherein nicht in Betracht.

Veröffentlichung im Internet

Das Internet gewinnt auch für Selbsthilfeorganisationen immer mehr an Bedeutung. Es gibt kaum einen Verein, der sich nicht auf einer eigenen Homepage im Internet präsentiert und Informationen über sich und seine Arbeit veröffentlicht. Darüber hinaus sind immer mehr Verbände in den sog. Sozialen Medien unterwegs, nicht zuletzt um den Austausch mit anderen Betroffenen zu fördern und vor allem um auf diesem Wege neue Mitglieder zu gewinnen.

Eine Veröffentlichung von personenbezogenen Daten im Internet ist wegen des nahezu unbegrenzten weltweiten Adressatenkreises und den damit verbundenen Gefahren aber grundsätzlich unzulässig, soweit sich der Betroffene nicht ausdrücklich hiermit einverstanden erklärt hat. In viel stärkerem Maße als bei anderen Medien sind Angaben im Internet recherchierbar und über Suchmaschinen abrufbar. Diese können dann wiederum umso leichter verwertet werden – was in der Regel zum Nachteil des Betroffenen geschieht. Zudem können vermeintlich gelöschte Einträge in den meisten Fällen, zumindest von IT-Profis, wiederhergestellt werden. Nach wie vor gilt der Grundsatz: „Das Netz vergisst nichts!“

Nichtsdestrotz können natürlich auch bestimmte „ungefährliche“ Angaben im Internet gemacht werden, ohne dass es einer ausdrücklichen Einwilligung bedarf. So ist auch hier die Veröffentlichung der „dienstlichen“ Kontaktdaten von Funktionsträgern eines Vereins in der Regel problemlos möglich. Das bedeutet allerdings – wie bereits oben betont –, dass zwar die Namen der Vorstandsmitglieder und auch des Geschäftsführers auf der Homepage des Verbandes aufgeführt werden dürfen. Als Kontaktadresse sollte man dabei aber immer nur die Anschrift der – soweit vorhanden – Geschäftsstelle des Vereins angeben. Die Veröffentlichung privater Adressen und sonstiger persönlicher Daten wie das Geburtsdatum setzt dagegen immer das entsprechende ausdrückliche Einverständnis des Betroffenen voraus.

Während bei anderen Vereinsarten ein berechtigtes Interesse in die kurzzeitige Veröffentlichung bestimmter Informationen ihrer Mitglieder im Internet auch ohne deren Einwilligung zu bejahen sein mag (z.B. bei Sportvereinen die Bekanntgabe von Wettkampfergebnissen oder Ranglisten), wird man dies bei Selbsthilfeorganisationen wegen des engen Bezugs zum Gesundheitsbereich wohl regelmäßig verneinen müssen.

Auch wenn eine Person vorab gefragt wird, ob sie mit einer Veröffentlichung einverstanden ist, macht es Sinn, ihr nicht nur die datenschutzrechtlich relevanten Informationen zukommen zu lassen, sondern sie zugleich auf die damit verbundenen Gefahren und Unsicherheiten hinzuweisen und sie entsprechend zu sensibilisieren. Das gilt erst recht, wenn jemand seine vollständige Privatadresse und ggf. weitere persönliche Details – etwa das Vorliegen einer Behinderung oder einer Erkrankung - preis gibt und darüber hinaus auch noch der Veröffentlichung eines oder mehrerer Fotos zustimmt.

Im Umgang mit sensiblen Daten – also etwa Gesundheitsdaten - besteht eine Pflicht zur besonderen Sorgsamkeit, erst recht wenn es um eine Veröffentlichung im Internet geht. Daher ist gerade bei Selbsthilfe-organisationen in diesem Zusammenhang zu beachten, dass die Vereins-zugehörigkeit in der Regel vermuten lässt, dass das betreffende Mitglied gleichfalls von der jeweiligen Behinderung oder Erkrankung betroffen ist. Deshalb sollte gerade auch in dieser Hinsicht immer überlegt werden, ob eine namentliche Erwähnung oder eine Bildveröffentlichung in der Presse oder gar im Internet Nachteile mit sich bringen kann. Denkbar ist dies etwa im Zusammenhang mit einem laufenden Bewerbungsverfahren, wenn der entsprechende Arbeitgeber durch eine Internetrecherche über den Bewerber von dessen Behinderung oder Erkrankung erfährt und er ihn deshalb nicht weiter berücksichtigt. Gleiches gilt für eventuelle Risikoeinstufungen bei Versicherungen. Dessen ungeachtet ist zu bedenken, dass es stets die freie und alleinige Entscheidung des Betroffenen ist, ob und inwieweit er seine Behinderung oder Erkrankung bekannt machen möchte. Es sollte daher niemand hierzu gedrängt werden, vor allem dann nicht, wenn sich die Information über das Internet an einen weltweiten Adressatenkreis richtet.

Die Bekanntgabe von Veranstaltungen oder sonstigen Ereignissen im Internet ist selbstverständlich problemlos, wenn sie nicht mit einer Weitergabe personenbezogener Daten verbunden ist. Werden in diesem Zusammenhang hingegen Personen genannt, kommt es darauf an, welche konkreten Angaben zu ihnen gemacht werden. Die namentliche Erwähnung eines eingeladenen

Referenten im Programm ist sicherlich auch ohne dessen vorherige ausdrückliche Einwilligung zulässig, denn die Bekanntmachung bzw. Werbung für die Veranstaltung ist üblich, und hierzu gehört auch die Angabe, wer an der Veranstaltung als Redner teilnimmt. Nichtsdestotrotz sollte in Zweifelsfällen immer vorab eine Einwilligung eingeholt werden. Das gilt etwa für den Fall, dass Vereinsmitglieder genannt werden, die in der Veranstaltung öffentlich über ihre Behinderung oder chronische Erkrankung sprechen werden. Wie immer gilt auch hier: Es sind so wenig Angaben wie möglich zu machen; Veröffentlichungen von Daten, die nicht im Zusammenhang mit der Veranstaltung stehen und daher nicht erforderlich sind oder auch besondere Kategorien von personenbezogenen Daten im Sinne von Art. 9 DSGVO sowie die Veröffentlichung von Fotos haben zu unterbleiben, wenn der Betreffende in eine Veröffentlichung nicht ausdrücklich eingewilligt hat.

Soziale Medien

Facebook, Google+, LinkedIn, Twitter oder auch Instagram und YouTube werden auch von Vereinen in zunehmendem Maße genutzt. Auch hier gilt selbstredend eine besondere Vorsicht im Umgang mit personenbezogenen Daten. Denn anders als bei einer eigenen Homepage, deren Inhalt und Zweck der Betreiber der Seite selbst festlegt, um sich bekannt zu machen und für sich zu werben, geht es bei sozialen Medien in erster Linie um das Sammeln und Auswerten von Nutzerdaten durch Dritte. Selbstverständlich ist es auch hier möglich, seine Angaben oder den zugriffsberechtigten Nutzerkreis zu beschränken. Sind aber einmal Inhalte bekannt geworden, ist es grundsätzlich nicht mehr möglich, diese einer Verwertung zu entziehen, auch wenn sie nachträglich gelöscht werden. Das liegt unter anderem an den oft bedenklichen und zudem schwer nachvollziehbaren Nutzerbedingungen, denen ein neues Mitglied erst einmal zustimmen muss.

Soziale Netzwerke sind zwar in der Regel kostenlos, der Nutzer zahlt aber dennoch einen Preis, nämlich indem seine eingegebenen Daten von Dritten, insbesondere von Werbeunternehmen, genutzt werden. Und je mehr diese Werbetreibenden über eine einzelne Person, aber auch über eine Organisation wie einen Selbsthilfeverband, in Erfahrung bringen, desto leichter ist es, diese gezielt zu beeinflussen und zu bewerben. Überdies sind

soziale Medien meist so aufgebaut, dass sie den Nutzer dazu verführen, immer mehr über sich preiszugeben.

Es ist daher umso wichtiger, bei der Nutzung von sozialen Medien genau hinzusehen, wie es um die Geschäftsbedingungen, um Einstellungen zum Datenschutz, Möglichkeiten zur Blockierung oder auch um die Sichtbarkeit der Einträge bestellt ist. Diese Prüfungen sind umso wichtiger, je mehr personenbezogene Daten einschließlich Fotos eingestellt werden. Es soll keineswegs der Vorteil von Sozialen Medien, etwa die damit verbundene Verbreitungsmöglichkeit von Informationen über den Verband und seine Selbsthilfetätigkeit, in Frage gestellt werden. Allerdings kommen auch hier die zuvor beschriebenen Datenschutzregelungen zur Anwendung. Das bedeutet, dass ein Verein – und hier insbesondere der Vorstand – auch bei der Nutzung sozialer Medien darauf achten muss, dass etwa die erforderliche Einwilligung in eine Veröffentlichung der Daten vorliegt. Auch sollte ein Betroffener darüber informiert werden, wenn die Angaben nicht auf der eigenen Homepage sondern auf einer Seite von Facebook oder LinkedIn veröffentlicht werden sollen. Der Vorstand sollte zudem von seinem Weisungsrecht hinreichend Gebrauch machen, um zu verhindern dass andere Vereinsmitglieder unzulässige oder zumindest datenschutzrechtlich bedenkliche Beiträge oder Bilder auf der vom Verein betriebenen Seite posten.

Pflichten beim Betreiben einer Homepage

Seit Februar 2016 sind Betreiber von Webseiten dazu verpflichtet, auf ihrer Homepage eine Datenschutzerklärung einzustellen. In dieser ist darzulegen, welche Daten beim Besuch der Webseite erfasst werden; das sind insbesondere die jeweilige IP-Adresse des Besuchers sowie die Angabe über Zeitpunkt und Dauer seines Besuches. Auch die Verwendung von sog. Cookies ist darzustellen, ferner muss angegeben werden, wenn Daten an einen Dritten weitergegeben werden. Bei dieser Datenschutzerklärung handelt es sich letztlich um nichts anderes als die nunmehr nach Art. 13 DSGVO anzugebenden Informationen. Danach hat der Verantwortliche (d.h. der Betreiber der Internetseite) der betroffenen Person (dem Nutzer) zum

Zeitpunkt der Erhebung der personenbezogenen Daten also insbesondere Folgendes mitzuteilen:

- Name und Kontaktdaten des Verantwortlichen, soweit vorhanden auch die Kontaktdaten des Datenschutzbeauftragten
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen und die Rechtsgrundlage für die Verarbeitung
- ggf. die berechtigten Interessen, die vom Verantwortlichen oder einem Dritten mit der Datenverarbeitung verfolgt werden (Fall des Art. 6 Abs. 1 f) DSGVO)
- im Falle einer Weitergabe der Daten die Empfänger oder die Kategorien von Empfängern
- ggf. die Absicht, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln
- die Dauer der Datenspeicherung bzw. die Kriterien für die Festlegung der Dauer
- das Bestehen des Rechts auf Auskunft, auf Berichtigung, auf Löschung oder auf Einschränkung der Verarbeitung
- das Bestehen eines Widerspruchsrechts
- das Bestehen eines Widerrufsrechts im Falle der vorausgegangenen Einholung einer ausdrücklichen Einwilligung (Fälle des Art. 6 Abs. 1 a) und des Art. 9 Abs. 2 a) DSGVO)
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- ob die Bereitstellung der Daten vorgeschrieben ist bzw. für einen Vertragsabschluss erforderlich ist und welche Folgen die Nicht-bereitstellung hätte

Die Datenschutzerklärung muss auf der Website gut sichtbar eingestellt werden, außerdem ist sie leicht verständlich Weise zu formulieren (also nicht bloß den Gesetzestext wiedergeben), welche Daten im Rahmen der Nutzung der Internetseite erfasst werden, was mit diesen geschieht und welche entsprechenden Rechte die Nutzer der Seite haben. Eine solche Verpflichtung bestand grundsätzlich auch schon in der Vergangenheit, weshalb die meisten Betreiber bereits eine Datenschutzerklärung auf ihrer Homepage verankert haben. Angesichts der neuen Vorgaben nach der DSGVO

sollten aber auch diese nochmals auf ihren Inhalt hin überprüft werden, da nunmehr zusätzliche Angaben in der Erklärung enthalten sein müssen.

Eine ausführliche Erläuterung zum Thema einschließlich einer Muster-Datenschutzerklärung findet sich in der Schrift „Datenschutz bei Betreiben einer Vereins-Webseite“ der BAG SELBSTHILFE.

Ein Hinweis für die Betreiber einer sog. Fanpage bei Facebook: Nach einem Urteil des Europäischen Gerichtshofs vom 05.06.2018 (Az.: C-210/16) sind sowohl Facebook als auch der Betreiber einer entsprechenden Fanpage für die Nutzerdaten verantwortlich, es besteht also eine geteilte Verantwortung. Die Entscheidung geht auf eine Vorlage durch das Bundesverwaltungsgericht zurück, das jetzt in der Sache abschließend entscheiden muss.

Eine Fanpage oder auch Fanseite bezeichnet eine Website, auf der gezielt Informationen über eine Person des öffentlichen Lebens oder etwa auch ein Unternehmen bereitgestellt werden. Ziel solcher Fanpages ist es häufig, für eigene bereitgestellte Angebote zu werben, also Kunden oder Mitarbeiter zu gewinnen. Problematisch an der Sache ist, dass der Betreiber einer Fanpage in seiner Datenschutzerklärung über Datenverarbeitungsvorgänge bei Facebook informieren soll, hierfür aber gar nicht die erforderliche Kenntnis hat, was mit den Daten bei Facebook tatsächlich passiert. Es ist daher zum jetzigen Zeitpunkt zu empfehlen, in der eigenen Datenschutzerklärung so genaue Angaben wie möglich zu machen – einschließlich des Hinweises, dass eine Facebook-Fanpage unterhalten wird – und dann von der Facebook-Fanpage aus einen Link zu der Datenschutzerklärung auf der eigenen Internetseite zu setzen. Auch wenn die Aufsichtsbehörden die derzeitige Praxis, insbesondere die fehlende Einwilligung der Nutzer, sehr kritisch sehen, wird empfohlen nicht in Panik zu verfallen, sondern die abschließende Entscheidung des Bundesverwaltungsgerichts abzuwarten, um dann ggf. entsprechende Anpassungen vorzunehmen.

Sperren und Löschen von Daten

Personenbezogene Daten dürfen grundsätzlich nur solange gespeichert werden, wie dies der Zweck der Speicherung erfordert. Ist dieser Zeitpunkt erreicht, wurde die entsprechende Einwilligung widerrufen oder bestand ohnehin kein Recht auf Verarbeitung, sind die personenbezogenen Daten gem. Art. 17 DSGVO grundsätzlich unverzüglich zu löschen.

Es ist daher möglichst genau festzulegen, welche Daten bis zu welchem Ereignis bzw. für welche Dauer zu speichern sind. Ist dieser Endzeitpunkt erreicht (etwa die Beendigung einer Mitgliedschaft durch Austritt, Ausschluss oder Tod), kann es jedoch sein, dass die Daten noch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden. In diesem Fall ist die Verarbeitung zunächst nur einzuschränken, Art. 18 Abs. 1 c) DSGVO. Die Dauer der Einschränkung hängt von der Erforderlichkeit der weiteren eingeschränkten Nutzung ab (z.B. für die Dauer eines Rechtsstreits). Eine Verwendung der Daten zu anderen Zwecken (etwa zum Zusenden von Werbeschreiben oder Spendenaufrufen) ist dann ohne vorherige Einwilligung grundsätzlich nicht mehr gestattet. Ist ein Zugriff auf die Daten nicht mehr erforderlich, sind die Daten endgültig zu löschen.

Löschen bedeutet, dass die Daten endgültig unlesbar gemacht werden, also nicht mehr abrufbar sind. Demzufolge stellt das Verschieben von Daten in den „Papierkorb“ eines PCs noch kein Löschen dar. Ähnliches gilt, wenn sich die Daten auf Papier befinden: ein einfaches Entsorgen als Altpapier genügt nicht, vielmehr sollten die Unterlagen so zerkleinert werden – etwa mit einem Aktenvernichter –, dass sie nicht mehr ohne Weiteres zusammengefügt werden können und damit wieder lesbar werden.

Beim Wechsel von Vorstandsmitgliedern oder hauptamtlichen Mitarbeitern des Vereins ist sicherzustellen, dass die im Besitz befindlichen Mitglieder- und sonstigen personenbezogenen Daten ordnungsgemäß und vollständig übergeben werden und keine Dateien oder (Sicherheits-)Kopien mehr beim bisherigen Inhaber verbleiben. Das sollte möglichst in den verbandseigenen Datenschutzrichtlinien (*s.u.*) geregelt werden.

Bestellung eines Datenschutzbeauftragten

Sinn und Zweck der Bestellung eines Datenschutzbeauftragten ist es, den Datenschutz innerhalb der betreffenden Stelle (Unternehmen, Behörde, Verein o.a.) dadurch zu stärken und effektiver zu gestalten, dass sich eine „unabhängige“ Person speziell mit der Frage befasst, ob und inwieweit die datenschutzrechtlichen Bestimmungen innerhalb der Organisation tatsächlich beachtet und umgesetzt werden. Das entbindet zwar nicht die Verantwortlichen – im Verein insbesondere den Vorstand und die Geschäftsführung – von ihren entsprechenden Pflichten und ihrer diesbezüglichen Haftung, hilft aber dabei, dass mittels eines neutralen Blicks möglichst alle Aspekte des Datenschutzes berücksichtigt werden. Personen, die einem bestimmten Aufgabenbereich zugeordnet sind, verlieren leicht den Überblick auf Aspekte außerhalb ihres Bereichs und übersehen mitunter aus „Betriebsblindheit“ wichtige datenschutzrelevante Begebenheiten. Außerdem neigt man oft dazu, Pflichten, die mit Zusatzarbeit verbunden sind, sowie immer wieder durchzuführende Kontrollen irgendwann zu vernachlässigen. Aus diesem Grunde ist es hilfreich, wenn innerhalb der Organisation eine qualifizierte Person einen Überblick über alle Aufgaben und Organisationseinheiten hat und die Verantwortlichen auf Handlungserfordernisse bzw. Versäumnisse beim Datenschutz hinweist.

Jeder Verein sollte sich deshalb überlegen, ob es für ihn Sinn macht, einen Datenschutzbeauftragten zu bestellen. In bestimmten Fällen ist eine Organisation ohnehin gesetzlich dazu verpflichtet, einen Datenschutzbeauftragten zu benennen (*s.u.*). Er kann aber auch auf freiwilliger Basis bestellt werden. Und das macht nicht zuletzt deshalb Sinn, weil dadurch der Vorstand und die Geschäftsführung, aber auch die Mitarbeiter, die im Verein mit der Datenverarbeitung befasst sind, entlastet und unterstützt werden.

Nach Art. 37 Abs. 1 DSGVO ist der Verein u.a. dann dazu verpflichtet, einen Datenschutzbeauftragten zu benennen, wenn dessen Kerntätigkeit die systematischen Überwachung von Betroffenen beinhaltet, wenn eine umfangreiche Verarbeitung besonderer Daten im Sinne von Art. 9 DSGVO stattfindet oder wenn die Kerntätigkeit in der Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten besteht.

Da unter Art. 9 DSGVO – wie gesehen – auch die von Selbsthilfeorganisationen häufig erfassten Gesundheitsdaten fallen, stellt sich die Frage, ob insoweit Vereine der Selbsthilfe grundsätzlich zu Bestellung eines Datenschutzbeauftragten verpflichtet sind. Art. 37 DSGVO verlangt allerdings, dass die Verarbeitung besonderer Daten (also etwa von Gesundheitsdaten) die „Kerntätigkeit“, also die Haupttätigkeit der Organisation darstellen muss. Soweit sie lediglich als Nebentätigkeit anzusehen ist, die die eigentliche Haupttätigkeit nur unterstützt, besteht noch keine Pflicht zur Bestellung eines Datenschutzbeauftragten. Anders als in Arztpraxen oder anderen medizinischen Einrichtungen, wo die Verarbeitung von Gesundheitsdaten in einem viel engerem Zusammenhang mit der Kerntätigkeit, der medizinischen Behandlung, steht, stellt die Verarbeitung von Gesundheitsdaten in Selbsthilfeorganisationen häufig nur eine unterstützende Tätigkeit dar, etwa zur statistischen Feststellung, in welchem Umfang Betroffene Mitglied im Verein sind.

Eine klare Abgrenzung bzw. Feststellung, ob ein Datenschutzbeauftragter gem. Art. 37 Abs. 1 DSGVO zu bestellen ist, lässt sich zumindest nicht allgemein treffen, zumal die Selbsthilfeorganisationen unterschiedlich ausgeprägt sind und auch unterschiedliche Leistungen anbieten. Das bedeutet: je größer die Zahl der erfassten Gesundheitsdaten ist – Art. 37 DSGVO verlangt zusätzlich, dass eine „umfangreiche“ Verarbeitung stattfindet – und neben der Abfrage beim Mitglied, ob er von der jeweiligen Erkrankung oder Behinderung betroffen ist, auch an anderer Stelle Gesundheitsdaten abfragt (z.B. im Rahmen eines Beratungsangebots oder in Form einer Datenerhebung bei den Treffen von Selbsthilfegruppen), desto eher wird man begründen können, dass die Verarbeitung von Gesundheitsdaten Teil der „Kerntätigkeit“ des Vereins ist. In diesem Fall ist also ein Datenschutzbeauftragter zu bestellen. Fragt ein Verein hingegen nicht ab, ob das Mitglied von der Erkrankung/Behinderung betroffen ist und werden auch im Rahmen anderer Vereinsaktivitäten keine Gesundheitsdaten erfasst, wird man von einem Erfordernis der Bestellung eines Datenschutzbeauftragten wohl absehen können.

Es wird empfohlen, im Zweifel Rücksprache mit dem zuständigen Landesdatenschutzbeauftragten zu halten und dessen Einschätzung zu der Frage, ob eine Bestellung erforderlich ist, einzuholen. Im Übrigen wird an dieser Stelle

nochmals darauf hingewiesen, dass auch die freiwillige Benennung eines Datenschutzbeauftragten möglich ist, die im Regelfall durchaus zu empfehlen ist (so dass sich dann auch nicht die leidige Frage stellt, ob eine gesetzliche Verpflichtung zur Bestellung besteht).

Eine andere gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten ergibt sich aus § 38 Abs.1 BDSG: Hiernach ist eine Bestellung erforderlich, wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Nimmt der Verein Verarbeitungen vor, die einer Datenschutzfolgeabschätzung gem. Art. 35 DSGVO unterliegen (*vgl. hierzu Näheres unten*), ist ebenfalls ein Datenschutzbeauftragter zu benennen.

Wie zuvor erwähnt, hat der Datenschutzbeauftragte auf die Einhaltung der datenschutzrechtlichen Vorschriften innerhalb der Organisation hinzuwirken. Diese Aufgabe umfasst Beratungs- und Kontrollfunktionen. Hierzu gehört vor allem, die mit der Datenverarbeitung befassten Personen (insbesondere die Mitgliederverwaltung) mit dem Datenschutzrecht und den diesbezüglichen Erfordernissen vertraut zu machen und zu beraten, aber auch die Geschäftsleitung und den Vorstand auf mögliche oder tatsächliche Verstöße hinzuweisen, da diese letztlich in der Verantwortung bleiben. Zum Kontrollbereich gehört vor allem die Überwachung der ordnungsgemäßen Anwendung der betreffenden EDV-Anlagen und Datenverarbeitungsprogramme. Er hat deshalb ein Anrecht auf vorhergehende Information, wenn ein bestimmtes Vorhaben oder technische Änderungen geplant sind. Die Aufgaben des Datenschutzbeauftragten sind in Art. 39 DSGVO näher geregelt. Ein Eingriffsrecht in die organisatorischen Abläufe und in die Unternehmensführung steht dem Datenschutzbeauftragten aus der DSGVO oder dem BDSG hingegen nicht zu. Er kann also nicht anordnen, dass eine bestimmte datenschutzrechtlich relevante Maßnahme auch tatsächlich ergriffen wird; dies ist dann Sache der für die Vereinsführung verantwortlichen Personen.

Um eine Interessenkollision zu vermeiden, ist der Datenschutzbeauftragte nicht aus der Reihe der Vorstandsmitglieder oder aus dem Kreis der für die

Datenverarbeitung des Vereins Verantwortlichen zu bestellen. Im Übrigen muss der Betreffende die zur Erfüllung der Aufgaben erforderliche Zuverlässigkeit und vor allem Fachkunde mitbringen, die etwa durch entsprechende Schulungen erlangt werden kann. Er muss nicht Mitglied des Vereins sein; die Aufgabe kann auch an ein externes Unternehmen übertragen werden, das entsprechende Dienstleistungen anbietet.

Die Voraussetzungen, die ein Datenschutzbeauftragter erfüllen muss, sowie seine Aufgaben mögen auf den ersten Blick umfangreich und kompliziert erscheinen. Wenn man aber bedenkt, dass gerade in kleineren Verbänden der Umfang an Datenverarbeitungsvorgängen durchaus begrenzt ist und vor allem viele Routinearbeiten verrichtet werden, die nur selten eine permanente neue Einarbeitung in ein datenschutzrelevantes Themengebiet erfordern, ist die Tätigkeit eines Datenschutzbeauftragten durchaus zu bewerkstelligen, auch in ehrenamtlicher Funktion.

Ist ein Datenschutzbeauftragter bestellt, sind seine Kontaktdaten übrigens zu veröffentlichen und insbesondere auch in den Informationen nach Art. 13 DSGVO an den Betroffenen, dessen Daten verarbeitet werden, aufzunehmen. Ferner sind die Daten der zuständigen Aufsichtsbehörde mitzuteilen.

Datenschutzordnung – Datenschutzrichtlinien

Schon in der Vergangenheit war Selbsthilfeverbänden empfohlen worden, sich einen Überblick darüber zu verschaffen, welche personenbezogenen Daten bei ihnen anfallen und in welcher Weise sie genutzt werden, um dann in einem zweiten Schritt interne Vorgaben zum Umgang und Schutz dieser Daten zu erstellen.

Die DSGVO verlangt nunmehr ausdrücklich, dass die Grundzüge der Datenerhebung, -verarbeitung und –nutzung schriftlich festgelegt werden. Das kann, muss aber nicht zwingend in der Satzung geschehen. Bei Detailregelungen macht es eigentlich mehr Sinn, diese in einer Vereins-ordnung (häufig unter dem Namen „Datenschutzrichtlinien“) zu verankern, weil diese schneller wieder geändert werden können als Satzungsregelungen, die grundsätzlich in einer Mitgliederversammlung beschlossen und überdies im Vereinsregister eingetragen werden müssen. Viele Verbände nehmen in ihrer Satzung daher auch nur einige datenschutzrechtliche Prinzipien auf, um

nach außen deutlich zu machen, dass der Verein den Datenschutz ernst nimmt. Nähere Einzelheiten und konkrete Anweisungen für den alltäglichen Umgang mit anfallenden Daten werden hingegen in einer eigenen Vereinsordnung geregelt.

Wichtig ist, dass diese Datenschutzordnung auch verständlich ist und sowohl der Betroffene als auch die Anwender im Verein (Vorstand, Mitarbeiter in der Geschäftsstelle etc.) ablesen können, was sie konkret zu beachten und zu tun haben beim Umgang mit personenbezogenen Daten. Es sollte daher auch nicht nur der Wortlaut einzelner Gesetzesregelungen wiedergegeben werden.

Für die Erstellung einer Datenschutzordnung bzw. von Datenschutzrichtlinien empfiehlt sich folgende Herangehensweise: Es macht Sinn, zunächst die Bereiche abzustecken, in denen eine Datenverarbeitung durch den Verein regelmäßig stattfindet, etwa bei der Mitgliederverwaltung, im Personalbereich, bei Veranstaltungen (an denen ggf. auch Nichtmitglieder teilnehmen), Beratung von Betroffenen, bei den Aktivitäten von Selbsthilfegruppen etc. Dies ist zweckmäßig, um sich von vornherein darüber im Klaren zu sein, wo sich eine Datenschutzrelevanz ergibt und dass sich Datenschutz im Verein nicht nur auf die reine Mitgliederverwaltung beschränkt.

Es bietet sich an, die einzelnen Datenverarbeitungsschritte nacheinander darzustellen. Dabei können etwa folgende Fragestellungen im Hinblick auf die Mitgliederdaten hilfreich sein (*Achtung – es handelt sich hierbei nicht um eine abschließende Auflistung*!):

1. *Datenerfassung:*

- Welche Daten werden von einem Neumitglied abgefragt?
- Wie werden bei einem Neumitglied dessen Daten erfasst (Entgegennahme eines Beitrittsformulars in Papierform, auch Angaben auf Online-Formular möglich)?
- Wer im Verein nimmt Daten entgegen, wer gibt sie in Computer ein (Mitgliederverwaltung, Vorstand)?

- Zu welchem Zeitpunkt und auf welche Weise wird das Neumitglied datenschutzrechtlich informiert?
- Werden auch Daten von Nichtmitgliedern erfasst, z.B. bei Treffen von Selbsthilfegruppen oder auf Vereinsveranstaltungen?
- Werden erforderliche Einwilligungen eingeholt und liegen entsprechende Nachweise vor? Wird auf Widerspruchsmöglichkeit hingewiesen?

2. *Speicherung und Nutzung:*

- Welche Daten werden gespeichert?
- In welcher Weise werden Sie gespeichert (Datei, Akten/Karteikarten, lokaler Rechner, gemeinsamer Server, externe Cloud)?
- Welche Sicherungsvorkehrungen bestehen (Software; Passwort-Schutz; Einsatz von Virenprüfer/Firewall etc.; Akten/Rechner unter Verschluss)?
- Wer hat Zugriff auf die Daten (Mitgliederverwaltung, Vorstand, andere Mitarbeiter)?
- An wen werden sie intern weitergeleitet (von unselbständiger Untergliederung an Landes- oder Bundesverband, von Bundesverband an Regionalgruppe)?
- Wofür werden Daten intern verwendet (z.B. um Mitglied anzuschreiben, um Mitgliedsbeitrag abzubuchen, um Statistiken zu erstellen)?

3. *Weitergabe von Daten:*

- Werden personenbezogene Daten an Dritte weitergegeben (z.B. an Dachverband oder an Verlagshaus, das Verbandszeitung an Mitglieder versendet)?
- Wird ggf. erforderliches Einverständnis eingeholt, wobei über Widerrufsmöglichkeit informiert wird?
- Bestehen vertragliche Regelungen / Anweisungen gegenüber dem Dritten hinsichtlich des Umgangs mit den weitergeleiteten Daten?

4. Löschen von Daten:

- Werden Daten unverzüglich gelöscht, wenn Zweck der Verarbeitung endet oder Einwilligung widerrufen wurde?

- Werden Daten zunächst mit Sperrvermerk weiterhin gespeichert (Einschränkung der Datenverarbeitung etwa zwecks Durchführung eines Rechtsstreits)?
- Werden Daten auf mobilen Speichern sowie Akten / Karteikarten durch ordnungsgemäße Vernichtung der Datenträger gelöscht?
- Ist dafür Sorge getragen, dass im Falle eines Wechsels der Funktionsträger oder eines Mitarbeiters die beim bisherigen Inhaber befindlichen Daten vollständig herausgegeben oder gelöscht werden?

Wie gesagt, es handelt sich hierbei nur um einige beispielhafte Fragestellungen, die je nach Verbandsart und –größe unterschiedlich ausfallen können. Die Datenschutzordnung sollte übrigens auch möglichst eine regelmäßige Schulung und generelle Sensibilisierung der mit der Datenverarbeitung befassten Funktionsträger vorsehen, nicht zuletzt, um eine notwendige Datenschutzkultur innerhalb des Vereins zu entwickeln.

Die Erstellung beinhaltet in der Tat am Anfang eine gewisse Fleißarbeit; ist sie aber einmal getan, ist das Ergebnis für die weiteren Datenschutz-Aktivitäten im Verein überaus hilfreich, weil dann umso leichter eine Regelung an neue Tatbestände und vielleicht auch an neue gesetzliche Vorgaben in der Zukunft angepasst werden kann.

Verpflichtung auf das Datengeheimnis

Während die DSGVO keine ausdrückliche Vorgabe enthält, wonach Personen, die für einen Verantwortlichen im Bereich der Datenverarbeitung tätig sind, auf das Datengeheimnis zu verpflichten sind, sieht § 53 BDSG eine entsprechende Verpflichtung vor. Danach dürfen mit Datenverarbeitung befasste Personen – im Verein also haupt- wie ehrenamtlich Tätige – personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). Sie sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort.

Denkbar ist folgende Erklärung (*Muster*):

Verpflichtung gem. § 53 BDSG zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG)

……

Name der verantwortlichen Stelle

Sehr geehrte(r) Frau / Herr …….

aufgrund Ihrer Aufgabenstellung verpflichten wir Sie auf die Wahrung des Datengeheimnisses. Es ist Ihnen untersagt, unbefugt personenbezogene Daten zu verarbeiten. Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Einwilligung oder eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze für die Verarbeitung personenbezogener Daten sind insbesondere in Art. 5 Abs. 1 DSGVO festgelegt. Danach müssen personenbezogene Daten

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 Durch-führung 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")

Wir weisen darauf hin, dass Verstöße gegen das Datengeheimnis mit Freiheits- oder Geldstrafe geahndet werden können. In der Verletzung des Datengeheimnisses kann zugleich eine Verletzung arbeitsrechtlicher Schweigepflichten bzw. entsprechender vereinsrechtlicher Obliegenheitspflichten liegen. Ferner können sich zivilrechtliche Schadensersatzansprüche ergeben.

Diese Verpflichtung besteht auch nach Beendigung Ihrer Tätigkeit fort.

Eine unterschriebene Zweitschrift dieses Schreibens reichen Sie bitte an …… zurück.

…….. ……..

Ort, Datum Unterschrift der verantwortlichen Stelle

Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung habe ich erhalten.

……. ……

Ort, Datum Unterschrift des Verpflichteten

Verzeichnis von Verarbeitungstätigkeiten

Nach Art. 30 DSGVO hat jeder Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten zu führen. Zwar besteht für Verantwortliche mit weniger als 250 Beschäftigten eine Ausnahme von dieser Pflicht; allerdings gilt diese Ausnahme u.a. wiederum dann nicht, wenn die Verarbeitung nicht nur gelegentlich oder eine Verarbeitung sensibler Daten im Sinne von Art. 9 oder Art. 10 DSGVO erfolgt. Das bedeutet für Vereine, insbesondere solche der Gesundheitsselbsthilfe, dass auch sie regelmäßig ein Verzeichnis führen müssen. Darin muss enthalten sein:

- Name und Kontaktdaten des Verantwortlichen (einschließlich seines Vertreters, *bei Vereinen also des Vorstandes i.S. des § 26 BGB*)
- Zwecke der Verarbeitung (*insbesondere Satzungszwecke und -aufgaben neben der Mitgliederverwaltung*)
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (*Mitglieder, hauptamtliche Mitarbeiter, Lieferanten etc. - Mitgliedsdaten (Kontaktdaten, ggf. Gesundheits- und weitere Daten), Personaldaten, Geschäftskundendaten etc.*)
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind bzw. noch offengelegt werden (*z.B. Dachverbände, Dienstleister)*
- Angaben über Drittlandtransfer einschließlich Angaben des Drittlandes sowie Dokumentierung geeigneter Garantieren (*bei den meisten Selbsthilfeorganisationen wohl nur Angabe erforderlich, dass keine Transfers erfolgen; ggf. Angaben bei Nutzung einer Cloud o.a. außerhalb der EU*)
- Wenn möglich, Fristen für die Löschung der verschiedenen Datenkategorien (*bei Mitgliederdaten in der Regel nur Ereignisse für Löschung maßgeblich: Kündigung der Mitgliedschaft, Ausschluss oder Tod*)
- Wenn möglich Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DSGVO (Sicherheit der Verarbeitung, *also z.B. Angaben zu Software, Passwortschutz, Verschlüsselung etc.)*

Das Verarbeitungsverzeichnis muss schriftlich oder in einem elektronischen Format geführt werden. Das Verzeichnis ist der Aufsichtsbehörde auf deren Anfrage zur Verfügung zu stellen.

Da sich der Inhalt des Verarbeitungsverzeichnisses in weiten Teilen mit dem Inhalt der Datenschutzordnung und den Informationen nach Art. 13 DSGVO deckt, dürfte sich der mit der Erstellung des Verzeichnisses verbundene Aufwand in Grenzen halten.

Datenschutz-Folgeabschätzung

Ein Verein hat nach Art. 35 DSGVO eine sog. Datenschutz-Folgeabschätzung vorzunehmen, wenn die Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke ein hohes Risiko für die Rechte und Freiheiten für die betroffene Person zur Folge hat. Dies ist vor allem dann der Fall, wenn eine umfangreiche Verarbeitung besonderer Kategorien von Daten im Sinne von Art. 9 DSGVO erfolgt oder wenn im Wege der Verarbeitung auf Grundlage von personenbezogenen Daten systematische und umfassende Bewertungen persönlicher Aspekte vorgenommen werden, die besondere Rechtswirkungen entfalten.

Ähnlich wie bei der Frage, ob Selbsthilfeorganisationen aufgrund der häufigen Erfassung von Gesundheitsdaten zur Bestellung eines Datenschutzbeauftragten verpflichtet sind, lässt sich auch hier nicht ohne Weiteres beantworten, ob ein Selbsthilfeverband zur Vornahme einer Datenschutz-Folgeabschätzung verpflichtet ist. Im Regelfall wird man dies wohl verneinen können. Je nach Umfang der Erhebung von Gesundheitsdaten kann das aber ausnahmsweise doch der Fall sein, weshalb im Zweifel auch hier eine Rücksprache mit der zuständigen Aufsichtsbehörde ratsam sein kann.

Eine Datenschutz-Folgeabschätzung hat 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 der Maßnahmen zur Risikoreduzierung zu enthalten.

Sanktionen - Meldepflichten

Mit der DSGVO sind die Eingriffs- und Sanktionsmöglichkeiten der Aufsichtsbehörden (das sind insbesondere die Beauftragten für den Datenschutz des Bundes und der Länder) erweitert worden. Sie haben weitreichende Befugnisse, die u.a. auch anlassunabhängige Kontrollen zulassen. Der Verantwortliche ist insoweit zur Mitwirkung verpflichtet, d.h. er muss den Behörden ggf. Zugang zu seinen Geschäftsräumen gewähren oder Unterlagen zur Verfügung stellen.

Es können Anordnungen getroffen werden, die sowohl zu einem bestimmten Handeln/Verhalten verpflichten oder auch zu einem bestimmten Unterlassen. Die wohl schärfste Anordnung ist die Untersagung des weiteren Betriebs des Verantwortlichen. Daneben können Bußgelder verhängt werden, die bis zu 20 Mio. Euro oder 4 % des Jahresumsatzes des Unternehmens betragen können. Diese Größenordnungen wirken auf den ersten Blick abschreckend, sie zielen aber wohl in erster Linie auf große Wirtschafts-unternehmen ab. Das bedeutet nicht, dass nicht auch Selbsthilfe-organisationen mit Sanktionen belegt werden können; in den meisten Fällen wird es aber im Bedarfsfall wohl erst zu einer Aufforderung kommen, ein bestimmtes Verhalten zu ändern, so das erst im Wiederholungsfall ein Bußgeld verhängt wird. Zu bedenken ist, dass im Schadensfall neben Bußgeldern auch Schadensersatz- und Schmerzensgeldzahlungen der Betroffenen auf den Verantwortlichen zukommen können. Schlimmstenfalls zieht eine Datenschutzverletzung sogar eine strafrechtliche Verfolgung nach sich.

Art. 33 DSGVO beinhaltet eine ausdrückliche Meldepflicht im Falle von Pannen oder Verstößen. So sind Datenschutz-Pannen bzw. -Verstöße binnen 72 Stunden nach Kenntnis bei der zuständigen Aufsichtsbehörde zu melden, und auch der Betroffene ist „ohne unangemessene Verzögerung“ zu informieren sind.

Datenschutz als Qualitätsmerkmal

Trotz der Vielzahl an gesetzlichen Vorgaben und Sanktionen sollte Datenschutz nicht als lästige Pflicht oder Übel betrachtet werden, sondern vielmehr – wie eingangs erwähnt - als Qualitätsmerkmal, mit dem die Chance verbunden ist, das Image des eigenen Vereins weiter zu verbessern. Denn je mehr das Mitglied in den sorgsamen Umgang seiner Daten vertrauen kann, desto größer wird auch sein Vertrauen in die Arbeit des Vereins insgesamt sein. Es kann daher – wie bereits ausgeführt – sinnvoll sein, den Datenschutz in der Vereinssatzung zu erwähnen, um zu demonstrieren wie wichtig er für die Organisation ist. Vor allem wird es auch als Qualitätsmerkmal von potentiellen Neumitgliedern wahrgenommen, wenn der Verein nicht nur auf dem Anmeldeformular, sondern ggf. auch auf der eigenen Homepage ungeachtet gesetzlicher Verpflichtungen Hinweise zu den datenschutzrechtlichen Vorkehrungen im Verein gibt.

Auch wenn die DSGVO nunmehr ausdrücklich mehr Transparenz bei der Datenverarbeitung verlangt, sollte der Verein auch ein ureigenes Interesse daran haben, den Mitgliedern alle erforderlichen Informationen in verständlicher Weise und prompt zur Verfügung zu stellen. Gleiches gilt für die verbandseigenen Datenschutzrichtlinien, die nicht nur für Klarheit und Transparenz beim Datenschutz sorgen, sondern auch etwaigen Konflikten im Zusammenhang mit der Einhaltung des Datenschutzes von vornherein wirksam begegnen können.