**EU-Datenschutz-Grundverordnung:**

# Was haben Vereine zu beachten?*

Im Frühjahr 2016 haben der Europäische Rat und das Europäische Parlament die EU-Datenschutz-Grundverordnung (DSGVO) verabschiedet. Ziel war es, die bestehenden Prinzipien des Datenschutzrechts – allem voran das Recht auf informationelle Selbstbestimmung – innerhalb der EU zu vereinheitlichen und zugleich den Datenschutz behutsam zu modernisieren. Künftig gelten in allen EU-Staaten grundsätzlich die gleichen Standards.

Die neue Grundverordnung wird am 25. Mai 2018 Geltung erlangen und die bisherige EU-Datenschutzrichtlinie (95/46/EG) ersetzen. In Deutschland wird am gleichen Tag auch ein neues bzw. überarbeitetes Bundesdatenschutzgesetz (BDSG) ergänzend in Kraft treten, das an den Inhalt der Grundverordnung angepasst worden ist. Dessen ungeachtet gilt die DSGVO unmittelbar in der gesamten Europäischen Union.

Mit der DSGVO soll in erster Linie der Datenschutz im Hinblick auf die Datennutzung und -verwertung durch international tätige Unternehmen und Organisationen, insbesondere auch Online-Dienste, gestärkt werden, und zwar auch dann, wenn diese von Orten außerhalb Europas auf die Daten eines in Europa Ansässigen einwirken. Auch für sie gilt künftig die DSGVO (sog. Marktortprinzip, vgl. Art. 3 DSGVO). Damit einher geht eine Stärkung des Persönlichkeitsrechts des einzelnen Bürgers und den sich daraus ableitenden Rechten im Zusammenhang mit der Erfassung, Verarbeitung und Nutzung seiner personenbezogenen Daten.

*Trotz größter Sorgfalt bei der Erstellung der vorliegenden Übersicht kann keine Gewähr für die inhaltliche Richtigkeit und Vollständigkeit übernommen werden. STAND: Februar 2018

**Grundprinzipien des Datenschutzes bleiben bestehen**

Für die in Deutschland ansässigen und agierenden Vereine und damit auch die Mitgliedsorganisationen der BAG SELBSTHILFE dürften nach jetzigem Stand nur begrenzt Anpassungserfordernisse im Zusammenhang mit dem zu beachtenden Datenschutz bestehen, da die bisherigen datenschutzrechtlichen Grundprinzipien fortgelten, wenn auch in weiterentwickelter Form. Wer die bisherigen Vorgaben zum Datenschutz hinreichend beachtet hat, ist im Grunde genommen bereits weitestgehend „auf der sicheren Seite“ und wird nur einzelne innerverbandliche Regelungen angleichen und Maßnahmen zum Datenschutz ergreifen müssen.

Das bedeutet aber nicht, dass die Neuregelungen ab Ende Mai unberücksichtigt bleiben könnten. Angesichts der künftig stärkeren Kontrollmöglichkeiten der Datenschutzbehörden und vor allem der strengeren Sanktionsmöglichkeiten im Falle eines Verstoßes sollte es im eigenen Interesse jedes Verbandes liegen, sich mit den neuen Vorgaben hinreichend zu befassen und zu prüfen, ob alle datenschutzrechtlichen Vorgaben eingehalten werden. Ein besonderes Augenmerk wird man dabei sicherlich auf die erhöhten Dokumentations-, Informations- und Nachweispflichten legen und prüfen müssen, ob die bisherigen Maßnahmen im Verein insoweit ausreichend sind. Gerade hier wird vermutlich eine gewisse „Fleißarbeit“ erforderlich werden.

In diesem Zusammenhang noch folgender Hinweis vorab: die EU-Datenschutz-Grundverordnung enthält zahlreiche unbestimmte Rechtsbegriffe und offene Formulierungen. Es bleibt abzuwarten, wie einzelne Regelungen künftig durch den Europäischen Datenschutzausschuss ausgelegt werden und welche Maßstäbe die Aufsichtsbehörden (d.h. die Datenschutzbeauftragten des Bundes und der Länder) in der Praxis anlegen. Auch die bislang veröffentlichten und durchaus lesenswerten Orientierungshilfen der Datenschutzkonferenz zu den einzelnen Artikeln der DSGVO (abrufbar u.a. auf der Internetseite der Bundesdatenschutzbeauftragten: www.bfdi.bund.de) stehen noch unter dem Vorbehalt einer zukünftigen Auslegung des genannten Ausschusses.

Deshalb können an dieser Stelle auch noch keine abschließenden und verbindlichen Angaben gemacht werden, welche konkreten Anforderungen im Einzelnen für Selbsthilfeorganisationen künftig bestehen. Wir werden die Entwicklung beobachten und erforderlichenfalls über wichtige Aspekte im Zusammenhang mit der DSGVO ergänzend berichten. Es ist aber sicherlich nicht zu befürchten, dass die Behörden ab Ende Mai schärfste Kontrollen bei allen Unternehmen und Organisationen durchführen und bei den kleinsten Verfehlungen oder Mängeln hohe Bußgelder auferlegen, wie es derzeit vielfach suggeriert wird. Es ist bekannt, dass viele Vorstände und Datenschutzbeauftragte in den Vereinen durch die teils aufgeregte Diskussionen und verwirrende Berichterstattung verunsichert sind. Wer jedoch die erforderliche Sensibilisierung für den Datenschutz aufbringt und die auch jetzt schon geltenden datenschutzrechtlichen Vorgaben beachtet, gleichzeitig in Ruhe prüft, welche der nachstehenden Hinweise Umsetzungen bzw. Maßnahmen im Verein erforderlich machen, dürfte mit der Beachtung des Datenschutzes in seiner Organisation auch nach der neuen Rechtslage ab dem 25. Mai nicht übermäßig Arbeit und Strapaze haben. Im Übrigen stehen Ihnen bei Rückfragen nicht nur die BAG SELBSTHILFE zur Verfügung, sondern auch die erwähnten Datenschutzbehörden, die natürlich auch weiterhin als Informations- und Beratungsstellen fungieren.

**Was ist neu?**

Die Neuregelungen beinhalten zunächst einige formelle Änderungen, etwa bei der Begrifflichkeit. So wird es künftig nur noch den (Ober-)Begriff der *Verarbeitung* geben, und die bisherige *Verantwortliche Stelle* wird künftig nur noch als der *Verantwortliche* bezeichnet. Im Übrigen sind die bisherigen Grundsätze des „Verbots mit Erlaubnisvorbehalts“, der „Datenvermeidung und Datensparsamkeit“, der „Zweckbindung“ und der „Transparenz“ auch nach der Datenschutz-Grundverordnung weiterhin maßgebend. Sie sind in den einzelnen Artikeln der Grundverordnung abgebildet. Dort finden sich aber auch die bereits erwähnten Nachweis- und Rechenschaftspflichten. So muss der Verantwortliche die Regelungen nicht nur *einhalten*, sondern nach Art. 5 Abs. 2 DSGVO die Einhaltung aller Regelungen grundsätzlich auch *nachweisen* können.

Folgenden Regelungen und Grundsätzen sind für Organisationen wie etwa Selbsthilfevereine von besonderer Bedeutung:

**Rechtmäßigkeit der Datenverarbeitung / Verbot mit Erlaubnisvorbehalt**

Nach wie vor ist eine Datenverarbeitung nur zulässig, wenn eine hinreichende Rechtsgrundlage vorliegt, Art. 6 DSGVO. Das kann eine gesetzliche Norm – vor allem der DSGVO oder des (neuen) Bundesdatenschutzgesetzes (BDSG) – sein oder aber auch die entsprechende Einwilligung des Betroffenen. Das Erfordernis bezieht sich dabei wie bisher auf alle Bereiche der Datenverarbeitung, also von der Datenerhebung, über die Speicherung, Nutzung und Weitergabe bis hin zur Löschung.

Eine Datenverarbeitung ist folglich – wie zuvor – auch zulässig, wenn die Verarbeitung für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist (Art. 6 Abs. 1 DSGVO). Deshalb bleibt auch die Erfassung und Verarbeitung der erforderlichen Daten der Mitglieder im Rahmen der Mitgliederverwaltung regelmäßig zulässig.

Ferner ist nach Art. 6 der DSGVO eine Datenverarbeitung unter anderem auch zulässig, wenn sie dem Schutz lebenswichtiger Interessen des Betroffenen oder dem öffentlichen Interesse bzw. der Erfüllung hoheitlicher Aufgaben dient.

**Einwilligung**

Wenn die Zulässigkeit der Datenerhebung und -verarbeitung auf einer Einwilligung beruht, ist darauf achten, dass diese nachweisbar ist (Art. 7 Abs. 1 DSGVO). Eine Schriftlichkeit ist zwar nicht (mehr) erforderlich, aber naturgemäß ist die Nachweisbarkeit im Regelfall am einfachsten, wenn die Einwilligung schriftlich erfolgt ist.

Bei der Einholung der Einwilligung ist darauf zu achten, dass es sich um eine „informierte Einwilligung“ handelt, d.h. dem Betroffenen müssen der Verantwortliche und der Zweck der Datenverarbeitung bekannt sein. Eine Einwilligung kann im Übrigen natürlich jederzeit widerrufen werden, worauf der Betroffene hinzuweisen ist (Näheres hierzu unten unter „Betroffenen-

rechte“). Aus dem Grundsatz der Datensparsamkeit (vgl. unten) folgt im Übrigen, dass keine Einwilligung in eine Erhebung von Daten verlangt werden darf, die für den betreffenden Zweck nicht erforderlich sind.

Wichtig im Zusammenhang mit der Einholung einer Einwilligung ist schließlich noch die klarstellende Regelung des Art. 7 Abs. 2 DSGVO: Wird die Einwilligung mit anderen Sachverhalten verknüpft, muss dies gegenüber dem Einwilligenden klar und leicht verständlich zum Ausdruck kommen. Ist das nicht der Fall, ist die Erklärung unwirksam. Wenn ein Verein also beispielsweise eine Einwilligung zur Veröffentlichung von persönlichen Daten des Mitglieds in der Verbandszeitung einholen will, sollte er diesen Sachverhalt klar trennen von einer etwaigen weiteren Einwilligung zur Weitergabe der Daten an ein Versicherungsunternehmen, mit dem der Verein kooperiert. Insoweit bieten es sich also an, jeweils klar und deutlich darzustellen, worum es jeweils geht und die Einwilligungen dann separat durch eigenständige Unterschriften einholen.

**Verarbeitung besonderer Kategorien personenbezogener Daten**

Die DSGVO beinhaltet in Art. 9 den besonderen Schutz sensibler Daten. Diese Regelung ist für diejenigen Selbsthilfeorganisationen wichtig, die bei Begründung einer neuen Mitgliedschaft abfragen, ob das Mitglied von der jeweiligen Erkrankung oder Behinderung betroffen ist, auf die sich die Selbsthilfe der Organisation bezieht:

Nach Abs. 1 ist die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder sexuellen Orientierung einer natürlichen Person untersagt. Abs. 2 a) lässt eine solche Datenerfassung allerdings zu, wenn die betroffene Person in die Verarbeitung für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt hat.

Selbsthilfeorganisationen, die beim Mitglied abfragen, ob es von der entsprechenden gesundheitlichen Beeinträchtigung betroffen ist, gestalten ihr

Mitgliedsantragsformular häufig in der Weise, dass das Mitglied lediglich anzukreuzen hat, ob die betreffende Erkrankung / Behinderung bei ihm vorliegt oder nicht. Schon nach der bisherigen Rechtslage war zweifelhaft, ob dies ausreichend ist. Es ist aber gerade im Hinblick auf die strengeren Vorgaben nach der DSGVO zu empfehlen, künftig ein ausdrückliches Einverständnis im Wege einer zusätzlichen Unterschrift einzuholen, z.B. unter die vorformulierte Erklärung *„Bei mir liegt die …-Erkrankung vor. Ich bin damit einverstanden, dass diese Angabe im Hinblick und zur Verfolgung der satzungsgemäßen Zwecke der Selbsthilfeaktivitäten des Vereins für die Dauer meiner Mitgliedschaft gespeichert wird*."

**Datensparsamkeit**

Art. 5 DSGVO sieht vor, dass die Verarbeitung personenbezogener Daten dem Zweck angemessen und sachlich relevant sowie auf das für den Zweck der Datenverarbeitung notwendige Maß beschränkt sein muss. Das bedeutet, dass wie bisher nur die wirklich notwendigen Daten abgefragt und gespeichert werden dürfen. Die Abfrage und Speicherung von Daten, die für die Mitgliederverwaltung irrelevant sind, etwa welche Hobbies oder welchen Schulabschluss das Mitglied hat, ist hingegen für Selbsthilfeorganisationen in der Regel nicht erforderlich und daher auch grundsätzlich nicht zulässig. Etwas anderes ist der Fall, wenn laut Satzung bestimmte Voraussetzungen für eine Mitgliedschaft erforderlich sind und deshalb eine Abfrage notwendig ist. Das betrifft bei vielen Selbsthilfeorganisationen die Abfrage, ob beim Mitglied die betreffende Erkrankung oder Behinderungsart vorliegt.

**Datensicherheit**

Angesichts der Tatsache, dass sich der IT-Bereich bekanntermaßen stetig weiterentwickelt, verzichtet die DSGVO auf genaue Vorgaben, welche technischen Sicherheitsmaßnahmen im Einzelnen zu ergreifen sind; das gilt auch für die Organisation. Die DSGVO macht aber deutlich, dass der Verantwortliche insoweit in der Pflicht steht (vgl. Art. 24 ff DSGVO). Es müssen nach wie vor geeignete, technische und organisatorische Maßnahmen getroffen werden, die sich am Stand der Technik orientieren. Dabei macht Art.

25 DSGVO klar, dass sich Datenschutz gerade durch entsprechende Technikgestaltung sowie durch verbraucher- und datenschutzfreundliche Voreinstellungen bei elektronischen Geräten erzielen lässt.

In organisatorischer Hinsicht bleibt zu erwähnen, dass hier wie bisher nur berechtigte Personen auf die personenbezogenen Daten Zugriff haben dürfen. Wie dies vor Ort konkret gehandhabt und geregelt wird (etwa die Darstellung, wie die Passwortvergabe erfolgt), ist zudem zu dokumentieren.

**Informationspflichten und Auskunftsrechte (Betroffenenrechte)**

Besondere Beachtung sollten die bereits erwähnten Betroffenenrechte finden, die durch die DSGVO eine stärkere Ausprägung erfahren als das bisher der Fall war. Sie beinhalten vor allem ein Recht auf umfassende Auskunft hinsichtlich erfolgten Erfassung und Verarbeitung der eigenen Daten. Umgekehrt bestehen für den Verantwortlichen aber auch weitreichende Informationspflichten, unabhängig etwaiger Auskunftsersuchen. So sind die Betroffenen – im Verein also insbesondere die Mitglieder, aber auch Mitarbeiter und Dritte, deren Daten der Verein verarbeitet – gemäß Art. 12 DSGVO umfassend und in leicht verständlicher Weise über alle Aktivitäten im Zusammenhang mit der Datenverarbeitung zu informieren. Art. 13 führt dabei die konkreten Angaben auf, die insoweit im Rahmen der Datenerhebung zu machen sind. Auf den ersten Blick mag die Liste überlang und mit viel Aufwand verbundenen erscheinen. Die Angaben dürften in der Regel aber verhältnismäßig schnell zusammenzutragen sein. Selbsthilfeorganisationen ist daher zu empfehlen, ein entsprechendes Informationsblatt anzufertigen, das dem Betroffenen dann im Zeitpunkt der Erhebung der Daten einfach ausgehändigt werden kann. Dessen Empfang sollte sich der Verein zum Nachweis der erbrachten Informationen und Hinweise möglichst quittieren lassen. Natürlich ist auch eine Übermittlung in elektronischer Form möglich. Die Liste muss folgende Angaben enthalten:

- Name und Kontaktdaten des Verantwortlichen (also des Vereins; in den meisten Fällen empfiehlt sich hier einfach die Anschrift und Telefonnummer der Geschäftsstelle) sowie dessen Vertreters (bei einem Verein also der vertretungsberechtigte Vorstand)

- die Kontaktdaten des Datenschutzbeauftragten (soweit ein solcher bestellt ist)
- die Verarbeitungszwecke sowie die Rechtsgrundlage für die Verarbeitung; das sind bei Mitgliedern die für die Mitgliederverwaltung erforderlichen Daten wie der Name, das Geburtsdatum, die Kontaktdaten und die Bankverbindung, ggf. weitere Daten wie die Angabe über das Vorliegen der jeweiligen Behinderung / Erkrankung. Als Rechtsgrundlage kommt Art. 6 Abs. 1 DSGVO i.V. mit dem mitgliedschaftlichen Vertragsverhältnis mit dem Verein in Betracht.
- die Empfänger der personenbezogenen Daten: das sind zum einen die eigenen Mitarbeiter, die z.B. mit der Mitgliederverwaltung betraut sind, neben etwaigen weiteren Personen wie z.B. Vorstandsmitgliedern (soweit sie tatsächlich Zugriff auf die Daten haben), zum anderen sind hier auch etwaige Stellen außerhalb des Vereins anzugeben, wenn zum Beispiel ein externes Verlagshaus die regelmäßig erscheinende Mitgliederzeitschrift erstellt und für deren Versendung die Kontaktdaten der Mitglieder erhält.
- die Dauer der Speicherung bzw. die Kriterien für die Festlegung der Dauer; das ist bei einer Mitgliedschaft regelmäßig die Dauer ebendieser; ggf. verlängert sich die Dauer aufgrund etwaiger Aufbewahrungspflichten, z.B. von Belegen für die Steuerbehörden gemäß der Abgabenordnung
- der Hinweis, dass ein Auskunftsrecht gegenüber dem Verantwortlichen hinsichtlich der gespeicherten Daten besteht; dazu gehört auch der Hinweis, dass ein Löschungs- bzw. Berichtigungsanspruch, ferner das Recht auf Einschränkung der Verarbeitung bzw. auf Widerspruch gegen die Verarbeitung oder Weitergabe der Daten an Dritte besteht.
- der Hinweis auf das Recht zum jederzeitigen Widerruf einer Einwilligung zzgl. des Hinweises, dass die Rechtmäßigkeit der Verarbeitung auf Grundlage der Einwilligung bis zum Widerruf unberührt bleibt
- der Hinweis, dass der Betroffene ein Beschwerderecht bei der zuständigen Aufsichtsbehörde hat
- die Angabe, dass die Daten aufgrund des begründeten Mitgliedschaftsverhältnisses (bzw. aufgrund eines anderen Rechtsgrundes, wie z.B. einem Arbeitsvertrag) erhoben und verarbeitet werden, sowie die

Angabe, welche Folgen die Nichtbereitstellung der Daten hätte. Letzteres ist insbesondere bei freiwilligen Angaben notwendig, die über die erforderlichen Kontaktdaten und die Bankverbindung hinausgehen.

Wir empfehlen, diese Informationen nicht nur im Falle einer Neumitgliedschaft und sonstiger neuen Datenerhebungen bereit zu stellen, sondern auch denjenigen zukommen zu lassen, deren Daten bereits erfasst sind. Da, wie gesagt, auch eine Übersendung der Informationen in elektronischer Form möglich ist, sollte zur Einsparung der Portokosten vorrangig dieser Weg gewählt werden, soweit die E-Mail-Adresse des Betreffenden bekannt ist. Denkbar wäre auch, die Informationen Mitgliedern im Zusammenhang mit der Übersendung anderen Unterlagen, etwa der Einladung zur Mitgliederversammlung, zukommen zu lassen, wenn eine solche demnächst ansteht. Ob es ausreichend ist, für bestehende Mitgliedschaften die Liste lediglich im Internet oder in der Mitgliederzeitung zu veröffentlichen, lässt sich nach jetzigem Stand nicht abschließend beurteilen. Es dürfte dann zumindest schwierig sein, im Streitfall nachzuweisen, dass der Einzelne tatsächlich Kenntnis von den Informationen erlangt hat. Deshalb raten wir dazu, vorsorglich den Weg der Einzelübersendung der Informationen zu wählen.

Mit den erwähnten Informationspflichten einher geht ein Auskunftsrecht des Betroffenen gegenüber dem Verantwortlichen (Art. 15 DSGVO). Ein Anspruch auf Auskunft darüber, welche seiner Daten der Verantwortliche gespeichert hat und vor allen Dingen, welche er an Dritte weitergegeben hat, bestand zwar auch schon bisher. Mit der DSGVO ist dieses Auskunftsrecht nunmehr jedoch erweitert worden. Es besteht darüber hinaus abgestuft, d.h. der Betroffene kann zunächst erfragen, ob überhaupt Daten, die ihn betreffen, verarbeitet werden. Darüber hinaus kann er bejahendenfalls Auskunft verlangen, welche konkreten Daten der Verantwortliche verarbeitet sowie um welche Kategorien von Daten es sich handelt (Kontaktdaten, Gesundheitsdaten etc.). Ferner kann er Auskünfte zu den oben aufgeführten einzelnen Informationen verlangen; die Auskunft kann dann je nach Sachlage mündlich, schriftlich oder auch in elektronischer Form ergehen. Ergeht ein Auskunftsersuchen, ist dem unverzüglich, spätestens aber innerhalb eines Monats nachzukommen. Wichtig ist, dass der Verantwortliche prüft, ob der Auskunftsersuchende tatsächlich berechtigt ist, also die betreffende Person ist, deren Daten verarbeitet werden.

Das Auskunftsersuchen dürfte für Selbsthilfeorganisationen vor allem im Hinblick auf die Weitergabe von Kontaktdaten an andere gleich Betroffenen zwecks gegenseitigen Austauschs von besonderer Bedeutung sein. Hier hat der Betroffene trotz seiner vorherigen Einwilligung in die Weitergabe immer ein Auskunftsrecht, wer welche konkreten Daten von ihm erhalten hat. Damit einher geht die Pflicht des Vereins, den Betroffenen umgehend darüber zu informieren, wenn er seine Daten an eine bestimmte Person weitergegeben hat. Zu berücksichtigen ist im Übrigen, dass der Betroffene natürlich auch ein Widerrufsrecht hat und seine Einwilligung in die Weitergabe seiner Kontaktdaten jederzeit zurückzunehmen kann.

Zu den erwähnenswerten Betroffenenrechten, die über die bisherigen Rechte hinausgehen, ist schließlich noch das stärker ausgeprägte Beschwerderecht bei der zuständigen Aufsichtsbehörde zu erwähnen (vgl. Art. 77 DSGVO). Daneben kommt natürlich auch nach wie vor die Möglichkeit in Betracht, gegen eine Datenschutzverletzung gerichtlich vorzugehen, wobei nunmehr sogar eine Art Verbandsklagerecht von Verbraucherschutzorganisationen besteht (Art. 80 DSGVO). Neben dem Ersatz eines materiellen Schadens ist im Übrigen nunmehr auch ausdrücklich der Ersatz von immateriellen Schäden (Schmerzensgeld) im Wege einer Schadensersatzklage möglich (Art. 82 DSGVO).

**Rechenschafts- und Dokumentationspflichten**

Bisher bestand grundsätzlich nur die Pflicht, ein sog. internes Verfahrens-verzeichnis zu erstellen – also eine Übersicht über die internen Abläufe und Zuständigkeiten bei der Datenverarbeitung – und nur in bestimmten Fällen eine zusätzliche Meldepflicht gegenüber der Aufsichtsbehörde bzw. ein Gebot zur Veröffentlichung. Künftig besteht nach Art. 30 DSGVO eine Pflicht zur Erstellung und zum Führen eines Verzeichnisses aller Verarbeitungstätigkeiten mit personenbezogenen Daten für alle Unternehmen und Organisationen, die eine Datenverarbeitung nicht nur gelegentlich durchführen, und zwar unabhängig von der Art der Daten und der Anzahl der mit der Verarbeitung befassten Personen. Schon wegen der regelmäßigen Mitgliederverwaltung dürften hiervon auch alle Selbsthilfeverbände betroffen sein.

Von der entsprechenden Dokumentationspflicht befreit sind letztlich nur Unternehmen und Organisationen mit weniger als 250 Mitarbeitern, die nur gelegentlich eine Datenverarbeitung vornehmen und überdies auch keine Verarbeitungen personenbezogenen Daten durchführen, die „ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen“. Von der Pflicht zur Erstellung eines entsprechenden Verzeichnisses sind umgekehrt auch externe Auftragnehmer betroffen, wenn an diese der Auftrag zur Datenverarbeitung erteilt worden ist.

Das Verzeichnis von Verarbeitungstätigkeiten ist künftig in erster Linie für die zuständige Aufsichtsbehörde gedacht und muss nicht mehr zwingend für jedermann einsehbar veröffentlicht werden. Die Aufsichtsbehörde kann das Verzeichnis jederzeit anfordern, weshalb es von den Organisationen bereitzuhalten ist und regelmäßig aktualisiert werden sollte. Die Dokumentation kann wahlweise in schriftlicher oder in elektronischer Form erfolgen.

Das Verzeichnis muss wesentliche Angaben zur Verarbeitung beinhalten, dazu gehört der Zweck der Verarbeitung, eine Beschreibung der Kategorien der personenbezogenen Daten (Kontaktdaten, Bankdaten, ggf. Gesundheitsdaten und weitere personenbezogene Daten), der betroffenen Personen (im Verein: Mitglieder, Mitarbeiter, Dritte) und der Empfänger (innerhalb der Organisation sowie im Falle einer Weiterleitung an Dritte). Ferner sind die technischen und organisatorischen Maßnahmen zu beschreiben, also vor allem auch Strukturen, Arbeitsprozesse und Kontrollmechanismen. Wie konkret diese Beschreibung zu erfolgen hat, ist der DSGVO nicht zu entnehmen, sie sollte jedoch so genau erfolgen, dass die Aufsichtsbehörde eine Rechtmäßigkeitsprüfung vornehmen kann.

Neben der Erstellung des Verzeichnisses beinhaltet die Rechenschafts- und Dokumentationspflicht nach der DSGVO auch den Nachweis der erforderlichen Einwilligungen zur Datenerhebung und -verarbeitung sowie der Ordnungsmäßigkeit der gesamten Verarbeitung (vgl. Art. 5 DSGVO). Letzteres beruht auf einer entsprechenden Vorgabe in Art. 24 DSGVO, wonach verlangt wird, die Umsetzung der Regelungen nach der DSGVO im Hinblick auf die konkrete Situation in der Organisation (Größenordnung der anfallenden Daten, Art der

Daten, Strukturen, technische Voraussetzungen, Anzahl der befassten Mitarbeiter, Verantwortlichkeiten etc.) sicherzustellen und hierzu einen entsprechenden Nachweis zu erbringen.

**Datenschutz-Folgenabschätzung**

Selbst wenn die Verarbeitung personenbezogener Daten rechtmäßig ist und die gesetzlichen Regelungen eingehalten werden, bleiben immer (Rest-)Risiken für die Betroffenen bestehen, etwa aufgrund eines möglichen Hackerangriffs. Diese Risiken erhöhen bzw. verschärfen sich, wenn es sich um besonders sensible Daten handelt oder eine Vielzahl an personenbezogenen Daten erhoben und umfassend ausgewertet wird.

Vor diesem Hintergrund sieht die DSGVO vor, dass im Falle eines hohen Risikos eine sog. Datenschutz-Folgenabschätzung vorzunehmen ist (Art. 35 DSGVO). Dabei geben die in Art. 35 Abs. 3 DSGVO genannten Beispielfälle einen Hinweis darauf, wann von einem solchen hohen Risiko auszugehen ist, etwa im Falle einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO. Hierunter fallen, wie oben dargelegt, auch Gesundheitsdaten. Aber selbst wenn eine Selbsthilfeorganisation bei einem Mitgliedsantrag abfragt, ob die betreffende Behinderung oder Erkrankung beim Neumitglied vorliegt, wird es sich hierbei in der Regel noch nicht um eine „umfangreiche Verarbeitung“ im Sinne der genannten Norm handeln.

Zum jetzigen Zeitpunkt kann aber noch keine abschließende Beurteilung abgegeben werden, ob und inwieweit Selbsthilfeorganisationen von einer Datenschutz-Folgenabschätzung tatsächlich regelmäßig absehen können bzw. welche konkreten Kriterien hierfür ausschlaggebend sind. Denn die Datenschutzaufsichtsbehörden werden hierzu noch eine Liste mit Verarbeitungstätigkeiten veröffentlichen, bei denen eine Datenschutz-Folgenabschätzung vorzunehmen ist. Wann diese Liste veröffentlicht wird, ist derzeit noch nicht bekannt.

## Meldepflicht bei Verstößen gegen den Datenschutz

Zu beachten ist, dass nach Art. 33 DSGVO Verstöße gegen den Datenschutz bzw. Datenpannen der Aufsichtsbehörde innerhalb von 72 Stunden zu melden sind; auch der Betroffene ist „ohne unangemessene Verzögerung“ hierüber zu informieren. Damit sind nicht nur selbst verursachte Verstöße gemeint, etwa die versehentliche Herausgabe von Mitgliedsdaten an Dritte ohne deren Wissen und Einwilligung der Betroffenen, sondern auch kaum kontrollierbare Einwirkungen von außen, die zu Datenschutz-Verstößen führen, etwa sog. Hackerangriffe.

## „Recht auf Vergessenwerden“ / Löschungsanspruch

Der Löschungsanspruch, der mit dem Wegfall des Grundes zur Daten-speicherung entsteht, wird in der DSGVO als „Recht auf Vergessenwerden“ bezeichnet, vgl. Art. 17 DSGVO. Damit einher geht die Pflicht, nicht mehr benötigte Daten unverzüglich zu löschen. Wie bisher kann einer sofortigen Löschung allerdings trotz Wegfalls des Grundes (z.B. Beendigung der Mitgliedschaft oder Widerruf einer Einwilligung) eine Pflicht oder Obliegenheit zur weiteren Speicherung entgegenstehen, wenn Sonderregelungen dies verlangen, zum Beispiel die Aufbewahrungspflicht von Steuerunterlagen nach der Abgabenordnung. Auch in den Fällen, dass etwa noch offene Beitragsforderungen bestehen oder ein Rechtsstreit zu erwarten ist, berechtigen den Verantwortlichen nach wie vor dazu, die erforderlichen Daten weiterhin zu speichern. Damit geht umgekehrt das Recht des Betroffenen auf Einschränkung der Verarbeitung einher (Art. 18 DSGVO), das dem bisherigen Anspruch auf Sperrung entspricht.

Wichtig ist, dass die Löschung datenschutzkonform erfolgt und dokumentiert wird. Je nach Art der zu löschenden Daten, kann es sinnvoll sein, Unterlagen in Papierform wie auch auf Datenspeichern befindliche Daten einem zertifizierten Entsorger zuzuführen. Übernimmt man selbst die Entsorgung, ist eine ordnungsmäße Vernichtung unter Beachtung der einschlägigen DIN 66399 sicherzustellen.

## Auftragsdatenverarbeitung

Überträgt ein Verantwortlicher die anfallende Datenverarbeitung oder Teile von ihr an einen externen Anbieter, so bestanden auch bisher schon genaue Vorgaben, wie sicherzustellen ist, dass diese Daten ordnungsgemäß verwendet werden und vor allem nicht weitergegeben bzw. dem Zugriff Dritter ausgesetzt sind. Diese Vorgaben werden nunmehr nochmals in Art. 28 DSGVO verschärft, und insbesondere den Auftragsnehmer treffen zusätzliche Pflichten. Die Vorgaben sind übrigens auch schon zu beachten, wenn Daten in der Cloud einer externen Firma abgelegt werden oder wenn eine externe Firma mit Wartungsarbeiten an den technischen Geräten beim Verantwortlichen beauftragt wird und dabei Zugriff auf die dort gespeicherten Daten hat.

## Datenschutzbeauftragter

Es bleibt bei den bisherigen Vorgaben, wann die Bestellung eines Datenschutzbeauftragten verpflichtend ist. Das ist vor allem der Fall, wenn mindestens 10 Personen regelmäßig mit der Datenverarbeitung beschäftigt sind. Zu beachten ist neuerdings aber auch, dass die Kontaktdaten des Datenschutzbeauftragten – soweit ein solcher bestellt ist – bekannt zu geben und überdies an die Aufsichtsbehörde zu melden sind (Art. 37 DSGVO).

## Aufsichtsbehörden und Bußgeldvorschriften

Mit der DSGVO erhalten die Aufsichtsbehörden – das sind in Deutschland in erster Linie die Bundesdatenschutzbeauftragte und die Landesdatenschutz-beauftragten – weitaus mehr Befugnisse als bisher (vgl. Art. 51 ff DSGVO). Dazu ist in der Grundverordnung ein umfassender Katalog von Untersuchungs- und Abhilfebefugnissen enthalten. Vor allem besteht künftig die Möglichkeit, bei Unternehmen und Organisationen (also auch bei Vereinen) anlassbezogene wie auch anlassunabhängige Überprüfungen vorzunehmen, d.h. sie sind u.a. berechtigt zum Zugang zu Geschäftsräumen und zum Zugriff auf technische Anlagen. Außerdem können sie diesbezügliche Anordnungen treffen, bis hin zur Untersagung einer Datenverarbeitung. Im Zusammenhang mit einer Untersuchung bestehen für den Verantwortlichen bzw. den Auftragsverarbeiter entsprechende Mitwirkungspflichten, und Anordnungen können insoweit auch

notfalls mit Zwangsmitteln durchgesetzt werden. Verstöße gegen die Regelungen der DSGVO bzw. das Nichtbefolgen von Anordnungen können im Übrigen ordnungswidrigkeits-rechtlich sanktioniert werden, einschließlich der Auferlegung von Bußgeldern von bis zu 20 Mio. Euro oder 4 % des Umsatzes. Die Möglichkeiten zur Ahndung von Verstößen sind damit erheblich verschärft worden.

Wie bisher ist jedoch davon auszugehen, dass die Behörden im Falle eines leichten Verstoßes oder Versäumnisses den betreffenden Verantwortlichen hierauf erst einmal nur ansprechen und eine entsprechende Nachbesserung innerhalb einer bestimmten Frist fordern. Dementsprechend sieht auch die DSGVO vor, dass zunächst vorsorgliche Warnungen bzw. Verwarnungen ausgesprochen werden können, wenn Verstöße gegen die DSGVO erkennbar werden.

**Zertifizierungstellen**

Schon bisher bestand die Möglichkeit, das eigene Datenschutz-Konzept bzw. die entsprechenden Vorkehrungen zertifizieren zu lassen, um hierdurch zum Ausdruck zu bringen, dass die datenschutzrechtlichen Vorgaben im Unternehmen oder in der Organisation eingehalten werden. Problematisch war allerdings die Uneinheitlichkeit der entsprechenden Datenschutzsiegel und Prüfzeichen sowie der vorausgehenden Zertifizierungsverfahren. Nach Art. 42 Abs. 5 DSGVO können nunmehr akkreditierte Zertifizierungsstellen, aber auch die zuständigen Aufsichtsbehörden eine Datenschutz-Zertifizierung nach DSGVO für maximal drei Jahre erteilen. Eine Zertifizierung kann zum Nachweis der Einhaltung aller datenschutzrechtlichen Vorgaben nach der DSGVO beitragen und dient nicht zuletzt als Qualitätsbeleg nach außen für den ordnungsgemäßen und gewissenhaften Umgang mit personenbezogenen Daten in der entsprechenden Organisation.

Ob es für jede Selbsthilfeorganisation Sinn macht, eine solche Zertifizierung zu beantragen, lässt sich derzeit nur schwer beantworten. Denn die konkreten Kriterien für die Vergabe einer Zertifizierung befinden sich ohnehin noch in der Entwicklung. Auf jeden Fall ist zu empfehlen, sich im Vorfeld nochmals über die genauen Rahmenbedingungen zu erkundigen.

**Umsetzungsschritte**

Obwohl die vorstehenden Erläuterungen umfangreich erscheinen, dürften – wie eingangs erwähnt – diejenigen Verbände, die die nach der bestehenden Rechtslage alle erforderlichen Maßnahmen zum Datenschutz bereits ergriffen haben, nur noch teilweise Anpassungen und Ergänzungen vornehmen müssen. Ein Hauptaugenmerk wird in der Betrachtung der gegebenen Situation in Sachen Datenschutz und die anschließende Klärung des Bedarfs sein, welche Maßnahmen vor dem Hintergrund des DSGVO noch zu treffen sind. Darüber hinaus wird vermutlich die Zusammenstellung der erforderlichen Dokumentationen sowie Informationen für den Betroffenen einen gewissen Aufwand erfordern. Schwierigster Punkt wird allerdings nach wie vor die Überzeugung aller mit der Datenverarbeitung befassten Personen im Verein sein, den Datenschutz hinreichend zu beachten und ernst zu nehmen. Die strengeren Vorgaben und Sanktionsmöglichkeiten nach der DSGVO mögen insoweit zwar zur Disziplinierung beitragen. Die Erfahrung zeigt jedoch, dass gerade im Rahmen der alltäglichen Arbeitsabläufe die Berücksichtigung des Datenschutzes allzu schnell aus dem Blick gerät. Auf jeden Fall sollten alle Personen in Ihrer Organisation, die mit der Datenverarbeitung zu tun haben oder hierfür (mit-)verantwortlich sind, über die DSGVO und die damit verbundenen Änderungen informiert werden.

Soweit ein Datenschutzbeauftragter bestellt ist, bietet es sich an, dass dieser die notwendigen Informationen weiterträgt. Grundsätzlich gehört es dann auch zu seinen Aufgaben, den Umsetzungsprozess zu begleiten und erforderliche Prüfungen vorzunehmen bzw. Hinweise zu geben. Selbstverständlich bleibt die Verantwortung für die hinreichende Umsetzung der DSGVO letztlich beim Vorstand. Von zentraler Bedeutung ist außerdem auch, dass Datenschutz künftig bei allen Maßnahmen und Vereinsaktivitäten von vornherein „mitgedacht“ wird, etwa bei der Durchführung von Veranstaltungen, bei der Aufnahme neuer Mitglieder und der Einstellung neuer Mitarbeiter, bei der Anschaffung neuer Technik und Software etc.

Im Hinblick auf die ersten Maßnahmen und Schritte zur Umsetzung der DSGVO ist zu empfehlen, sich zunächst einen umfassenden Überblick über den Ist-Zustand im Zusammenhang mit der Datenerfassung und -verarbeitung in der

eigenen Organisation zu verschaffen: Welche Daten (von Mitgliedern, Mitarbeitern, sonstigen Personen) werden gespeichert und welche werden an Dritte weitergegeben? Liegen hierfür Einwilligungen bzw. Ermächtigungsgrundlagen vor? Wie sehen die internen Arbeitsabläufe, Zuständigkeiten und Berechtigungen im Zusammenhang mit der Datenverarbeitung aus? Ist dies in einer Geschäftsordnung oder durch konkrete Dienstanweisungen geregelt? Welche Sicherheitsvorkehrungen bestehen, etwa bei den technischen Voraussetzungen (Hard- wie Software), bei der Passwortvergabe, bei der Schulung der mit der Datenverarbeitung befassten Personen im Verein oder auch bei der Löschung der Daten? Wird die Datenverarbeitung bereits in Form eines Verfahrensverzeichnisses, einer Vorabkontrolle oder auch eines vergleichbaren Konzepts seitens der Vorstandes/der Geschäftsführung bzw. des Datenschutzbeauftragten dokumentiert?

Im Anschluss wäre dieser Ist-Zustand mit den oben aufgeführten Erfordernissen nach der DSGVO zu vergleichen. Vermutlich dürften danach für die Selbsthilfeorganisationen der BAG SELBSTHILFE vor allem folgende Maßnahmen und Arbeiten erforderlich werden:

- Zusammenstellung der Informationen für alle Personen(gruppen), deren personenbezogenen Daten erfasst und verarbeitet werden, sowie Zuleitung dieser Informationen an die Betreffenden bzw. Bereitstellung für künftige Fälle einer neuen Datenerhebung (etwa bei Begründung einer neuen Mitgliedschaft) sowie bei Auskunftsersuchen

sowie

- Erstellung einer Dokumentation über alle Abläufe, Zuständigkeiten, Sicherheitsvorkehrungen etc. im Zusammenhang mit der im Verein erfolgenden Datenverarbeitung (ggf. ist hier nur eine Überarbeitung einer bereits bestehenden Übersicht bzw. eines Verfahrensverzeichnisses erforderlich; dieses ist auf jeden Fall auch auf seine Aktualität zu überprüfen)