Richtlinie

zum Datenschutz

in der Deutsche Taekwondo Union e.V.

(DSR)

Version 1.0 vom 03.01.2024

Datenschutzbeauftragter / Foth

Inhaltsverzeichnis

Version	Beschreibung	Datum	Autor
1.0	Initiale Erstellung	12. Dezember 2023	MFO
1.1	Aufnahme verbandsspezifischer Fragen	01. Januar 2023	MFO

ds-sport@ibs-data-protection.de

1 Präambel

Ab dem 25. Mai 2018 wird die Datenschutz-Grundverordnung (DS-GVO) in Deutschland und in allen anderen Mitgliedstaaten der Europäischen Union geltendes Recht. Die DS-GVO ist ab diesem Zeitpunkt unmittelbar anwendbar und verdrängt die bisher geltenden datenschutzrechtlichen Regelungen. An einigen Stellen der Grundverordnung ist der nationale Gesetzgeber ermächtigt, die Regelungen der Verordnung zu konkretisieren und zu ergänzen (sogenannte Öffnungsklauseln). Hiervon hat der Gesetzgeber durch die Schaffung des BDSG-neu Gebrauch gemacht. Rechtsgrundlage für die Verarbeitung personenbezogener Daten sind daher ab dem 25. Mai 2018 die DS-GVO (mitsamt ihren „Erwägungsgründen“) und das BDSG-neu.

Verarbeitet ein Verein (Verband) ganz oder teilweise automatisiert personenbezogene Daten seiner Mitglieder und sonstiger Personen oder erfolgt eine nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, ist nach Art. 2 Abs. 1 DS-GVO deren Anwendungsbereich eröffnet.

Unerheblich ist dabei, ob der Verein ins Vereinsregister eingetragen ist und damit eine eigene Rechtspersönlichkeit besitzt, oder ob es sich um einen nicht rechtsfähigen Verein handelt.

Da die DS-GVO nicht mehr zwischen öffentlichen und nicht-öffentlichen Stellen unterscheidet, gelten für Vereine grundsätzlich sämtliche Vorschriften der DS-GVO.

2 Grundsätze der Verarbeitung personenbezogener Daten

Die Basis für jede Verarbeitung personenbezogener Daten bilden die gesetzlich definierten Grundsätze. Diese sind bei der Planung, Einführung, Verarbeitung und Nutzung personenbezogener Daten jederzeit zu beachten.

3 Begriffsbestimmungen

Personenbezogene Daten sind nicht nur die zur unmittelbaren Identifizierung einer natürlichen Person erforderlichen Angaben, wie etwa Name, Anschrift und Geburtsdatum, sondern darüber hinaus alle Informationen, die sich auf eine in sonstiger Weise identifizierte oder identifizierbare natürliche Personen beziehen (Art. 4 Nr. 1 DS-GVO), wie beispielsweise Familienstand, Zahl der Kinder, Beruf, Telefonnummer, E-Mail-Adresse, Anschrift, Eigentums- oder Besitzverhältnisse, persönliche Interessen, Mitgliedschaft in Organisationen, Datum des Vereinsbeitritts, sportliche Leistungen, Platzierung bei einem Wettbewerb und dergleichen. Dies gilt für Informationen jedweder Art, also für Schrift, Bild oder Tonaufnahmen. Nicht von der DS-GVO geschützt

werden Angaben über Verstorbene, wie etwa in einem Nachruf für ein verstorbenes Vereinsmitglied im Vereinsblatt oder die Nennung auf einer Liste der Verstorbenen (Erwägungsgrund 27 DS-GVO). Statt einer Unterteilung in die Erhebung, Verarbeitung oder Nutzung der Daten wie bisher wird in der DS-GVO einheitlich der Begriff Verarbeitung verwendet. Der Begriff ist sehr weit gefasst und umfasst jeden Vorgang oder jede Vorgangsreihe in Zusammenhang mit personenbezogenen Daten. Als Verarbeitungsarten nennt die DS-GVO neben dem Erheben, Erfassen, Verwenden, Offenlegen, Verbreiten, Abgleichen das Löschen sowie das Vernichten (Art. 4 Nr. 1 DS-GVO).

Dateisystem ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob die Sammlung zentral, dezentral oder nach funktionalen oder geographischen Gesichtspunkten geordnet geführt wird (Art. 4 Nr. 6 DS-GVO). Dazu zählen auch Papier-Akten.

Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DS-GVO). Dem Verein (Verband) sind seine unselbständigen Untergliederungen wie Abteilungen, Ortsvereine oder Ortsgruppen sowie seine Funktionsträger, Auftragnehmer (s. u. Nr. 3.2), und seine Mitarbeiter, soweit diese im Rahmen der Aufgabenerfüllung für den Verein tätig werden, zuzurechnen. Die Vereinsmitglieder einerseits sowie die Dachverbände andererseits, in denen der Verein selbst Mitglied ist, sind dagegen als außerhalb des Vereins stehende Stellen und damit als Dritte anzusehen.

Auftragsverarbeiter ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DS-GVO). Eine Auftragsverarbeitung spielt beispielsweise bei der Verlagerung der Mitgliederverwaltung in eine Cloud eine wichtige Rolle (s. u. Nr. 3.3), auch bei der EDV-Wartung und der Aktenvernichtung.

3.1 *Rechtmäßigkeit der Verarbeitung*

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten richtet sich nach Art. 6 Abs. 1 DS-GVO. Damit eine Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage, die sich aus der DS-GVO, aus dem sonstigen Unionsrecht oder dem Recht der Mitgliedsstaaten ergibt, verarbeitet werden (Art. 6 Abs. 1 DS-GVO; Erwägungsgrund 40 DS-GVO). Datenschutzrechtlich ist nicht etwa alles erlaubt, was nicht ausdrücklich verboten ist. Vielmehr bedarf umgekehrt jede

Verarbeitung personenbezogener Daten einer Rechtsgrundlage.

Rechtsgrundlagen

Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten kommen insbesondere Art. 6 Abs. 1 lit. b) und lit. f) DS-GVO in Betracht. Die Mitgliedschaft in einem Verein ist als Vertragsverhältnis zwischen den Mitgliedern und dem Verein anzusehen, dessen Inhalt im Wesentlichen durch die Vereinssatzung und sie ergänzende Regelungen (z.B. eine Vereinsordnung) vorgegeben wird. Eine Vereinssatzung bestimmt insoweit die Vereinsziele, für welche die Mitgliederdaten genutzt werden können.

Erhebt ein Verein personenbezogene Daten von einer betroffenen Person (z. B. Vereinsmitglied, Teilnehmer an einem Wettbewerb oder Lehrgang), so sind die Zwecke, für welche die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen (Art. 5 Abs. 1 lit. b) DS-GVO).

Hierbei ist jedoch zu beachten, dass die Vereinssatzung einer Inhaltskontrolle nach § 242 des Bürgerlichen Gesetzbuches (BGB) unterliegt. Das Vereinsmitglied ist vor unbillig überraschenden Bestimmungen und Belastungen zu schützen, mit denen es beim Vereinsbeitritt nicht rechnen konnte. Regelungen in der Vereinssatzung, die verfassungsrechtlich geschützte Positionen der Mitglieder beeinträchtigen, sind daher unwirksam. Dies kann etwa dann der Fall sein, wenn der Verein durch die Satzung eine Verarbeitung personenbezogener Daten vorsieht, die weder für die Begründung und Durchführung des zwischen Mitglied und Verein durch den Beitritt zustande kommenden rechtsgeschäftsähnlichen Schuldverhältnisses noch für die Erreichung des Vereinszwecks erforderlich ist.

Auch später darf die Vereinsatzung in Bezug auf die Verarbeitung personenbezogener Daten nicht einfach durch Mehrheitsbeschluss geändert werden. Erfordert der neue Vereinszweck eine weitergehende Verarbeitung personenbezogener Daten, darf die Satzung nur insoweit geändert werden, wie der neue Verarbeitungszweck mit dem ursprünglichen in einem Zusammenhang steht (vgl. Art. 6 Abs. 4 lit. a) DS-GVO, Erwägungsgrund 50). Aus dem Vertragsverhältnis folgt, dass der Verein bei der Erhebung, Verarbeitung und Nutzung von Daten die Datenschutzgrundrechte seiner Mitglieder angemessen berücksichtigen muss.

Informationspflichten

Erfolgt eine Erhebung personenbezogener Daten direkt bei der betroffenen Person, so hat der Verein aus Gründen der Transparenz von Datenverarbeitungsprozessen zum Zeitpunkt der Da-

tenerhebung eine entsprechende datenschutzrechtliche Unterrichtung vorzunehmen (Art. 13 Abs. 1 und Abs. 2 DS-GVO). Daraus folgt, dass der Verein in jedem Formular, das er zur Erhebung personenbezogener Daten nutzt, auf Folgendes hinweisen muss:

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
- Kontaktdaten des Datenschutzbeauftragten
- Zwecke der Verarbeitung (bitte im Einzelnen aufzählen)
- Rechtsgrundlage der Verarbeitung
- berechtigte Interessen i.S.d. Art. 6 Abs. 1 lit. f) DS-GVO
- Empfänger oder Kategorien von Empfängern (z.B. Weitergabe personenbezogener Daten an eine Versicherung, an den Dachverband, an alle Vereinsmitglieder, im Internet)
- Absicht über Drittlandtransfer (z.B. bei Mitgliederverwaltung in der Cloud), sowie Hinweis auf (Fehlen von) Garantien zur Datensicherheit
- Speicherdauer der personenbezogenen Daten
- Belehrung über Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht gegen Verarbeitung)
- Hinweis auf jederzeitiges Widerrufsrecht der Einwilligung
- Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde

Teilt der Verantwortliche die vorgesehenen Informationen nicht, nicht vollständig oder inhaltlich unrichtig mit, so verletzt er seine Informationspflichten. Das ist gemäß Art. 83 Abs. 5 lit. b) DS-GVO bußgeldbewehrt. Werden personenbezogene Datei auf andere Weise als bei der betroffenen Person erhoben, so richten sich die Informationspflichten nach Art. 14 Abs. 1 und Abs. 2 DS-GVO. Die meisten der Informationspflichten aus Art. 14 Abs. 1 und Abs. 2 DS-GVO haben denselben Inhalt wie Art. 13 Abs. 1 und Abs. 2 DS-GVO. Zusätzlich muss der Verein die betroffene Person über die Kategorie der verarbeiteten personenbezogenen Daten und über die Quelle der erhobenen Daten informieren. Der Verein muss diese Informationen innerhalb einer angemessenen Frist, spätestens jedoch innerhalb eines Monats nach der Erhebung erteilen (Art. 14 Abs. 3 lit a) DS-GVO). Ein Verstoß gegen die Informationspflicht kann eine Geldbuße gemäß Art. 83 Abs. 5 lit. b) DS-GVO zur Folge haben.

Schriftliche Regelungen zum Datenschutz - Datenschutzrichtlinie

Den Verein trifft die Pflicht, die Grundzüge der Datenerhebung, -verarbeitung und -nutzung schriftlich festzulegen. Entsprechende Datenschutzregelungen können entweder in die Vereinssatzung aufgenommen oder in einem gesonderten Regelwerk niedergelegt werden. Für Letzteres gibt es keine feste Bezeichnung; am gebräuchlichsten sind noch die Begriffe „Datenschutz-

ordnung“, „Datenschutzrichtlinie“ oder „Datenverarbeitungsrichtlinie“. Die Datenschutzordnung kann, wenn die Vereinssatzung nichts anderes bestimmt, vom Vorstand oder von der Mitgliederversammlung beschlossen werden und muss nicht die Qualität einer Satzung habe.

Es ist empfehlenswert, sich beim Aufbau der Datenschutzregelungen am Weg der Daten von der Erhebung über die Speicherung, Nutzung, Verarbeitung (insbesondere Übermittlung) bis zu ihrer Sperrung und Löschung zu orientieren. Dabei ist jeweils konkret festzulegen, welche Daten (z.B. Name, Vorname, Adresse, E-Mail-Adresse usw.) welcher Personen (z.B. Vereinsmitglieder, Teilnehmer an Veranstaltungen oder Lehrgängen, Besucher von Veranstaltungen) für welche Zwecke verwendet werden, ggf. auch, ob Vordrucke und Formulare zum Einsatz kommen. Die bloße Wiedergabe des Wortlauts der Bestimmungen der DS-GVO bzw. des BDSG-neu sind in keinem Fall ausreichend. Die DS-GVO bzw. das BDSG-neu machen die Zulässigkeit der Verarbeitung von Daten vielfach von Interessenabwägungen abhängig oder stellt sie unter den Vorbehalt der Erforderlichkeit. Im Interesse der Rechtssicherheit sollten diese abstrakten Vorgaben soweit irgend möglich konkretisiert und durch auf die Besonderheiten und Bedürfnisse des jeweiligen Vereins angepasste eindeutige Regelungen ersetzt werden.

Der Verein sollte insbesondere schriftlich festlegen, welche Daten beim Vereinseintritt für die Verfolgung des Vereinsziels und für die Mitgliederbetreuung und -verwaltung notwendigerweise erhoben werden. Auch sollte geregelt werden, welche Daten für welche andere Zwecke des Vereins oder zur Wahrnehmung der Interessen Dritter bei den Mitgliedern in Erfahrung gebracht werden. Ferner muss geregelt werden, welche Daten von Dritten erhoben werden, wobei hier auch der Erhebungszweck festzulegen ist. Auch sollte erkennbar sein, welche Angaben für Leistungen des Vereins erforderlich sind, die nicht erbracht werden können, wenn der Betroffene nicht die dafür erforderlichen Auskünfte gibt.

Der Verein sollte außerdem regeln, welcher Funktionsträger zu welchen Daten Zugang hat und zu welchem Zweck er Daten von Mitgliedern und Dritten verarbeiten und nutzen darf. Ferner sollte geregelt werden, welche Daten zu welchem Zweck im Wege der Auftragsdatenverarbeitung (s. u. Nr. 3.2) verarbeitet werden.

Des Weiteren sollte der Verein festlegen, zu welchem Zweck welche Daten von wem an welche Stellen (das können auch Vereinsmitglieder sein) übermittelt werden bzw. welche Daten so gespeichert werden (dürfen), dass Dritte - also Personen, die die nicht zur regelmäßigen Nutzung der Daten befugt sind (s. u. Nr. 4.1) - darauf Zugriff nehmen können. Der Kreis dieser Zugriffsberechtigten muss genau beschrieben sein. Auch muss geregelt werden, unter welchen Vo-

raussetzungen welche Datenübermittlung erfolgen darf, insbesondere welche Interessen des Vereins oder des Empfängers dabei als berechtigt anzusehen sind. Auch sollte festgelegt werden, zu welchem Zweck die Empfänger die erhaltenen Daten nutzen dürfen und ob sie sie weitergeben können. Ferner sollte geregelt sein, welche Daten üblicherweise am „Schwarzen Brett“ oder in den Vereinsnachrichten offenbart und welche in das Internet oder Intranet eingestellt werden.

Einwilligung

Eine Einwilligung in die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist erforderlich, soweit der Verein in weitergehendem Maße personenbezogene Daten verarbeitet, als er aufgrund der unten unter Nr. 2, 4 und 5 dargestellten Regelungen befugt ist. Es empfiehlt sich nicht, Einwilligungen für Datenverarbeitungsmaßnahmen einzuholen, die bereits aufgrund einer gesetzlichen Erlaubnis möglich sind. Denn dadurch wird beim Betroffenen der Eindruck erweckt, er könne mit der Verweigerung der Einwilligung oder ihrem späterem Widerruf die Datenverarbeitung verhindern. Hat der Verein aber von vornherein die Absicht, im Falle der Verweigerung des Einverständnisses auf die gesetzliche Verarbeitungsbefugnis zurückzugreifen, wird der Betroffene getäuscht, wenn man ihn erst nach seiner ausdrücklichen Einwilligung fragt, dann aber doch auf gesetzliche Ermächtigungen zurückgreift.

Eine Einwilligung ist datenschutzrechtlich nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht und dieser zuvor ausreichend und verständlich darüber informiert worden ist, welche Daten aufgrund der Einwilligung für welchen Zweck vom Verein verarbeitet werden sollen. Insbesondere soll darauf aufmerksam gemacht werden, welche verschiedenen Verarbeitungsvorgänge i.S. des Art. 4 lit. a) DS-GVO vorgesehen sind, unter welchen Voraussetzungen die Daten an Dritte weitergegeben werden, dass die Erklärung freiwillig ist, wie lange die Daten bei wem gespeichert sein sollen und was die Einwilligung rechtlich für die betroffene Person bedeutet. Soweit es nach den Umständen des Einzelfalles erforderlich ist, oder wenn die betroffene Person das verlangt, soll sie auch über die Folgen der Verweigerung der Einwilligung belehrt werden (§ 51 Abs. 4 Sätze 3 und 4 BDSG-neu). Auch soll die betroffene Person vor der Abgabe der Einwilligung darauf aufmerksam gemacht werden, dass sie diese stets widerrufen kann (§ 51 Abs. 3 Satz 3 BDSG-neu). Eine Dokumentation dieser Informationen ist nicht vorgeschrieben, doch ist der Erklärungsempfänger ggf. beweispflichtig, dass bzw. mit welchem Inhalt die Hinweise erfolgt sind. Die Aufnahme in einem Verein darf grundsätzlich nicht von der Einwilligung in die Datenverarbeitung für vereinsfremde Zwecke abhängig gemacht werden (Art. 7 Abs. 4 DS-GVO).

Im Gegensatz zum BDSG, das für Einwilligungen grundsätzlich die Schriftform und nur ausnahmsweise auch die elektronische Form zulässt, ermöglicht die DS-GVO, dass die Einwilligung schriftlich, elektronisch, mündlich oder sogar konkludent erfolgen kann.

Jedoch muss der Verein für den Fall, dass die Verarbeitung auf einer Einwilligung beruht, nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat (Art. 7 Abs. 1 DS-GVO). Aus diesem Grund ist zu anzuraten, Einwilligungen zum Zwecke des Nachweises schriftlich einzuholen oder die Abgabe einer Einwilligung anderweitig zu dokumentieren.

Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche oder elektronische Erklärung, muss bereits das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von anderen Sachverhalten klar zu unterscheiden ist (Art. 7 Abs. 2 Satz 1 DS-GVO; § 51 Abs. 2 BDSG-neu). Nicht zuletzt deswegen muss die Einwilligungspassage selbst, wenn sie Teil eines größeren Textes ist, optisch hervorgehoben werden.

Dies kann durch drucktechnische Hervorhebung oder Absetzen vom sonstigen Erklärungstext geschehen. Da grundsätzlich für jede Art der Datenverarbeitung i. S. des Art. 6 lit. a) DS-GVO und für jeden Verarbeitungsvorgang eine gesonderte Einwilligung eingeholt werden muss (Erwägungsgrund 43 DS-GVO), soll bei Einwilligungen zu Datenübermittlungen an verschiedene Empfänger für unterschiedliche Zwecke der Vordruck so gestaltet sein, dass ein Beitrittswilliger bei der Abgabe seiner Erklärung durch Ankreuzen differenzieren kann.

Datenschutzrechtliche Einwilligungen der Vereinsmitglieder können nicht durch Mehrheitsbeschlüsse der Mitgliederversammlung oder des Vorstands ersetzt werden. Eine sogenannte „Widerspruchslösung“, wonach die Einwilligung unterstellt wird, wenn der Betroffene einer Datenverarbeitungsmaßnahme - etwa der Veröffentlichung seiner Personalien im Internet - nicht ausdrücklich widerspricht, stellt keine wirksame Einwilligung dar.

Eine starre Altersgrenze in Bezug auf die Einwilligungsfähigkeit kennt die DS-GVO außerhalb des Art. 8 DS-GVO (diese Vorschrift gilt nur im Zusammenhang mit kindorientierten Telemedien, wie z.B. an Kinder gerichtete Onlineshops und -spiele) nicht. Kinder und Jugendliche können daher in die Verarbeitung ihrer personenbezogenen Daten selbst einwilligen, wenn sie in der Lage sind, die Konsequenzen der Verwendung ihrer Daten zu übersehen und sich deshalb auch verbindlich dazu zu äußern. Maßgeblich ist der jeweilige Verwendungszusammen-

hang der Daten und der Reifegrad bzw. die Lebenserfahrung des Betroffenen. Bei Kindern unter 13 Jahren ist regelmäßig davon auszugehen, dass sie die Konsequenzen der Verwendung ihrer Daten nicht übersehen können. Ist die Einsichtsfähigkeit zu verneinen, ist die Verarbeitung seiner personenbezogenen Daten nur mit Einwilligung seines Sorgeberechtigten zulässig.

Als Anlage ist das Muster einer Einwilligungserklärung für die Veröffentlichung personenbezogener Mitgliederdaten im Internet beigefügt. Es empfiehlt sich, eine solche Einwilligung von Neumitgliedern bereits bei der Aufnahme in den Verein einzuholen. Altmitglieder können über die Vereinsmitteilungen eine allgemeine Information mit einer derartigen Einwilligungserklärung und dem Hinweis auf das jederzeitige Widerrufsrecht erhalten. Dabei sollte ein Formular Folgendes berücksichtigen:

- Das Vereinsmitglied erteilt seine Einwilligung freiwillig und kann sie jederzeit widerrufen. Das Mitglied kann den Umfang der zu veröffentlichenden Daten von vornherein beschränken.

- Dem Mitglied muss die Tragweite seiner Erklärung bewusst sein. Das ist nur der Fall, wenn es weiß, welche seiner Daten in das Internet eingestellt werden sollen.

4 Schutzbedarf und Schutzmaßnahmen

Jede Verarbeitung personenbezogener Daten stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Das betrifft auch solche Verarbeitungen, die aus datenschutzrechtlicher Sicht zulässig sind, also auf der Basis einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung erfolgen. Das Haus muss unter Berücksichtigung der Eingriffsintensität den jeweiligen Schutzbedarf im Zusammenhang mit der Verarbeitung von personenbezogenen Daten ermitteln, um anschließend systematisch abgeleitete standardisierte Schutzmaßnahmen (insbesondere geeignete und angemessene technisch und organisatorische Maßnahmen) zu definieren. Je höher der Schutzbedarf ist, desto höher müssen die Schutzmaßnahmen im Einzelnen sein, so dass stets ein angemessenes Schutzniveau gewährleistet wird.

4.1 *Schutzbedarf*

Bei der Ermittlung des Schutzbedarfs, die in der Meldung einer Verarbeitungstätigkeit integriert ist, wird die Perspektive der betroffenen Person und deren Grundrechtsausübung eingenommen. Diese Perspektive unterscheidet sich daher grundlegend von der Sicht des IT-Grundschutzes.

Für den Schutzbedarf personenbezogener Daten sind entsprechend des Standard-Datenschutzmodells (SDM) die drei Schutzbedarfskategorien „normal “, „hoch“ und „sehr hoch“ für Verfahren zur Verarbeitung personenbezogener Daten definiert.

Schutzbedarfskategorie „normal“:

Da jede Verarbeitung personenbezogener Daten einen Eingriff in die Grundrechte der betroffenen Person darstellt, kann der Schutzbedarf niemals niedriger als „normal“ sein. Deshalb ist grundsätzlich davon auszugehen, dass jeder Prozess, in dem personenbezogene Daten verarbeitet werden, mindestens normalen Schutzbedarf aufweist. Weniger schutzbedürftig können folgerichtig nur Verarbeitungen mit nichtpersonenbezogenen Daten sein.

Verarbeitungen mit normalem Schutzbedarf:

- Verarbeitung von frei zugänglichen personenbezogenen Daten, in die Einsicht gewährt wird, ohne dass der Einsichtnehmende ein berechtigtes Interesse geltend machen muss.

- Verarbeitung von personenbezogenen Daten, deren Missbrauch zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist.

Beispiele: Anschriften/Daten aus frei zugänglichen Verzeichnissen oder Quellen, interne Kommunikationsdaten, Adressbücher, Mitgliederverzeichnisse, Benutzerkataloge in Bibliotheken, Organigramme, Betriebliche Namens- und Telefonverzeichnisse, Arbeitsanweisungen, Prozess- und Organisationshandbücher, Personal- und Betriebsratsmitteilungen

Schutzbedarfskategorie „hoch“:

Ein hoher Schutzbedarf für einen Prozess, in dem personenbezogene Daten verarbeitet werden, besteht insbesondere dann, wenn betroffene Personen von den Entscheidungen bzw. Leistungen einer Organisation abhängig sind, wenn die Verarbeitung zu erheblichen Konsequenzen für die betroffene Person führen kann, wenn die Verarbeitung gesetzlich als besonders schutzwürdig (z.B. immer bei der Verarbeitung besonderer Kategorien personenbezogener Daten) ausgewiesen ist oder wenn die Verarbeitung keine real nachweislich funktionierende Möglichkeiten der Intervention und des Selbstschutzes für betroffene Personen bereitstellt.

Verarbeitungen mit hohem Schutzbedarf:

- Verarbeitung von personenbezogenen Daten, deren Missbrauch betroffene Personen in deren gesellschaftlichen Stellung oder in deren wirtschaftlichen Verhältnissen beein-

trächtigen kann ("Ansehen"),

- Verarbeitung eindeutig identifizierender, hoch verknüpfbarer Daten
- Verarbeitung von personenbezogenen Daten, die realistischer Weise zu erwartende Auswirkungen auf die Grundrechtsausübung einer Vielzahl von betroffener Personen haben können

Beispiele: Mitglieder- und Personaldaten (z.B. private Adressen, Bankverbindungen, Kontonummern, Geburtsdatum, Alter, Familienstand, Konfession, Staatsangehörigkeit, Einkommen, lebenslang gültige Steueridentifikationsnummer, Vermögen, Grundbesitz, Handlungsvollmacht, Zeitkontierung, Reisekostenabrechnung, Personalbeurteilungen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten), öffentliche Videoüberwachung

Schutzbedarfskategorie „ sehr hoch“ :

Von sehr hohem Schutzbedarf ist auszugehen, wenn betroffene Personen von den Entscheidungen bzw. Leistungen einer Organisation existentiell abhängig ist und zusätzliche Risiken für die betroffene Person nicht bemerkbar sind.

Verarbeitungen mit sehr hohem Schutzbedarf:

- Verarbeitung von personenbezogenen Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der betroffenen Person erheblich beeinträchtigen kann ("Existenz"),
- Verarbeitung von personenbezogenen Daten, deren Missbrauch Gesundheit, Leben oder Freiheit der betroffenen Person beeinträchtigen kann.

Beispiele: Medizinische Daten, Gerichts- und Prozessakten, Gesundheitsdaten, Unterbringung in Anstalten, Straffälligkeit, Ordnungswidrigkeiten schwerwiegender Art, dienstliche Beurteilungen, psychologisch-medizinische Untersuchungsergebnisse, Daten von Opfern einer möglichen strafbaren Handlung, Schulden, Pfändungen, Insolvenzen.

4.2 *Schutzmaßnahmen*

Bei der Beschreibung der Schutzmaßnahmen, die ebenfalls in der Meldung einer Verarbeitungstätigkeit integriert ist, werden insbesondere unter Berücksichtigung des festgelegten Schutzbedarfs, des Stands der Technik und der Implementierungskosten konkret getroffene Maßnahmen dokumentiert.

Die geeigneten Schutzmaßnahmen sind individuell für die einzelne Verarbeitungstätigkeit zu bestimmen. Eine verbindliche abschließende Festschreibung der Schutzmaßnahmen anhand des Schutzbedarfs ist daher nicht möglich.

Um trotzdem für die Bestimmung der Schutzmaßnahmen eine Orientierung zu geben, wird im Folgenden dargestellt, welche Schutzmaßnahmen in der Regel ein geeignetes Schutzniveau sicherstellen. Hierbei ist davon auszugehen, dass die jeweils höhere Schutzbedarfskategorie die Schutzmaßnahmen des niedrigeren Schutzbedarfs einhält.

	Schutzbedarfskategorie		
	normal	**hoch** zusätzlich zu den Maßnahmen "normal"	**sehr hoch** zusätzlich zu den Maßnahmen "normal" und "hoch", wenn für das Erreichen des Schutzniveaus individuell erforderlich
Zutrittskontrolle	• Pförtner • Türsicherung	• Restriktive Schlüsselvergabe • Überwachungseinrichtung (Alarmanlage, Video) • Kartenleser (Betriebsausweis)	• Zertifizierungen • Monitoring durch Externe • Aktive Incident-Systeme • Jährliche Audits • Einsatz von Prüfsummen, elektronische Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts • Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept) • Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten • Protokollierung von Zugriffen und Änderungen,
Zugangskontrolle	• User-Kennung und Passwort	• Zusätzlicher System-Log	
Zugriffskontrolle	• Differenzierte Berechtigungsvergabe • Vier-Augen-Prinzip	• Benutzerprofile • Rollen	
Weitergabekontrolle	• Verschlüsselung	• Protokollierung • Transportsicherung • Dokumentation von Abfragen	
Eingabekontrolle	• Protokollierung	• Funktionstrennung (Produktion/Test)	
Auftragskontrolle	• Eindeutige Vertragsgestaltung • Einbeziehung DSB • Formalisierte Auftragserteilung (Auftragsformular) • Kontrolle der Vertragsausführung	•	
Verfügbarkeitskontrolle	• Back up Verfahren • Unterbrechungsfreie Stromversorgung • Virenschutz / Firewall	• Sicherheitskonzept • Spiegeln von Festblatten • Getrennte Aufbewahrung • Vorliegen eines Notfallplans	
Pseudonymisierung	•	• Pseudonymisierung	
Trennungsgebot	• Mandantenfähigkeit	• Benutzerprofile	
Organisatorische Maßnahmen	• Datenschutz-Richtlinie • Verpflichtung auf das Datengeheimnis und Bankgeheimnis • Schulungen • Meldeprozess für Datenschutzverletzungen • Datenschutzmanagementsystem	• Spezielle Arbeitsanweisung	

5 Operative Datenschutz-Anforderungen

Einführung einer Verarbeitung und Datenschutzfolgeabschätzung

Damit die Anforderungen an die Rechenschaftspflicht zur Einhaltung der Datenschutzvorschriften erfüllt werden können, sind die Bereiche verpflichtet, den Datenschutzbeauftragten über die Einführung einer Verarbeitungstätigkeit personenbezogener Daten vor der Inbetriebnahme in Kenntnis zu setzen. Zur Vermeidung von nachträglichen Anpassungen bei IT-Anwendungen ist der Datenschutzbeauftragte schon im Frühstadium einer Planung einzubeziehen.

In besonderen Fällen, soweit die Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist (oder Verfahren, die bei den Aufsichtsbehörden zusätzlich als Risiko-Verfahren gelistet sind), ist darüber hinaus die Durchführung einer sog. Datenschutzfolgenabschätzung durch den verantwortlichen Bereich vorzunehmen und dem Datenschutzbeauftragten vorzulegen.

Verzeichnis der Verarbeitungstätigkeiten

Der Begriff Verarbeitungstätigkeit umfasst jede Art der Verwendung von personenbezogenen Daten (erheben, speichern, übermitteln, auswerten etc.). Der Begriff Verarbeitungstätigkeit bezieht sich auf bestimmte Prozesse / Vorgänge, die zu einem oder mehreren gemeinsamen Zwecken bzw. in einheitlicher technischer oder organisatorischer Weise Verarbeitungen vereinen und in einer Verarbeitungstätigkeit zusammengefasst werden. Beispiele: Personalbetreuung, Bewerbermanagement, Wettkämpfe, Seminare, etc.

Verfahren ganz oder teilweise automatisierter Verarbeitung personenbezogener Daten sowie nichtautomatisierte Verarbeitungen, die in einem Dateisystem gespeichert sind oder gespeichert werden, sind dem Datenschutzbeauftragten zu melden.

Gem. den gesetzlichen Vorschriften sind mindestens folgende Angaben in der Verarbeitungstätigkeit zu erheben. Weitere Informationen zur Erfüllung der Rechenschaftspflichten können zusätzlich erhoben werden:

a) den Namen und die Kontaktdaten des Verantwortlichen und die Kontaktdaten des Datenschutzbeauftragten;
b) die Zwecke der Verarbeitung;
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden;
e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland;
f) die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
g) eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Zusätzliche Angaben sind u.a.:

h) Rechtsgrundlage der Verarbeitung
i) Wahrung der Betroffenen-Rechte (Einwilligung, Transparenz, Auskunftsfähigkeit)
j) Vorsehen einer Datenportabilität
k) Herkunft der Daten
l) Betroffene Systeme und Anwendungen

Prüfungen der Datenverarbeitung

Der Datenschutzbeauftragte führt turnusmäßig und risikoorientiert Prüfungen von Verarbeitungen und Prozessen durch, um die Kontrolle auf Einhaltung durch die Verantwortlichen auf Wirksamkeit zu prüfen. Ein turnusmäßiger Auditplan zur Sicherstellung der Überwachung der Anforderungen für risikobehaftete Verarbeitungen mit einem Turnus von 3 Jahren wird als Basis durch den Datenschutzbeauftragten erstellt und dient dem Nachweis im Rahmen des Datenschutz-Managements zur Erfüllung der Rechenschaftspflicht.

Interne Mitarbeiterverpflichtungen

Jeder Beschäftigte, der Umgang mit personenbezogenen Daten hat, ist auf die Vertraulichkeit zu verpflichten. Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars.

Die unterzeichnete Verpflichtungserklärung ist Bestandteil des Arbeitsvertrages. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

Externe Mitarbeiterverpflichtungen

Jeder externe Beschäftigte (Trainer, Referenten, usw.), der Umgang mit personenbezogenen Daten hat, ist auf die Vertraulichkeit zu verpflichten. Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars.

Auskunftsersuchen

Zur Klärung der Zulässigkeit eines Auskunftsersuchens ist gegebenenfalls der Datenschutzbe-

auftragte hinzuzuziehen. Auskünfte an öffentliche Stellen sind in der Regel zulässig, wenn die Anfragen aufgrund einer Rechtsvorschrift erfolgen. Behörden und öffentliche Stellen müssen ihre Anfrage unter Angabe der Rechtsgrundlage (Paragraph und Gesetz) sowie der Nennung des Zwecks des Auskunftsersuchens stellen. Alle nichtroutinemäßigen Anfragen öffentlicher Stellen (z.B. der Polizei) sind, sofern sie einen datenschutzrechtlichen Bezug aufweisen, zur Prüfung an den Vorgesetzten, in Zweifelsfällen an den Datenschutzbeauftragten zu leiten.

Bei Auskunftsersuchen per E-Mail zu personenbezogenen Daten ist die Identität des Anfragenden eindeutig zu verifizieren. Bei Wunsch, die Antwort zur Auskunft elektronisch zu erhalten, ist die Empfängeradresse im Vorwege zu verifizieren und die zu übermittelnden Daten zu verschlüsseln. Eine Zustimmung des Betroffenen zu einer unverschlüsselten Übertragung ist als Option in den gesetzlichen Vorgaben nicht vorgesehen.

Auftragsverarbeitung

Werden personenbezogene Daten im Auftrag (z.B. Internet-Hoster, Gehaltsabrechnungen, o. ä.) durch andere Stellen ("Auftragverarbeiter") erhoben, verarbeitet oder genutzt, verbleibt gemäß gesetzlicher Vorschriften die datenschutzrechtliche Verantwortung beim Auftraggeber.

Als Beispiele für Varianten der Auftragsverarbeitung lassen sich unterscheiden:

- externe Datenhaltung (Auslagerung eines Rechenzentrums),
- Fernwartung von Hard- und Software,
- Archivierungsservice (manuell und elektronisch)
- Werbung, Telefonmarketing, Papier-/Aktenvernichtung.

Bei der Auftragsverarbeitung schreibt der Auftraggeber die technischen und organisatorischen Maßnahmen zur Datensicherung und zur Gewährleistung der Vertraulichkeit beim Auftragsverarbeiter vor. Dem Auftragsverarbeiter wird nur die tatsächliche Verarbeitung oder Nutzung nach Weisung und unter materieller Verantwortung des Auftraggebers übertragen. Bei der Auftragsverarbeitung wird damit lediglich eine "Hilfsfunktion" der eigentlichen Aufgabe ausgelagert. Der Auftraggeber hat sich demzufolge auch von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz zu überzeugen.

Der Datenschutzbeauftragte ist von dem verantwortlichen bzw. beauftragenden Bereich vor der Vergabe des Auftrages bei der Vertragsgestaltung hinzuzuziehen, um bei der Festlegung der datenschutzrelevanten Anforderungen bei der Vertragsgestaltung mitzuwirken. Das Gesetz schreibt Kontrollen bzgl. Einhaltung der datenschutzrechtlichen Vorschriften bei den Auf-

tragsverarbeitern vor.

Datenportabilität

Für bestimmte Verarbeitungen zu denen betroffene Personen (Mietglied oder Beschäftigter) Daten im Rahmen einer Einwilligung, Vertrages oder Vertragsanbahnung zur Verfügung gestellt hat, besteht das Recht der betroffenen Personen, diese Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln.

Die betroffenen Prozesse werden im Rahmen der Verarbeitungstätigkeit ermittelt. Der zuständige Fachbereich muss ggf. mit dem technischen Betreuer oder Hersteller die Möglichkeit der Datenportatbilität sicherstellen (gesetzliche Anforderung und Forderung der Privacy by Design).

Löschen von Daten

Der Zeitraum in dem personenbezogene Daten zu bestimmten Zwecken rechtmäßig verarbeitet werden endet, sobald die Verarbeitung nicht mehr erforderlich ist. Ab diesem Punkt müssen die Daten gelöscht werden, es sei denn gesetzliche oder vertragliche **Aufbewahrungsfristen** stehen einer Löschung entgegen. Während der Aufbewahrungsfrist müssen die Datenbestände gesperrt werden, da nur noch ein eingeschränkter Zugriff auf die Daten erforderlich ist. Neben gesetzlichen Aufbewahrungsfristen aus steuerlichen, handelsrechtlichen oder sonstigen Gründen können auch selbst definierte Aufbewahrungsfristen im Rahmen einer Interessenabwägung als Rechtsgrundlage für die weitere Speicherung in Frage kommen. Löschkonzepte müssen für die Systeme in den Prozessen nachvollziehbare Anforderungen enthalten, weil sie nur dann als Grundlage für die Löschung geeignet sind. Dazu sind die Kategorien personenbezogener Daten einer Standardlöschfristzuzuordnen, die gesetzliche oder empfohlene Grundlage der Frist exakt zu benennen und der Startzeitpunkt anzugeben.

Beispiel-Regelsatz

- **Kategorie personenbezogener Daten:** Kundenvertragsdaten
  - **Startzeitpunkt:** Ab Ende Vorgang
    - **Standardlöschfrist:** 10 Jahre
      - **Gesetzl. Grundlage oder Herleitung:** HGB § 257 Abs. 4

Zu den Löschregeln ist die Art der Umsetzung im technischen Bereich zu dokumentieren (au-

tomatisch, halbautomatisch oder manuell). Ggf. sind Funktionen oder Routinen der Systeme zu benennen. Der Zeitpunkt der Durchführung ist klar zu beschreiben (z. B. im ersten Quartal des Folgejahres, im Dezember des Kalenderjahres), die verantwortlich durchführende Person ist aufzuführen (z. B. IT-Anwendungsverantwortlicher, fachliche Systembetreuung). Ebenso müssen Angaben zur Dokumentation oder Nachvollziehbarkeit der durchgeführten Löschung dokumentiert werden.

Privacy by Design / Privacy by Default

Verarbeitungen, Verfahren und Prozesse müssen den gesetzlichen Anforderungen für Privacy by Design („Datenschutz durch Technik“) und Privacy by Default („Datenschutz durch datenschutzfreundliche Voreinstellungen“) gerecht werden. Neben Möglichkeiten der Pseudonymisierung ist auch die Anonymisierung eine mögliche Maßnahme, um den Geboten des Datenschutzes durch Technikgestaltung (Privacy by Design) zu genügen. Ferner ist die Nutzerauthentifizierung (Berechtigungskonzepte) sinnvoll, die technische Umsetzung des Widerspruchsrechts (Transparenzpflichten) sowie die Erfüllung der Anforderung an das zeitgerechte Löschen von personenbezogenen Daten. Ferner sind Maßnahmen zur technischen Sicherheit nach dem Stand der Technik zu treffen.

Datenschutzfreundliche Grundeinstellungen (Privacy by Default) müssen zum Standard werden und beinhalten eine einfache Sprache und Bedienbarkeit von Datenschutzerklärungen und –menüs, genaue und verständliche Aufklärung über die Verwendung von Daten und die Datennutzung oder Datenweitergabe, die nicht zwingend für den Zweck notwendig ist, nur nach expliziter Zustimmung der betroffenen Person. Die verantwortlichen Bereiche haben beim Design (Eigenentwicklungen) oder der Beschaffung zwingend auf die Anforderungen zu achten und ggf. ist die Beratung des Datenschutzbeauftragten im Vorfeld bereits in Anspruch zu nehmen.

Meldepflicht bei Datenpannen

Im Falle eines Abhandenkommens von Daten oder der unberechtigten Kenntnisnahme von Daten durch Dritte, kann es zu meldepflichtigen Vorfällen gegenüber der Datenschutzaufsichtsbehörde kommen. In diesen Fällen ist die Vorgehensweise und Angaben aus dem „Notfallhandbuch – Datenpanne“ anzuwenden.

Eine unzulässige Veröffentlichung von Mitglieder- und Mitarbeiterdaten führt in der Regel zu Imageverlusten. Die materiellen und immateriellen Schäden, die durch ungenügenden Datenschutz entstehen, können nur geschätzt werden.

Datenschutzvorfälle sind gem. den gesetzlichen Anforderungen innerhalb von 72 Stunden der zuständigen Datenschutzaufsichtsbehörde zu melden.

Werden gesetzliche Auflagen zum Datenschutz, wie die Benachrichtigung der Betroffenen und vorgeschriebene Meldungen an die Aufsichtsbehörde nicht oder nicht rechtzeitig erfüllt, so drohen weitere Strafen.

Darüber hinaus kann ein Verstoß gegen datenschutzrechtliche Vorschriften zudem zu Schadensersatzverpflichtungen führen und unabhängig davon auch arbeitsrechtliche Konsequenzen für einzelne Mitarbeiter haben.

Profiling / Scoring

Das Profiling[1] und Scoring (z. B. Ermittlung eines Wertes auf Basis einer statistischen Analyse, der z. B. die Bonität, Leistungsfähigkeit, Risiken einer Person repräsentiert) von Personen unterliegt hohen Anforderungen (ggf. Einwilligung, Widerrufsmöglichkeit, Informationspflichten, Offenlegung der verwendeten Daten). Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Wenn das Scoring oder Profiling für den Abschluss eines Vertrages oder der Erfüllung eines Vertrages erforderlich ist, kann eine Zulässigkeit der Anwendung vorliegen. Gleiches gilt, wenn eine entsprechende Rechtsvorschrift oder Einwilligung vorliegt, die die automatisierte Entscheidung rechtfertigt. Im Rahmen der Informationspflichten ist die betroffene Person transparent über diese Vorgehensweise zu informieren. Außerdem ist in der Regel eine Datenschutzfolgenabschätzung durchzuführen.

Beschäftigtendatenschutz

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach 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 (Kollektivvereinbarung) ergeben-

[1] „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Das Scoring ist ein Spezialfall des Profiling.

den Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Werbung / Marketing

Sofern ein Mietglied nicht widersprochen hat, ist die Briefwerbung in Form der Eigenwerbung, für eigene Produkte im Zusammenhang mit der Mietgliedschaft, zulässig.

Die Werbeansprache Mietgliedern per Telefon ist nur zulässig, wenn eine ausdrückliche Einwilligung vorliegt. Hierbei muss das Mitglied darauf hingewiesen werden, dass er der Verwendung jederzeit widersprechen kann.

Die Werbeansprache Mietgliedern per E-Mail/Fax ist nur zulässig, wenn eine vorherige ausdrückliche Einwilligung vorliegt. Ausnahmsweise kann die Werbeansprache zulässig sein, wenn

a) wenn der Verein im Zusammenhang mit der Mitgliedschaft von dem Mitglied dessen elektronische Postadresse erhalten hat,

b) das Mitglied der Verwendung nicht widersprochen hat und

c) das Mitglied bei der Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann.

Für die werbliche Ansprache sind die Vorschriften aus den Datenschutzgesetzen, den Vorgaben zum unlauteren Wettbewerb (UWG) und zukünftig aus der ePrivacy-Verordnung zu beachten.

Online-Angebote

Für Online-Angebote (Webseiten, Newsletter, Formulare, usw.) sind ebenfalls die Datenschutzvorgaben, die Vorgaben zum unlauteren Wettbewerb (UWG) zu beachten und die ePrivacy-Verordnung zu beachten (Impressum auf den Webseiten, Datenschutzerklärung, Cookie-Einwilligungen, usw.).

Für die Nutzung von Tracking-Informationen (Cookies, Tracking, Trageting) im Online-Bereich ist die Nutzung auf eine explizite Einwilligung zu stützen und mit den entsprechenden Informationspflichten zu versehen.

Schulungen und Fortbildungen

Bei allen technischen Vorkehrungen zur Datensicherheit ist und bleibt der Mensch der entscheidende Faktor. Das Datenschutzbewusstsein eines jeden Mitarbeiters ist von grundlegender Bedeutung für den ordnungsgemäßen und sicheren Umgang mit den uns anvertrauten Daten. Jeder Mitarbeiter hat sich deshalb mit den Vorschriften zum Datenschutz (Informationsblätter) vertraut zu machen.

Aufsichtsbehörde

Die zuständige Datenschutzaufsichtsbehörde steht dem Datenschutzbeauftragten ggf. zur Beantwortung und Klärung strittiger Sachverhalte zur Verfügung. Ebenso obliegt es der Aufsichtsbehörde Kontrollen auf Einhaltung der Vorschriften jederzeit bei dem Verein vorzunehmen.

Anfragen und Informationen an die Datenschutzaufsichtsbehörde sind grundsätzlich über den Datenschutzbeauftragten zu führen.

Jedes Mitglied und Beschäftigter hat jederzeit das Recht sich zu Klärungen oder Beschwerden auch persönlich an die Datenschutzaufsichtsbehörde zu wenden.

Controlling / Rechenschaftspflichten

Der Verein hat gem. den gesetzlichen Bestimmungen über die Einhaltung der Vorschriften umfänglich Rechenschaft abzulegen. Durch die nachzuhaltenden dokumentierten Kontrollen der verantwortlichen Bereiche und der dokumentierten Prüfung auf Wirksamkeit durch den Datenschutzbeauftragten wird der Nachweis der Rechenschaftspflicht ermöglicht.

Schwachstellen bei den Kontrollen oder der Wirksamkeit sind mit Maßnahmen und Umsetzungsterminen zur Minderung der Risiken zu definieren. Regelmäßige risikoorientierte Audits gewährleisten die jeweils aktuelle Einschätzung der datenschutzrelevanten Risikolage für den Verein.

6 Verbandsspezifische Anforderungen

6.1 *Nutzung von Mitgliederdaten*

Innerhalb eines Vereins sind die Aufgaben in der Regel abgegrenzt und bestimmten Funktionsträgern zugewiesen. Wer für was zuständig ist, wird durch die Satzung oder die Geschäftsordnung bestimmt. Für den Umgang mit Mitgliederdaten gilt, dass jeder Funktionsträger nur die für die Erfüllung seiner Aufgaben erforderlichen Mitgliederdaten kennen, verarbeiten oder nutzen darf. So darf etwa der Vorstand auf alle Mitgliederdaten zugreifen, wenn er diese zur Aufgabenerledigung benötigt. Auch müssen der Vereinsgeschäftsstelle alle Mitgliederdaten regelmäßig für die Mitgliederverwaltung und -betreuung zur Verfügung stehen, während es in der Regel für den Kassierer genügt, wenn er die für den Einzug der Mitgliedsbeiträge relevanten Angaben (Name, Anschrift und Bankverbindung) kennt. Dabei dürfen die Daten grundsätzlich nur zur Verfolgung des Vereinszwecks bzw. zur Betreuung und Verwaltung von Mitgliedern genutzt werden (Art. 6 Abs. 1 lit. b) DS-GVO). Nur ausnahmsweise ist es möglich, diese Daten für sonstige berechtige Interessen des Vereins oder Dritter zu nutzen, vorausgesetzt, dem stehen keine schutzwürdigen Interessen der Vereinsmitglieder entgegen (Art. 6 Abs. 1 lit. f) DS-GVO).

6.2 *Nutzung von Daten Dritter*

Daten Dritter, etwa von Lieferanten, Besuchern oder Aushilfsspielern anderer Vereine, dürfen gespeichert und genutzt werden, wenn dies für die Begründung oder Durchführung eines rechtsgeschäftlichen Schuldverhältnisses (Vertrag) mit diesen Personen erforderlich ist (Art. 6 Abs. 1 lit. b) DS-GVO) oder der Verein ein berechtigtes Interesse daran hat und nicht erkennbar ist, dass dem schutzwürdigen Interessen der Betroffenen entgegenstehen (Art. 6 Abs. 1 lit. f) DS-GVO, s. o. Nr. 2.1). Diese Daten dürfen grundsätzlich nur zu dem Zweck verwendet werden, zu dem sie der Verein erhoben oder erhalten hat. Lediglich dann, wenn eine Weiterverarbeitung der Daten mit dem Zweck der ursprünglichen Datenerhebung als vereinbar anzusehen ist, ist eine Zweckänderung zulässig (Art. 6 Abs. 4 DS-GVO). Denn ein Vertragspartner darf sich in der Regel darauf verlassen, dass der Verein seine Daten nur im Rahmen des Vertragsverhältnisses nutzt.

6.3 *Nutzung der Daten des Vereins für Spendenaufrufe und Werbung*

Vereine haben regelmäßig ein erhebliches Interesse an der Mitglieder- und Spendenwerbung,

um einen ausreichenden Mitgliederbestand und genügend finanzielle Mittel sicherzustellen. Die Daten seiner Vereinsmitglieder darf der Verein nur für Spendenaufrufe und für Werbung zur Erreichung der eigenen Ziele des Vereins nutzen (Art. 6 Abs. 1 lit. b) DS-GVO). Die Nutzung von Mitgliederdaten für die Werbung Dritter ist ohne Einwilligung der Mitglieder (s. o. Nr. 1.3.4) grundsätzlich nicht zulässig.

Daten Dritter, die dem Verein bekannt sind, etwa von Personen, die regelmäßig Eintrittskarten für Spiele beziehen, darf der Verein für Werbezwecke nutzen, wenn diese entweder darin eingewilligt haben (s.o. Nr. 1.3.4) oder der Verein berechtigte Interessen an der Nutzung zu Werbezwecken hat und keine Interessen oder Grundrechte des Dritten überwiegen (Art. 6 Abs. 1 lit. f) DS-GVO). Einzubeziehen in diese Interessenabwägung sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen (Erwägungsgrund 47 DS-GVO).

Die vernünftigen Erwartungen werden bei werblichen Ansprachen maßgebend durch die Informationen nach Art. 13, 14 DS-GVO zu den Zwecken der Datenverarbeitung bestimmt (s.o. Nr. 1.3.2). Informiert der Verein daher transparent und umfassend über eine vorgesehene Nutzung der Daten, geht die Erwartung der betroffenen Person in aller Regel auch dahin, dass ihre Daten entsprechend genutzt werden. Zu beachten ist jedoch, dass die von der Werbung betroffene Person ein jederzeitiges Widerspruchsrecht hat (Art. 21 Abs. 2 DS-GVO), auf das der Verein ausdrücklich hinzuweisen hat (Art. 21 Abs. 4 DS-GVO). Ein solcher Widerspruch hat zur Folge, dass die personenbezogenen Daten für Werbezwecke nicht mehr verwendet werden dürfen (Art. 21 Abs. 3 DS-GVO). Widerspricht der Adressat der Nutzung seiner Daten für Werbezwecke gegenüber dem Verein, ist dies zu respektieren. Telefonische Werbung bei Dritten ist ohne ausdrückliche Einwilligung des Betroffenen nicht zulässig, ebenso wenig in der Regel E-Mail-Werbung.

Der Verein kann auch eine Firma beauftragen, mit Hilfe der Daten, die ihr der Verein im Rahmen einer Auftragsdatenverarbeitung zugänglich macht, solche Werbemaßnahmen durchzuführen (s. o. Nr. 3.2). Dabei ist die eingeschaltete Firma zu verpflichten, sowohl die vom Verein überlassenen, als auch die bei der Werbeaktion erhobenen Daten nicht für eigene Zwecke - insbesondere für Werbeaktionen für Dritte – zu nutzen und sämtliche Daten nach Abschluss der Aktion vollständig an den Verein abzuliefern.

6.4 *Verarbeitung personenbezogener Daten durch den Verein*

Übermittlung an Dritte

Zur Datenübermittlung gehört jede Art von Veröffentlichung personenbezogener Angaben, z.B. in einer Tageszeitung oder im Internet. Nach Art. 6 Abs. 1 lit. b) DS-GVO können die Daten von Mitgliedern weitergegeben werden, wenn dies zur Erreichung des Vereinszwecks, insbesondere zur Verwaltung und Betreuung der Mitglieder erforderlich ist. Darüber hinaus darf der Verein die Daten seiner Mitglieder und anderer Personen auch zu einem anderen Zweck als zu dem, zu dem sie erhoben worden sind, übermitteln, wenn der Verein oder der Empfänger daran ein berechtigtes Interesse hat und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (Art. 6 Abs. 1 lit. f) DS-GVO, s.o. Nr. 2.1).

Datenübermittlung an Vereinsmitglieder

Bei den Vereinsmitgliedern handelt es sich im Verhältnis zum Verein um Dritte. Vereinsmitglieder dürfen also nicht einfach auf die Daten der anderen Mitglieder Zugriff nehmen, sei es, dass an sie Mitgliederlisten ausgegeben werden, sei es, dass die Personalien aller Mitglieder im Vereinsheim oder an einer anderen Stelle ausgehängt oder so in das Internet eingestellt werden, dass die anderen Mitglieder die Daten unter Verwendung eines Passworts abrufen können. Vielmehr müssen die rechtlichen Voraussetzungen für die Zulässigkeit einer Übermittlung vorliegen.

Besteht der Vereinszweck darin, die persönlichen oder geschäftlichen Kontakte zu pflegen, ist die Herausgabe einer Mitgliederliste zur Erreichung des Vereinsziels nach Art. 6 Abs. 1 lit. b) DS-GVO zulässig. Dieser Vereinszweck muss sich aus der Satzung ergeben. Dies kann insbesondere bei Selbsthilfe- und Ehemaligenvereinen der Fall sein. Welche Angaben dabei in die Mitgliederliste aufgenommen werden dürfen, hängt vom jeweiligen Vereinszweck ab, wobei die Interessen und die schutzwürdigen Belange der Mitglieder angemessen zu berücksichtigen sind (s. o. Nr. 2.1). Der Verein muss dabei sicherstellen, dass die Mitglieder, die ihre schutzwürdigen Interessen durch die Herausgabe der Mitgliederliste beeinträchtigt sehen, die Möglichkeit haben, der Aufnahme ihrer Daten in diese zu widersprechen. Die Daten in der Mitgliederliste sollten sich möglichst auf die zur Kontaktaufnahme notwendigen Angaben beschränken. Bei der Herausgabe der Mitgliederliste ist darauf hinzuweisen, dass diese nur für Vereinszwecke verwendet werden darf und eine Verwendung für andere Zwecke (insbesondere für kommerzielle Zwecke) sowie die Überlassung der Liste an außenstehende Dritte nicht zulässig ist. Ein solcher Hinweis soll verhindern, dass beispielsweise Vereinsmitglieder oder außenstehende Dritte

die Liste für ihre beruflichen oder politischen Zwecke nutzen.

Dient die Datenübermittlung an andere Vereinsmitglieder nicht der Förderung des Vereinszwecks, können personenbezogene Daten der Vereinsmitglieder durch den Verein an andere Vereinsmitglieder nur übermittelt werden, wenn der Verein oder der Empfänger ein berechtigtes Interesse daran hat. Dabei hat die Übermittlung zu unterbleiben, wenn erkennbar ist, dass Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (Art. 6 Abs. 1 lit. f) DS-GVO; s.o. Nr. 2.1). Es darf nicht verkannt werden, dass Vereinsmitglieder sich grundsätzlich darauf verlassen dürfen, dass der Verein ihre Daten ausschließlich für die Förderung der Vereinszwecke und zu Verwaltung und Betreuung der Mitglieder nutzt.

Bekanntgabe zur Wahrnehmung satzungsmäßiger Mitgliederrechte

Regelungen in Vereinssatzungen sehen vielfach vor, dass beispielsweise Anträge auf Einberufung einer außerordentlichen Mitgliederversammlung oder auf Ergänzung der Tagesordnung der Mitgliederversammlung davon abhängig gemacht werden, dass eine bestimmte Mindestzahl von Mitgliedern die Einberufung bzw. Ergänzung verlangt. Wenn der Verein nicht generell eine Mitgliederliste oder ein Mitgliederverzeichnis herausgibt (vgl. dazu Nr. 5.1), kann es erforderlich sein, dass er Mitgliedern beispielsweise durch Einsicht in diese Unterlagen oder durch Überlassung einer Adressliste ermöglicht, eine ausreichende Anzahl anderer Mitglieder für die Unterstützung eines solchen Antrags zu erreichen.

Die Bekanntgabe von Mitgliederdaten für diesen Zweck ist wegen der Pflicht des Vereins, die Ausübung satzungsmäßiger Rechte zu ermöglichen, regelmäßig im Vereinsinteresse erforderlich, ohne dass Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (Art. 6 Abs. 1 lit. f) DS-GVO). Um Missbräuchen entgegenzuwirken, empfiehlt es sich, von den Mitgliedern, denen die Adressen bekannt gegeben werden, eine Zusicherung zu verlangen, dass die Adressen nicht für andere Zwecke verwendet werden. Bei Vereinen, bei denen ein Interesse der Mitglieder besteht, dass ihre Daten vertraulich behandelt werden oder bei denen die Zugehörigkeit zum Verein ein besonders sensitives Datum darstellt (z.B. Parteien, Gewerkschaften, Selbsthilfegruppen), können jedoch Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person dem Interesse einer Bekanntgabe ihres Namens und ihrer Anschrift überwiegen. In solchen Fällen sollte der Verein eine Regelung in der Satzung treffen oder die Mitglieder ausreichend informieren, ohne ihre Daten bekannt zu geben. Dies kann etwa dadurch geschehen, dass in einer Vereinspublikation auf den beabsichtigten Antrag, die Gründe und den Antragsteller hingewiesen und auf diese Weise interessierten Mitgliedern die

Möglichkeit der Kontaktaufnahme zur Unterstützung eröffnet wird.

Mitteilungen in Aushängen und Vereinspublikationen

In vielen Vereinen ist es üblich, personenbezogene Informationen an einem „Schwarzen Brett“ oder in Vereinsblättern bekannt zu geben. Obwohl sich das „Schwarze Brett“ meist auf dem Vereinsgelände befindet und das „Vereinsnachrichtenblatt“ in erster Linie für Vereinsmitglieder bestimmt ist, handelt es sich hier um die Übermittlung dieser Angaben an einen nicht überschaubaren Kreis von Adressaten, die davon Kenntnis nehmen können, weil nie ausgeschlossen werden kann, dass auch Fremde die Anschlagtafeln auf dem Vereinsgelände oder das Mitteilungsblatt lesen. Personenbezogene Daten dürfen dabei nach Art. 6 Abs. 1 lit. b) und lit. f) DS-GVO nur offenbart werden, wenn es für die Erreichung des Vereinszwecks unbedingt erforderlich ist - was etwa bei Mannschaftsaufstellungen oder Spielergebnissen angenommen werden kann - oder wenn der Verein oder die Personen, die davon Kenntnis nehmen können, ein berechtigtes Interesse an der Veröffentlichung haben und Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Letzteres ist stets bei Mitteilungen mit ehrenrührigem Inhalt der Fall, etwa bei Hausverboten, Vereinsstrafen und Spielersperren.

Insbesondere die Veröffentlichung von Sportgerichtsurteilen in vollem Wortlaut würde die Betroffenen unnötig an den Pranger stellen und damit deren schutzwürdige Belange beeinträchtigen. In diesen Fällen genügt es nämlich, wenn der Betroffene und die Funktionsträger des Vereins oder die von ihm Beauftragten (z.B. Schiedsrichter) davon wissen. Doch müssen letztere dabei nicht über die Höhe der verhängten Geldbuße, die Art des Verstoßes, über die Verfahrenskosten sowie über die Urteilsbegründung im Einzelnen unterrichtet werden. Soll das Urteil zur Warnung anderer Sportler oder sonstiger Mitglieder eines Vereins veröffentlicht werden, genügt hierfür eine Veröffentlichung in anonymisierter Form.

Persönliche Nachrichten mit einem Bezug zum Verein wie Eintritte, Austritte, Spenden, Geburtstage und Jubiläen können veröffentlicht werden, wenn dem Verein keine schutzwürdigen Belange des Betroffenen bekannt sind, die dem entgegenstehen. Es empfiehlt sich, beim Eintritt in den Verein darauf aufmerksam zu machen, welche Ereignisse üblicherweise am „Schwarzen Brett“ oder im Vereinsblatt veröffentlicht werden und darum zu bitten, mitzuteilen, wenn dies nicht gewünscht wird. Informationen aus dem persönlichen Lebensbereich eines Vereinsmitglieds (z.B. Eheschließungen, Geburt von Kindern, Abschluss von Schul- und Berufsausbildungen) dürfen nur veröffentlicht werden, wenn das Mitglieder ausdrücklich sein Einverständnis erklärt hat (s. o. Nr. 1.3.4). Vergleichbares gilt für die Bekanntgabe der Höhe der Spende eines

Vereinsmitgliedes. Spender und Sponsoren außerhalb des Vereins dürfen nur mit ihrem Einverständnis öffentlich bekannt gegeben werden, da ihr Interesse an vertraulicher Behandlung grundsätzlich überwiegt.

Die „dienstlichen“ Erreichbarkeitsdaten von Funktionsträgern des Vereins, insbesondere der Vorstände, können in der Regel in der genannten Form bekannt gegeben werden. Dagegen dürfen Mitgliederlisten für gewöhnlich nur am „Schwarzen Brett“ ausgehängt oder im Vereinsblatt veröffentlicht werden, wenn die Betroffenen insoweit eingewilligt haben (s. o. Nr. 1.3.4).

Datenübermittlung an Dachverbände und andere Vereine

Dachverbände, bei denen ein Verein Mitglied ist, sind im Verhältnis zu seinen Mitgliedern datenschutzrechtlich Dritte. Personenbezogene Daten der eigenen Mitglieder dürfen an andere Vereine im Rahmen der Erforderlichkeit nur übermittelt werden, soweit diese dort benötigt werden, um die Vereinsziele des übermittelnden Vereins oder um die Ziele des anderen Vereins zu verwirklichen, etwa bei der überregionalen Organisation eines Turniers, und sofern keine Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (Art. 6 Abs. 1 lit. b) und lit f) DS-GVO; s. o. Nr. 2.1).

Ist ein Verein verpflichtet, die Daten seiner Mitglieder regelmäßig einer Dachorganisation - beispielsweise einem Bundes- oder Landesverband - zu übermitteln (etwa in Form von Mitgliederlisten), sollte dies in der Vereinssatzung geregelt werden.

Dadurch wird klargestellt, dass die Übermittlung im Vereinsinteresse erforderlich ist und keine Interessen oder Grundrechte und Grundfreiheiten der Vereinsmitglieder überwiegen (Art. 6 Abs. 1 lit. f) DS-GVO). Fehlt eine Satzungsregelung, sollten die Mitglieder (Neumitglieder möglichst bereits im Aufnahmeverfahren) über die Übermittlung ihrer Daten an die Dachorganisation und den Übermittlungszweck informiert und ihnen Gelegenheit zu Einwendungen gegeben werden. Der Verein ist darüber hinaus verpflichtet, dafür Sorge zu tragen, dass die von ihm weitergegebenen Mitgliederdaten vom Dritten nicht zweckentfremdet genutzt werden (etwa durch Verkauf der Mitgliederadressen für Werbezwecke) oder dies allenfalls mit Einverständnis des Vereins und Einwilligung der betroffenen Mitglieder geschieht.

Sollen Mitgliederlisten oder im Einzelfall sonstige Mitgliederdaten auf freiwilliger Basis ohne vertragliche oder sonstige Verpflichtung an Dachverbände oder andere Vereine weitergegeben werden, ist dies nur unter den oben genannten Voraussetzungen zulässig. Soweit die Weitergabe im berechtigten Interesse des Vereins oder des Empfängers erfolgen soll, empfiehlt es

sich in Zweifelsfällen, die Mitglieder vor der beabsichtigten Datenübermittlung zu informieren und ihnen die Möglichkeit zu geben, Einwendungen gegen die Weitergabe ihrer Daten geltend zu machen.

Bietet der Dachverband eine Versicherung für die Mitglieder eines Vereins an, die in erster Linie dem Verein dient, um sich gegen Haftungsansprüche seiner Mitglieder zu schützen, wenn diese beim Sport oder bei vergleichbar gefahrgeneigten Tätigkeiten verunglücken, hat der Verein ein berechtigtes Interesse, die für die Begründung des Versicherungsverhältnisses erforderlichen Daten seiner Mitglieder dem Dachverband zuzuleiten, es sei denn, das Mitglied hat ein überwiegendes schutzwürdiges Interesse, dass dies unterbleibt, wenn es etwa selbst bereits gegen dieses Risiko versichert ist. Will aber der Dachverband nur erreichen, dass sich die Vereinsmitglieder in eigenem Interesse bei ihm oder bei einer von ihm vermittelten Versicherung versichern können, darf der Verein deren Daten nur mit ihrer Einwilligung (s. o. Nr. 1.3.4) an den Dachverband übermitteln.

Andererseits ist es zulässig, dass ein Verein, der eine bestimmte Anzahl Delegierter zur Delegiertenversammlung des Dachverbandes entsenden darf, dem Dachverband eine Namensliste seiner Mitglieder übermittelt, damit dieser feststellen kann, ob die entsandten Delegierten auch Mitglieder eines Vereins sind, der Delegierte entsenden darf. Es muss stets durch entsprechende Vereinbarungen mit dem Dachverband sichergestellt sein, dass die ihm zugänglich gemachten Daten dort für keinen anderen Zweck genutzt werden, also nicht etwa für Werbemaßnahmen des Dachverbandes oder gar Dritter.

Datenübermittlung an Sponsoren und Firmen zu Werbezwecken

Nicht selten verlangen Sponsoren als Gegenleistung für ihre Unterstützung die Bekanntgabe von Mitgliederdaten, die dann zu Werbezwecken eingesetzt werden. Aber auch für manche Wirtschaftsunternehmen sind die Daten von Vereinsmitgliedern für Werbezwecke interessant. Die Bekanntgabe von Mitgliederdaten für Werbezwecke ist aber in der Regel vom Vereinszweck nicht gedeckt. Sofern also die Bekanntgabe von Mitgliederdaten an Sponsoren und Wirtschaftsunternehmen für Werbezwecke weder in der Satzung noch durch Mitgliederbeschluss festgelegt ist, sollten die Vereine bei der Übermittlung von Mitgliederdaten an Sponsoren und Wirtschaftsunternehmen zu Werbezwecken grundsätzlich zurückhaltend verfahren. Bei einer Mitgliedschaft in einem Verein handelt es sich um ein personenrechtliches Rechtsverhältnis, aus dem sich für den Verein besondere Rücksichtnahmepflichten in Bezug auf die schutzwürdigen Belange seiner Mitglieder ergeben, die je nach Art des Vereins unterschiedlich stark sind.

Insbesondere Mitglieder örtlicher Vereine vertrauen regelmäßig darauf, dass der Verein ihre Daten grundsätzlich nicht für vereinsfremde Zwecke verwendet. Bei größeren Vereinen hingegen - wie z.B. einem Automobilclub - kann eine andere Situation gegeben sein.

Der Verein darf personenbezogene Daten der Mitglieder für Werbezwecke daher nur übermitteln, wenn diese entweder darin eingewilligt haben oder der Verein oder ein Dritter berechtigte Interessen an der Nutzung zu Werbezwecken hat und keine Interessen oder Grundrechte und Grundfreiheiten der Mitglieder überwiegen. Entscheiden sind auch hier die vernünftigen Erwartungen der betroffenen Person. Informiert der Verein transparent und umfassend über eine entsprechende werbliche Nutzung, geht die Erwartung der betroffenen Person in aller Regel auch dahin, dass ihre Daten entsprechend genutzt werden (vgl. insoweit die Ausführungen oben unter Nr. 4.3) Zu beachten ist auch hier, dass das Mitglied ein jederzeitiges Widerspruchsrecht hat, auf das der Verein ausdrücklich hinweisen muss. Dies kann beispielsweise dadurch geschehen, dass in den Aufnahmeantrag oder in die Satzung ein entsprechender Hinweis aufgenommen wird. Es ist darüber hinaus empfehlenswert, im Rahmen der Jahreshauptversammlung nochmals auf das Widerspruchsrecht hinzuweisen. Erfolgt ein solcher Widerspruch, hat dies zur Folge, dass die personenbezogenen Daten für Werbezwecke nicht mehr verwendet werden dürfen (Art. 21 Abs. 3 DS-GVO). Die Namen der Vereinsmitglieder, die der Übermittlung ihrer Daten für Werbezwecke widersprochen haben, sind in eine separate sogenannte Sperrdatei aufzunehmen. Vor jeder Übermittlung der Mitgliederdaten an Sponsoren und Wirtschaftsunternehmen zu Werbezwecken ist dann ein Abgleich mit der Sperrdatei durchzuführen.

Soweit Vereine ihren Mitgliedern gegenüber zur Rücksichtnahme verpflichtet sind, dürfen Mitgliederdaten nur mit Einwilligung der betroffenen Mitglieder an Sponsoren oder Wirtschaftsunternehmen (z.B. Versicherungen, Banken, Zeitschriftenverlage) übermittelt werden. Dies gilt in besonderem Maße, wenn es sich um besonders schutzbedürftige Daten i.S. des Art. 9 DS-GVO handelt (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheitsdaten etc.). Oft ergibt sich das Geheimhaltungsinteresse der Mitglieder schon aus dem Vereinszweck, so beispielsweise bei einer Suchtkranken-Selbsthilfegruppe oder einer Elterninitiative verhaltensgestörter Kinder. Darüber hinaus kann sich die besondere Sensibilität und damit die erhöhte Schutzwürdigkeit der Daten auch aus der Vereinsmitgliedschaft ergeben, wenn sich daraus Rückschlüsse z.B. auf die rassische oder ethnische Herkunft oder Gesundheitsdaten ziehen lassen.

Bei der Weitergabe der Mitgliederdaten muss jedoch auch der Umstand berücksichtigt werden, dass der Datenempfänger diese Daten wiederum für Werbezwecke anderer Unternehmen weitergeben oder nutzen kann. Deshalb sollte die Verwendung der weitergegebenen Daten unbedingt auf den konkreten Werbezweck des Datenempfängers beschränkt und eine Nutzung oder Übermittlung der Daten für fremde Werbezwecke vertraglich ausgeschlossen werden. Daten von Mitgliedern, bei denen ein entgegenstehendes Interesse erkennbar ist, dürfen auf keinen Fall weitergegeben werden.

In der Praxis ergeben sich bei Vereinen häufig Probleme mit der Weitergabe von Mitgliederdaten an Versicherungsunternehmen oder Versicherungsvertreter im Rahmen von Gruppenversicherungsverträgen. Dabei handelt es sich um Rahmenverträge zwischen Vereinen und Versicherungsunternehmen, die den Vereinsmitgliedern unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen.

Die Datenschutzaufsichtsbehörden vertreten hierzu inzwischen die Auffassung, dass ein Verein im Rahmen eines Gruppenversicherungsvertrags dem Versicherungsunternehmen bzw. dem Versicherungsvertreter die Daten seiner Mitglieder nur übermitteln darf, wenn das betreffende Mitglied eine ausdrückliche und informierte schriftliche Einwilligung erteilt hat. Dies gilt für Neu- und für Altmitglieder, die bei Abschluss des Gruppenversicherungsvertrags bereits Vereinsmitglieder waren, gleichermaßen. Die Einwilligungserklärung sollte zweckmäßigerweise bereits in der Beitrittserklärung oder im Aufnahmeantrag vorgesehen werden, wobei das Mitglied darüber aufzuklären ist, welche Daten an welches Unternehmen weitergegeben werden sollen.

Einzelne Versicherungen haben für Vereine eine „Stellungnahme zur Zulässigkeit von Datenübermittlungen“ oder ähnlich betiteltes Papier erarbeitet, in dem geringere Anforderungen an den Datenschutz genannt werden. Vereine sollten sich hiervon nicht irritieren lassen und der Rechtsauffassung der Datenschutzaufsichtsbehörden folgen. Dies empfiehlt sich auch im Hinblick auf die künftig im Raum stehenden Bußgelder.

Veröffentlichungen im Internet

Das Internet bietet für Vereine und Verbände große Chancen zur Selbstdarstellung, birgt aber auch Risiken für die betroffenen Vereinsmitglieder. Die Veröffentlichung von personenbezogenen Daten im Internet ohne Passwortschutz stellt datenschutzrechtlich eine Übermittlung dieser Daten an Jedermann dar. Sie ist nicht zuletzt wegen der weltweiten Verbreitung der Informationen, weil dieses Medium nichts mehr vergisst, wegen der elektronischen Recherchierbarkeit

und weil die Möglichkeit der Auswertung von Internetinformationen für Zwecke der Profilbildung und Werbung besteht, grundsätzlich nicht unproblematisch. So besitzt die Information, dass jemand z.B. eine bestimmte Sportart ausübt, einer bestimmten Altersgruppe zuzurechnen ist oder ein unfallträchtiges Hobby hat, u.U. auch für andere Stellen Relevanz (Arbeitgeber, Werbeindustrie). Auch können diese Daten in Staaten abgerufen werden, die keine der DS-GVO vergleichbare Schutzbestimmungen kennen. Ferner ist die Authentizität der Daten nicht garantiert, da diese einfach verfälscht werden können. Deswegen ist die Veröffentlichung personenbezogener Daten durch einen Verein im Internet grundsätzlich unzulässig, wenn sich der Betroffene nicht ausdrücklich damit einverstanden erklärt hat (s. o. Nr. 1.3.4).

Allerdings gibt es auch hier Ausnahmen. So dürfen die Funktionsträger eines Vereins auch ohne ausdrückliche Einwilligung mit ihrer „dienstlichen“ Erreichbarkeit in das Internet auf der Homepage des Vereins eingestellt werden. Die private Adresse des Funktionsträgers darf allerdings nur mit seinem Einverständnis veröffentlicht werden (s. o. Nr. 1.3.4).

Informationen über Vereinsmitglieder (z.B. Spielergebnisse und persönliche Leistungen, Mannschaftsaufstellungen, Ranglisten, Torschützen usw.) oder Dritte (z.B. Spielergebnisse externer Teilnehmer an einem Wettkampf) können ausnahmsweise auch ohne Einwilligung kurzzeitig ins Internet eingestellt werden, wenn die Betroffenen darüber informiert sind und keine schutzwürdigen Interessen oder Grundrechte und Grundfreiheiten der Veröffentlichung im Einzelfall überwiegen. Rechtsgrundlage hierfür ist Art. 6 Abs. 1 lit. f) DS-GVO. Die zulässige Dauer der Veröffentlichung hängt von der Bedeutung des Ereignisses, auf das sich die Veröffentlichung bezieht, und dem daraus abzuleitenden Informationsinteresse der Öffentlichkeit ab.

Die von einem Verein oder Verband ausgerichteten Veranstaltungen (z. B. Spiele in der Bezirksklasse) sind öffentlich. Die Namen und die Ergebnisse werden im Rahmen solcher Veranstaltungen üblicherweise öffentlich bekannt gegeben. Die in Ranglisten enthaltenen Daten sind zwar nicht allgemein zugänglich, stammen jedoch aus allgemein zugänglichen Quellen und stellen nur eine Zusammenfassung und Auswertung dieser Daten dar.

Um den Eingriff in das Persönlichkeitsrecht in Grenzen zu halten, dürfen bei derartigen Veröffentlichungen jedoch allenfalls Nachname, Vorname, Vereinszugehörigkeit und eventuell in begründeten Ausnahmefällen der Geburtsjahrgang aufgeführt werden. Bei einer Veröffentlichung eines Fotos, des vollen Geburtsdatums (Tag, Monat und Jahr), der privaten Anschrift oder der Bankverbindung des Betroffenen überwiegen dessen Interessen oder Grundrechts oder Grundfreiheiten berechtigte Vereins oder Verbandes; sie wäre daher nur mit ausdrücklicher Einwilli-

gung der Betroffenen zulässig. Im Übrigen muss - wie oben aufgeführt - sichergestellt sein, dass die Daten nach angemessener Zeit gelöscht werden.

Veröffentlichungen im Intranet

Wenn ein Verein seinen Mitgliedern und Funktionsträgern Informationen über das Internet in passwortgeschützten Bereichen (Intranet) zur Verfügung stellt, können über die Vergabe von Benutzerkennungen und Passwörtern individuelle Zugriffsberechtigungen eingerichtet werden. Dies hat den Vorteil, dass beliebige Dritte die Daten nicht einsehen können, berechtigte Nutzer jedoch jederzeit über das Internet auf diejenigen personenbezogenen Daten zugreifen können, die sie zur Wahrnehmung ihrer Rechte und Pflichten als Mitglied oder Funktionsträger des Vereins benötigen (s. o. Nr. 4.1 und 5.1)

Personenbezogene Auskünfte an die Presse und sonstige Massenmedien

Veröffentlichungen in Verbandszeitschriften und in sonstigen allgemein zugänglichen Publikationen dürfen genauso wie Pressemitteilungen und -auskünfte nur in personenbezogener Form erfolgen, wenn es sich um ein Ereignis von öffentlichem Interesse handelt. Dabei ist darauf zu achten, dass die schutzwürdigen Belange der betroffenen Vereinsmitglieder gewahrt werden (s. o. Nr. 2.1). Ausschlaggebend ist, ob die Veranstaltung, über die berichtet werden soll, öffentlich ist oder war, was der Betroffene gegenüber der Presse selbst erklärt hat und was die Presse ihrerseits in Erfahrung bringen konnte. Personenbezogene Daten können dabei u.U. offenbart werden, wenn es um besondere Leistungen eines Mitglieds geht oder wenn der Verein wegen des Ausschlusses eines Mitglieds in der Öffentlichkeit ins Gerede gekommen ist und eine Information im Interesse des Vereins oder der Öffentlichkeit erforderlich erscheint. Stets darf der Verein dabei nur die unbedingt notwendigen persönlichen Angaben offenbaren. Auskünfte zum privaten, nicht vereinsbezogenen Bereich eines Vereinsmitglieds sollten ohne Einwilligung (s. o. Nr. 1.3.4) grundsätzlich nicht erfolgen. Hier überragt das schutzwürdige Interesse des Betroffenen stets das Informationsinteresse der Allgemeinheit.

Übermittlung für Zwecke der Wahlwerbung

Die Übermittlung von Mitgliederdaten an politische Parteien bzw. Gruppierungen oder an Kandidaten bei Wahlen für Zwecke der Wahlwerbung ist ohne schriftliche Einwilligung der Betroffenen (s. o. Nr. 1.3.4) unzulässig. Mitglieder des Vereinsvorstands, andere Personen, die im Verein eine Funktion haben, oder Vereinsmitglieder dürfen für Zwecke der eigenen Wahlwerbung nicht auf personenbezogene Daten der Mitglieder des Vereins zurückgreifen. Diese Daten wurden für die Verfolgung des Vereinszwecks (der Vereinszwecke) erhoben und gespeichert. Eine

Nutzung für jede Art von Wahlwerbung verletzt schutzwürdige Belange der Mitglieder und ist deswegen unzulässig.

Übermittlung von Mitgliederdaten an die Gemeindeverwaltung

Verlangt eine Gemeindeverwaltung, die an einen Verein freiwillige finanzielle Leistungen erbringt, deren Höhe von der Mitgliederzahl oder der Anzahl bestimmter Mitglieder (etwa der Anzahl der Jugendlichen, die in Mannschaften mitspielen) abhängt, zu Kontrollzwecken die Vorlage von Listen mit den Namen der Betroffenen, ist der Verein grundsätzlich berechtigt, diese Daten zu übermitteln, weil es sowohl zur Wahrnehmung berechtigter eigener Interessen - nämlich um in den Genuss der Vereinsförderung durch die Gemeinde zu kommen - als auch zur Wahrnehmung berechtigter Interessen eines Dritten - der Gemeinde - erforderlich ist und Interessen oder Grundrechte der betroffenen Vereinsmitglieder einer Datenübermittlung nach Art. 6 Abs. 1 lit. f) DS-GVO nicht überwiegen. Der Verein kann sich darauf verlassen, dass die Gemeinde diese Daten nur verwendet, um nachzuprüfen, ob die ihr vom Verein übermittelten Zahlen zutreffend sind und die Daten umgehend wieder löscht.

Datenübermittlung an den Arbeitgeber eines Mitglieds und an die Versicherung

Krankenversicherungen sind grundsätzlich berechtigt zu erfahren, gegen wen und in welchem Umfang ihnen ein Regressanspruch wegen der Verletzung einer Person, an die sie deswegen Leistungen erbracht haben, durch ein Vereinsmitglied zusteht.

Für die gesetzlichen Krankenversicherungen ergibt sich dies aus § 67a des Zehnten Buchs des Sozialgesetzbuchs, für die privaten Krankenversicherer aus Art. 6 Abs. 1 lit. b) DSGVO wegen des Versicherungsvertrags zwischen dem Geschädigten und seiner Versicherung. Der Verein darf diese Anfragen grundsätzlich nach Art. 6 Abs. 1 lit f) DS-GVO beantworten. Dabei wird es allerdings genügen, der Versicherung nur den Namen des Schädigers mitzuteilen, damit sie sich an diesen wenden kann. Sollte dies nicht ausreichen, können auch weitere Angaben, etwa über den Spielverlauf, erfolgen. Um auch hier die schutzwürdigen Belange des Betroffenen angemessen berücksichtigen zu können (s. o. Nr. 2.1), sollte dieser vor der Übermittlung der Daten angehört werden. Vergleichbares gilt, wenn ein Arbeitgeber eines Vereinsmitglieds beim Verein in Erfahrung bringen will, ob sein Arbeitnehmer an einer Vereinsveranstaltung teilgenommen hat, obwohl dieser krankheitsbedingt nicht zur Arbeit erschienen ist.

6.5 *Recht auf Löschung und Einschränkung personenbezogener Daten*

Das Recht auf Löschung richtet sich nach Art. 17 Abs. 1 DS-GVO. Danach sind personenbezo-

gene Daten unverzüglich zu löschen, sofern sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, die betroffene Person ihre Einwilligung widerruft oder Widerspruch gegen die Verarbeitung einlegt, die personenbezogenen Daten unrechtmäßig verarbeitet wurden oder wenn die Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

Bezüglich des Zwecks muss der Verein daher festlegen, welche Arten von Daten bis zu welchem Ereignis (z.B. Austritt aus dem Verein, Tod) oder für welche Dauer verarbeitet werden. Mit Erreichen des festgelegten Zeitpunkts muss eine Einschränkung der Verarbeitung erfolgen, sofern die betroffene Person sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt und eine Einschränkung verlangt (Art. 18 Abs. 1 lit c) DS-GVO; sog. Protokolldatei). Ansonsten sind sie mit Zweckerreichung zu löschen. Die Länge der Einschränkung der Verarbeitung orientiert sich grundsätzlich daran, wie lange mit Rückfragen des Betroffenen, mit Gerichtsverfahren oder mit sonstigen Vorgängen zu rechnen ist, die die Kenntnis des Datums noch erforderlich machen. Auch die Länge der Dokumentationsfristen sollte für jede Datenart vorgegeben werden. Eingeschränkte Daten dürfen ohne Einwilligung des Betroffenen (s. o. Nr. 1.3.3) nur noch verarbeitet werden, wenn Rechtsansprüche durch den Verantwortlichen geltend gemacht, ausgeübt oder verteidigt werden, wenn Rechte einer anderen natürlichen oder juristischen Person geschützt werden sollen oder wenn dies aus Gründen eines wichtigen öffentlichen Interesses der Union oder des Mitgliedsstaates geschieht (Art. 18 Abs. 2 DS-GVO).

Der Verein hat die Möglichkeit, ein Vereinsarchiv zu führen und dort auch Vorgänge mit personenbezogenen Daten, die für eine aktive Nutzung nicht mehr benötigt werden, aufzubewahren. Dabei sollte jedoch sichergestellt sein, dass nur ein sehr kleiner zuverlässiger Personenkreis dazu Zugang hat. Die Nutzung des Archivguts in personenbezogener Form ist nur sehr eingeschränkt zulässig. Die Einzelheiten sollten ebenfalls geregelt werden. Wichtig ist auch, dass der Verein Unterlagen, die nicht mehr benötigt werden, so entsorgt, dass Dritte keine Kenntnis von den darin enthaltenen personenbezogenen Daten erlangen können. Insbesondere dürfen Mitgliederund Spenderlisten nicht unzerkleinert in Müllcontainer geworfen werden.

Beim Ausscheiden oder dem Wechsel von Funktionsträgern ist sicherzustellen, dass sämtliche Mitgliederdaten entweder ordnungsgemäß gelöscht oder an den Nachfolger oder einen anderen Funktionsträger des Vereins übergeben werden und keine Kopien und Dateien mit Mitgliederdaten beim bisherigen Funktionsträger verbleiben. Auch hierzu sollte der Verein Regelungen treffen.

Die erforderlichen Regelungen zu Speicherfristen sowie zur Sperrung und Löschung von Daten und ggfs. zur Nutzung von Archivgut können entweder in der Vereinssatzung oder außerhalb der Satzung in einer Datenschutzordnung bzw. in einer gesonderten Datenlöschkonzeption getroffen werden.

Organisatorisches

6.6 *Benennung eines Datenschutzbeauftragten*

Der Verein hat einen Datenschutzbeauftragen zu benennen, wenn dessen Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person erforderlich macht (z.B. Videoüberwachung im Stadion) oder die Kerntätigkeit in der Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DS-GVO (z.B. Gesundheitsdaten in Selbsthilfegruppen) oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO besteht (Art. 37 Abs. 1 lit. b) und lit c) DS-GVO). Die Verarbeitung personenbezogener Daten als primärer Geschäftszweck dürfte jedoch bei Vereinen in der Regel nicht der Fall sein.

Darüber hinaus ist ein Datenschutzbeauftragter zu benennen, wenn mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Nimmt der Verein Verarbeitungen vor, die einer Datenschutzfolgeabschätzung gemäß Art. 35 DS-GVO (s.u. Nr. 7.2) unterliegen, so ist ebenfalls ein Datenschutzbeauftragter zu benennen (§ 38 Abs. 1 BDSG-neu).

Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt.

Zur Vermeidung einer Interessenkollision dürfen die Aufgaben des Datenschutzbeauftragten nicht vom Vereinsvorstand oder dem für die Datenverarbeitung des Vereins Verantwortlichen wahrgenommen werden, da diese Personen sich nicht selbst wirksam überwachen können. Der Datenschutzbeauftragte muss nicht Mitglied des Vereins sein (Art. 37 Abs. 6 DS-GVO).

Die Aufgaben des Datenschutzbeauftragten sind in Art. 39 DS-GVO geregelt. Insbesondere obliegt dem Datenschutzbeauftragten die Pflicht, den Verein bzw. die dort mit der Verarbeitung personenbezogener Daten Beschäftigten hinsichtlich ihrer datenschutzrechtlichen Pflichten zu unterrichten und zu beraten. Zudem wirkt er auf die Überwachung und Einhaltung datenschutz-

rechtlicher Vorschriften hin. Er hat insbesondere die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen.

Zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten.

Der Verein hat die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und die Daten der zuständigen Aufsichtsbehörde mitzuteilen. Für die Veröffentlichung der Kontaktdaten ist es ausreichend, wenn die E-Mail-Adresse des Datenschutzbeauftragten auf der Vereinshomepage frei zugänglich genannt wird.

Besteht keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten, muss sich der Vereinsvorstand selbst um die Einhaltung des Datenschutzes durch den Verein kümmern. Er kann auch auf freiwilliger Basis einen Datenschutzbeauftragten bestellen.

6.7 *Datenschutz-Folgeabschätzung*

Der Verein hat nur dann eine 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 (Art. 35 Abs. 1 DS-GVO). Dies insbesondere dann der Fall, wenn eine umfangreiche Verarbeitung besonderer Kategorie von Daten gemäß Art. 9 DS-GVO erfolgt oder wenn im Wege der Verarbeitung auf Grundlage von personenbezogenen Daten systematische und umfassende Bewertungen persönlicher Aspekte vorgenommen werden, die als Grundlage für Entscheidungen dienen, die Rechtswirkungen gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen (Art. 35 Abs. 3 DS-GVO).

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 des Massnahmen zur Risikoreduzierung zu enthalten (Art. 37 Abs. 7 DS-GVO). Eine Datenschutzfolgeabschätzung dürfte aber bei Vereinen nur in den seltensten Fällen notwendig sein.

7 Referenzen

7.1 *Gesetzliche Basis*

- EU-Datenschutzgrundverordnung (ab 25. Mai 2018)
- Bundesdatenschutzgesetz-Neu (BDSG, ab 25. Mai 2018)

7.2 *Sonstige Referenzen*

- Die DIN 66398 ist die "Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten".
- Datenschutz im Verein nach der Datenschutzgrundverordnung (DS-GVO) Informationen über die datenschutzrechtlichen Rahmenbedingungen beim Umgang mit personenbezogenen Daten in der Vereinsarbeit – Landesbeauftragte für Datenschutz Baden-Württemberg