

Datenschutz im Schützenverein

Stand: Mai 2006

Inhaltsverzeichnis

1. Einführung

2. Rechtsgrundlagen und Grundsätze des Datenschutzes

Rechtsgrundlagen
Datenschutzgrundsätze

3. Datenverarbeitung für eigene Zwecke des Vereins

Datenverarbeitung für satzungsgemäße Zwecke des Vereins
Nutzung für sonstige berechnigte Interessen des Vereins

4. Beispiele für eine Offenbarung bzw. Übermittlung von Daten innerhalb des Vereins

Vereinsinterne Aushänge
Bekanntgabe von Daten zur Wahrnehmung satzungsmäßiger Mitgliederrechte
Sonstige Offenbarung von Daten an Vereinsmitglieder, Mitgliederlisten

5. Datenverarbeitung für sonstige Zwecke

6. Beispiele für die Übermittlung von Daten an Dritte außerhalb des Vereins

Übermittlung an Dachorganisationen und Verbände
Veröffentlichung von Spenderdaten
Gruppenversicherungsverträge
Übermittlungen an die Presse

7. Werbung

Werbeveranstaltungen
Telefon-, Fax- und E-Mailwerbung
Übermittlung an Sponsoren und Wirtschaftsunternehmen
Personenbezogene Daten für Mitglieder- und Spendenwerbung
Werbung durch Vereinsmitglieder
Werbung mit zugekauften Adressen
Werbung durch professionelle Werbefirmen
Wahlwerbung

8. Veröffentlichung im Internet und E-Mailverkehr

Veröffentlichung von Wettkampfergebnissen, Mannschaftsaufstellungen und Ranglisten
Veröffentlichung von Daten über Verbands- und Vereinsfunktionäre
Veröffentlichung von Urteilen der Vereinsgerichtsbarkeit
Veröffentlichung von Daten über Minderjährige
E-Mailverkehr

9. Löschung von personenbezogenen Daten**10. Datenverarbeitung im Auftrag****11. Datenschutzgrundsätze und Regelungen für die Datenverarbeitung im Verein****12. Verpflichtung auf das Datengeheimnis****13. Bestellung eines Datenschutzbeauftragten****14. Technische und organisatorische Maßnahmen****15. Bußgeld und Schadensersatz****16. Zusätzliche Informationen zum Datenschutz und zur Datensicherheit****Anlagen**

Einwilligung für eine Veröffentlichung personenbezogener Daten im Internet

Verpflichtung auf das Datengeheimnis

Datenschutzverpflichtung über Datenverarbeitung im Auftrag

Merkblatt Technische und organisatorische Maßnahmen im Schützenverein

Datenschutzgrundsätze und Regelungen für die Datenverarbeitung im Verein

Datenschutzregelung in der Vereinssatzung

Datenschutzhinweis in der Beitrittserklärung

Einwilligungserklärung der Erziehungsberechtigten zur Internetpräsentation auf der Vereinshomepage

1. Einführung

Schützenvereine verarbeiten im Zusammenhang mit der Vereinsführung und der Mitgliederverwaltung personenbezogene Daten über ihre Mitglieder, ggf. auch über Sponsoren und Förderer. Daneben fallen im Zusammenhang mit dem Vereins- und Sportbetrieb weitere personenbezogene Daten an. Diese Verarbeitung fällt, weil personenbezogene Daten verarbeitet werden, unter den Geltungsbereich des Bundesdatenschutzgesetzes (BDSG) und ist nur insoweit zulässig, als das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder die Vereinsmitglieder eingewilligt haben.

Personenbezogene Daten sind alle Daten, die sich auf eine natürliche Person, hier regelmäßig auf ein Vereinsmitglied, beziehen oder beziehen lassen. Dazu gehören z.B. Name, Anschrift, Geburtsdatum, Aufnahme datum in den Verein, Bankverbindung u.s.w. Hinzu kommen dann Daten aus dem Sportbetrieb, wie Ergebnisse und Platzierungen bei Meisterschaften, Teilnehmerlisten, Informationen über absolvierte Lehrgänge (Sportlehrgänge, Jugend-, Fachübungs- und Schießleiterlehrgänge u.a.), Informationen über ehrenamtliche Tätigkeiten oder über den Besitz von Sportwaffen.

Unter Datenverarbeitung versteht das Bundesdatenschutzgesetz die Erhebung, Speicherung, Verarbeitung, Nutzung und Übermittlung von Daten unabhängig davon, ob die Verarbeitung in automatisierten Verfahren, z.B. auf PCs, oder in nicht automatisierten Verfahren, z.B. mit Karteikarten, stattfindet. Auch Listen oder Tabellen, z.B. aus Text- oder Tabellenkalkulationssystemen, gehören dazu. Unerheblich ist dabei auch, ob der Verein in das Vereinsregister eingetragen ist oder ob es sich um einen nicht eingetragenen Verein handelt.

Die personenbezogenen Daten über die Vereinsmitglieder sind z.B. für die Werbung von großem Interesse. Um diese Daten über die Vereinsmitglieder vor einer unbefugten oder missbräuchlichen Nutzung zu schützen, sind bei der Erhebung, Speicherung, Verarbeitung, Nutzung und Übermittlung die Regelungen des Datenschutzes zu beachten.

2. Rechtsgrundlagen und Grundsätze des Datenschutzes

Rechtsgrundlagen

Der Datenschutz für nichtöffentliche Unternehmen, dazu gehören auch die Vereine, ist im Bundesdatenschutzgesetz (BDSG) geregelt. Nach den Vorschriften dieses Gesetzes ist die Erhebung, Speicherung, Verarbeitung, Nutzung und Übermittlung personenbezogener Daten zulässig, wenn das BDSG oder eine andere Rechtsvorschrift diese erlaubt oder der Betroffene eingewilligt hat (Verbot mit Erlaubnisvorbehalt).

Grundsätzlich erlaubt das Bundesdatenschutzgesetz eine Erhebung, Verarbeitung, Nutzung und Übermittlung von personenbezogenen Daten,

- wenn es der Zweckbestimmung eines Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses dient oder
- soweit es zur Wahrung der berechtigten Interessen des Vereins erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt oder
- wenn die Daten allgemein zugänglich sind oder der Verein sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse der Betroffenen am Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse des Vereins offensichtlich überwiegt.

Das Mitgliedschaftsverhältnis zu einem Schützenverein stellt ein vertragsähnliches Vertrauensverhältnis dar. Zulässig ist in diesem Rahmen jede Erhebung, Speicherung, Verarbeitung, Nutzung oder Offenbarung personenbezogener Daten, soweit es zur Erfüllung der in der Satzung festgelegten Vereinszwecke erforderlich ist, z.B. Name, Anschrift, Geburtsdatum, Eintrittsdatum, Sportdaten. Über diesen unbedingt erforderlichen Bestand an personenbezogenen Daten hinaus dürfen unter dem Gesichtspunkt der Wahrung berechtigter Interessen des Vereins weitere Daten gespeichert werden, die im Rahmen des Vereinszwecks liegen und die geeignet sind, diesen zu fördern (z.B. über bestimmte Qualifikationen wie Jugendleiterausbildung etc.)¹⁾. Mit Einwilligung dürfen darüber hinaus weitere Daten gespeichert werden, z.B. Bankdaten für den Beitragseinzug. Dies gilt auch für Personen, die einen Aufnahmeantrag gestellt haben, aber noch nicht aufgenommen sind. In diesem Rahmen dürfen vor der Aufnahme in den Verein die zur Abwicklung des Aufnahmeverfahrens und der Begründung der Mitgliedschaft erforderlichen Daten erhoben und gespeichert werden.

Datenschutzgrundsätze

Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind folgende Grundsätze zu beachten:

- Es dürfen nur die personenbezogenen Daten erhoben, verarbeitet und genutzt werden, die für die Erfüllung der Vereinszwecke erforderlich sind (Grundsatz der Datenvermeidung und Datensparsamkeit).
- Personenbezogene Daten dürfen nur vom Mitglied erhoben werden.
- Die Mitglieder müssen über die Tatsache der Datenspeicherung und über die Zwecke der Verarbeitung unterrichtet werden.

¹⁾ 1. Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz Sachsen-Anhalt 2001-2003 S. 24 ff.

- Werden Daten an andere Stellen übermittelt, müssen die Betroffenen über die Art der zu übermittelnden Daten und den Zweck der Übermittlung und über die Empfänger der Daten unterrichtet werden (dazu gehört auch die Übermittlung der Daten an den Bezirk im Rahmen der Mitgliedermeldung).
- Werden Daten erhoben, die für die Verfolgung der Vereinszwecke nicht unbedingt erforderlich sind und damit der Freiwilligkeit unterliegen, ist der Betroffene über den Zweck der Verarbeitung, auf die Freiwilligkeit seiner Angaben und auf sein jederzeitiges Widerrufsrecht zu unterrichten.
- Sollen Daten erstmals ohne Wissen des Betroffenen an Dritte übermittelt werden, ist er über diese Übermittlung zu unterrichten, falls erforderlich, ist die Einwilligung der Betroffenen einzuholen.
- Personenbezogene Daten dürfen nur solange gespeichert und verarbeitet werden, wie dies für die Vereinszwecke erforderlich ist.

Diese Benachrichtigungs- und Informationspflichten sollen die Betroffenen in die Lage versetzen, ihr Selbstbestimmungsrecht über ihre Daten und ihre Rechte nach dem Datenschutzgesetz, insbesondere das Recht auf Auskunft, Berichtigung und Löschung, auszuüben. Diese Informations- und Benachrichtigungspflichten entfallen nur dann, wenn der Betroffene bereits auf andere Weise über die Verarbeitung seiner Daten informiert ist.

Das Mitgliedschaftsverhältnis zu einem Schützenverein ist ein personenrechtliches Rechtsverhältnis und unterliegt einem besonderen Vertrauensschutz. Dieser Vertrauensschutz begründet auf Seiten des Vereins ein hohes Maß an Sorgfalt im Umgang mit den personenbezogenen Daten der Mitglieder und ist bei der Gewichtung der Schutzwürdigkeit der Interessen der Mitglieder zu berücksichtigen.

3. Datenverarbeitung für eigene Zwecke des Vereins

Datenverarbeitung für satzungsgemäße Zwecke des Vereins

Mitgliederdaten dürfen im Rahmen der Vereinsmitgliedschaft für Vereinszwecke erhoben, verarbeitet und genutzt werden. Zu diesen Verarbeitungsverfahren für eigene Zwecke des Vereins gehören insbesondere

- alle Verfahren zur Führung des Mitgliederbestandes,
- Verfahren zur Berechnung und Einziehung der Beiträge,
- Verfahren zur Abwicklung förmlicher Anwendungen wie Mitgliedermeldungen, Einladungen u.a., wenn in diesen Systemen personenbezogene Daten gespeichert werden,
- Verfahren zur Abwicklung des Sportbetriebes, wie Vereinsmeisterschaften, Jahreswertungen, Vergleichs- und Freundschaftsschießen und sonsti-

- ge sportliche Veranstaltungen sowie Meldungen zu Meisterschaften und Wettkämpfen,
- Verfahren zur Vorbereitung und Abwicklung von gesellschaftlichen und sonstigen Aktivitäten des Vereins im Zusammenhang mit der Erfüllung der Vereinszwecke oder zur allgemeinen Gestaltung des Vereinslebens.

Da diese Verarbeitungsverfahren für die Wahrnehmung der Vereinszwecke erforderlich sind bzw. den Zwecken des Vereins dienen, besteht von Seiten des Datenschutzgesetzes eine Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung der hierfür erforderlichen personenbezogenen Daten. Eine Einwilligung der Mitglieder ist deshalb nicht erforderlich, wohl aber deren Information über die Tatsache der Speicherung, Verarbeitung und Nutzung dieser Daten.

Nutzung für sonstige berechtigte Interessen des Vereins

Zur Wahrung berechtigter Interessen des Vereins dürfen über die engen Satzungszwecke hinausgehend weitere Mitgliederdaten erhoben und verarbeitet werden. Dazu gehören z.B. der Name von Inhabern von Übungsleiterlizenzen, Teilnehmer an Kursen und Schulungen, insbesondere auch von Schulungen, die der Bayerische Sportschützenbund e.V. für Schützen und Vereinsfunktionäre anbietet, aber auch Daten über Spender und Sponsoren. Die Verarbeitung und Nutzung dieser personenbezogenen Daten ist zulässig, soweit dadurch nicht überwiegende schutzwürdige Interessen der Betroffenen am Ausschluss der Verarbeitung oder Nutzung bestehen.

Neben dieser Nutzung von Daten für die Erfüllung von berechtigten Interessen des Vereins dürfen auch Daten gespeichert werden, bei denen kein unmittelbarer Sachzusammenhang mit dem Vereinszweck besteht, die aber der Vereinsarbeit dienen. Die Speicherung und Nutzung dieser Daten ist zulässig, wenn ein schutzwürdiges Interesse des Betroffenen am Ausschluss der Speicherung oder Nutzung der Daten nicht offensichtlich überwiegt, z.B. Telefon- und Faxnummer.

Die berechtigten Interessen des Vereins und die schutzwürdigen Interessen der Betroffenen sind bei der Beurteilung der Zulässigkeit der Erhebung und Nutzung dieser Daten gegeneinander abzuwägen. Auch wenn diese Abwägung zu dem Ergebnis führt, dass die Erhebung oder Nutzung der personenbezogenen Daten zulässig ist, ergibt sich daraus für den Verein kein Rechtsanspruch auf die Erhebung und Nutzung dieser Daten. Erhebt also ein Betroffener trotz grundsätzlicher Zulässigkeit Einwendungen gegen die Speicherung dieser zwar nützlichen, aber für die Verfolgung der Vereinszwecke nicht zwingend erforderlichen Daten, hat die Erhebung zu unterbleiben bzw. sind diese Daten zu löschen. Für Daten wie Beruf, Familienstand, Zahl der Kinder oder weitere Daten aus dem persönlichen Lebensbereich des Mitgliedes lässt sich i.d.R. kein be-

rechichtiges Interesse des Vereins begründen. Hier überwiegt das berechtigte schutzwürdige Interesse der Mitglieder am Schutz der Privatsphäre.

4. Beispiele für eine Offenbarung bzw. Übermittlung von Daten innerhalb des Vereins

Innerhalb der Vorstandschaft des Vereins dürfen die Funktionsträger (Vorsitzender, Kassier, Schriftführer, Sportleiter u.a.) Zugang zu allen personenbezogenen Daten besitzen, die sie zur Erfüllung ihrer Aufgaben benötigen. Personenbezogene Daten dürfen deshalb im erforderlichen Umfang gegenseitig ausgetauscht bzw. zur Verfügung gestellt werden. Im Umkehrschluss bedeutet dies aber auch, dass diejenigen personenbezogenen Daten, die für die Erfüllung der Aufgaben des jeweiligen Vorstandsmitgliedes nicht erforderlich sind, diesem auch nicht zugänglich sein dürfen. Dies trifft insbesondere auf Bankdaten im Zusammenhang mit dem Beitragseinzug zu, deren Zugang auf den Kassier begrenzt werden sollte.

Bezüglich der übrigen Vereinsmitglieder besteht eine Offenbarungsbefugnis grundsätzlich nur, wenn ein berechtigtes Auskunftsinteresse von Seiten der Mitglieder besteht und schutzwürdige Interessen der Mitglieder einer Offenbarung nicht entgegenstehen. Insbesondere bei großen Vereinen, in denen zwischen den Mitgliedern keine besondere persönliche Verbundenheit mehr besteht, ist es denkbar, dass einzelne Mitglieder ein Interesse an einer vertraulichen Behandlung ihrer Daten haben. Hier ist eine Güterabwägung zwischen dem Auskunftsinteresse des einzelnen Mitgliedes und einem möglichen schutzwürdigen Interesse der übrigen Mitglieder zu treffen. Führt diese Abwägung zu dem Ergebnis, dass eine Offenbarung zulässig ist, ist diese auf die notwendigsten Daten zu beschränken und die Empfänger sind zu verpflichten, die offenbarten personenbezogenen Daten nur für den dargelegten Zweck zu verwenden. Die folgenden Beispiele sind Tätigkeitsberichten und sonstigen Veröffentlichungen von Aufsichtsbehörden für den Datenschutz entnommen und verdeutlichen dieses Abwägungsprinzip.

Vereinsinterne Aushänge

Bei vereinsinternen Aushängen am schwarzen Brett sind je nach Art und Inhalt des Aushanges unterschiedliche Gesichtspunkte zu beachten. Informationen über Ergebnisse von offiziellen Meisterschaften, Veranstaltungen und Wettkämpfen, z.B. Gaumeisterschaften, Rundenwettkämpfen oder sonstigen öffentlichen Veranstaltungen, dürfen am schwarzen Brett ausgehängt werden. Gleiches gilt für Mannschaftsaufstellungen für Meisterschaften und Rundenwettkämpfe und für Meldungen für öffentlich zugängliche Wettbewerbe. Diese Wettkämpfe und Veranstaltungen sind öffentlich und für jedermann zugänglich. Dies ist den teilnehmenden Sportlern auch bekannt. Eine öf-

fentliche Bekanntgabe dieser Daten verletzt deshalb keine schutzwürdigen Interessen der teilnehmenden Sportler.

Eine andere Beurteilung ergibt sich bei vereinsinternen Wettbewerben wie Vereinsmeisterschaften, Ranglistenwettbewerben oder sonstigen vereinsinternen Veranstaltungen, die nicht öffentlich zugänglich bzw. als nichtöffentliche Veranstaltung organisiert sind, sowie für sonstige vereinsinterne Informationen wie z.B. Trainingspläne. Ein Aushang dieser vereinsinternen Informationen ist ohne weiteres zulässig, wenn das schwarze Brett nur Vereinsmitgliedern zugänglich ist. Wenn das Vereinsheim auch von anderen Vereinen oder von den Vereinsmitgliedern oder deren Angehörigen auch für andere Veranstaltungen genutzt wird, z.B. für private Geburtstagsfeiern u.a. und in diesem Zusammenhang auch vereinsfremde Personen Zugang zu diesen Informationen erhalten oder gar der Verein in einer Gastwirtschaft beheimatet ist und sich der Aushang in einem allgemein zugänglichen Bereich, z.B. Gastraum, befindet, sollte das Verfahren im Verein verbindlich geregelt werden. Besondere Sorgfalt ist in diesem Zusammenhang auch geboten, wenn z.B. durch den Aushang besondere persönliche Verhältnisse, z.B. eine Behinderung, offenbart werden, z.B. bei einem Aushang von Ergebnissen über Behindertenwettbewerbe. Derartige Ausgänge dürfen nicht ohne Einwilligung der betroffenen Teilnehmer vereinsfremden Personen zugänglich sein, weil Gesundheitsdaten vom Datenschutzrecht als besonders sensible Daten eingestuft werden. Grundsätzlich sollten die Ausgänge dann, wenn auch vereinsfremde Personen Kenntnis nehmen können, auf die notwendigsten Inhalte beschränkt werden. Auf die Angabe von Adressen und Geburtsdaten sollte deshalb verzichtet werden.

Der Aushang von Daten über die Vorstandschaft und sonstige Funktionäre im Verein ist zulässig, um den Mitgliedern des Vereins die Kontaktaufnahme mit diesen Personen zu ermöglichen. Grundsätzlich bestehen auch keine Bedenken dagegen, dem Aushang eine Fotografie der betroffenen Personen beizufügen.

Der Aushang von personenbezogenen Daten im Rahmen eines Aufnahmeverfahrens, insbesondere in Vereinen, in denen auch mit scharfen Waffen geschossen wird, ist zulässig. Allerdings müssen die Interessenten vorher über dieses Verfahren informiert werden. Dies gilt insbesondere dann, wenn dem Aushang ein Foto beigelegt wird.

Vorsicht ist auch bei einem Aushang von Informationen über Jubiläen, Geburtstagen oder sonstigen Mitteilungen aus dem persönlichen Lebensbereich der Mitglieder sowie von Beitritten oder Austritten aus dem Verein geboten. Dies gilt insbesondere bei passiven oder fördernden Mitgliedern und bei größeren Vereinen, in denen sich die einzelnen Mitglieder nicht näher kennen. Ein Aushang von Adressdaten oder von Daten aus dem persönlichen Lebensbereich der Mitglieder am schwarzen Brett bedarf grundsätzlich der Einwilligung der betroffenen Mitglieder.

Grundsätzlich ist auch zu berücksichtigen, an welcher Stelle sich der Aushang befindet. Handelt es sich um einen Schaukasten im Außenbereich des Vereinsheimes, bestehen keine Bedenken dagegen, dort Ergebnisse von sportlichen Veranstaltungen zu publizieren. Hier darf ausgehängt werden, was auch in der Presse veröffentlicht werden darf. Aushänge über das vereinsinterne Geschehen, z.B. im Zusammenhang mit einem Aufnahmeverfahren, dürfen dagegen nur an Stellen innerhalb des Vereinsheimes ausgehängt werden, die nicht öffentlich zugänglich sind.

Bekanntgabe von Daten zur Wahrnehmung satzungsmäßiger Mitgliederrechte

Sehen Satzung, Geschäftsordnung oder sonstige vereinsinterne Regelungen vor, dass zur Wahrnehmung von Mitgliederrechten die Beteiligung oder die Unterschrift einer bestimmten Mindestanzahl von Mitgliedern erforderlich ist, hat der Verein aufgrund seiner Pflicht, die Wahrnehmung der Mitgliederrechte zu ermöglichen, die erforderlichen Unterlagen, z.B. Mitgliederlisten, zur Verfügung zu stellen bzw. Einsicht zu gewähren. Es empfiehlt sich jedoch, die Einsicht nehmenden Personen zu verpflichten, diese Daten nicht für andere Zwecke zu verwenden. Die Einsicht ist dabei auf diejenigen Daten zu beschränken, deren Kenntnis für die Wahrung der Mitgliederrechte und zur Kontaktaufnahme erforderlich ist.

Sonstige Offenbarung von Daten an Vereinsmitglieder, Mitgliederlisten

Wünschen einzelne Vereinsmitglieder Mitgliederdaten, z.B. zur persönlichen Kontaktaufnahme für private und/oder gesellschaftliche Zwecke, zur Bildung von Fahrgemeinschaften etc., ist das berechtigte Interesse an der Kenntnis dieser Daten gegen ein eventuelles schutzwürdiges Interesse der Betroffenen Vereinsmitglieder abzuwägen. Für die Beurteilung der Zulässigkeit der Offenbarung von Daten für diese Zwecke sind die individuellen Besonderheiten, die Kultur und die Tradition des Vereins maßgeblich. In einem kleinen Verein, in dem ohnehin fast jeder jeden kennt und in dem ein gewisses Maß an persönlicher Verbundenheit besteht und die Pflege des persönlichen Kontaktes eine gewisse Tradition und Bedeutung hat, bestehen keine ernsthaften Bedenken gegen eine Offenbarung von Kontaktdaten. Handelt es sich um einen großen Verein, eventuell mit verschiedenen Sparten und Abteilungen und einer gewissen Anonymität der einzelnen Mitglieder, ist eine Offenbarung bedenklich.

Grundsätzlich dürfen nicht beliebige Daten offenbart werden, sondern nur die für eine Kontaktaufnahme erforderlichen Daten wie Name, Anschrift, Telefonnummer und ggf. E-Mailadresse sowie die Abteilung des Vereins, in der der Betroffene Mitglied ist.

Empfehlung

Zu empfehlen ist hier, zu Art, Ort Inhalt und Anlässen von Aushängen und zur Offenlegung von Mitgliederlisten einen Mitgliederbeschluss herbeizuführen. Zusätzlich sollte festgelegt werden, für welche Zwecke eine derartige Mitgliederliste verwendet werden darf. Mitglieder, die sich gegen eine vereinsinterne Offenbarung ihrer personenbezogenen Daten oder gegen eine Mitgliederliste wenden, werden dann nicht erfasst. Bei einer Neuaufnahme müssen die Interessenten über diese Regelungen unterrichtet werden.

5. Datenverarbeitung für sonstige Zwecke

Die Datenverarbeitung für sonstige Zwecke betrifft hauptsächlich die Offenbarung/Übermittlung von personenbezogenen Daten über Mitglieder an Personen oder Stellen außerhalb des Vereins, an sog. Dritte. Zu diesen Dritten können auch Mitglieder des Vereins gehören, wenn diese die personenbezogenen Daten für eigene Zwecke nutzen wollen, z.B. Sponsoren oder sonstige Förderer des Vereins.

Die Offenbarung personenbezogener Daten bzw. deren Übermittlung an Dritte ist ein besonders sensibler Vorgang. Es muss deshalb sorgfältig geprüft werden, ob durch die Übermittlung schutzwürdige Interessen der Mitglieder verletzt werden können. Kann dies nicht ausgeschlossen werden, darf die Übermittlung nicht ohne Einwilligung des Mitgliedes vorgenommen werden.

Die Übermittlung oder Nutzung von Mitgliederdaten ist zulässig, soweit sie

- zur Wahrung berechtigter Interessen eines Dritten oder
- zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder
- zur Verfolgung von Straftaten

erforderlich ist. Darüber hinaus ist eine Übermittlung unter bestimmten Voraussetzungen für Werbung, Markt- und Meinungsforschung zulässig.

Besteht für die Übermittlung der personenbezogenen Daten keine Rechtsgrundlage im o.g. Sinne, ist in jedem Fall die Einwilligung der Mitglieder erforderlich. Diese Einwilligung ist nur dann rechtswirksam, wenn sie auf einer freiwilligen Entscheidung der Mitglieder beruht und die Mitglieder vorher ausreichend und klar über die Freiwilligkeit, die Art der Daten, den Zweck der Erhebung, Verarbeitung, Nutzung oder Übermittlung der Daten, über die Empfänger und über die jederzeitige Möglichkeit der Rücknahme der Einwilligung informiert worden sind (informierte Einwilligung). Diese Einwilligung ist grundsätzlich schriftlich einzuholen und kann jederzeit für die Zukunft widerrufen werden.

6. Beispiele für eine Übermittlung von Daten an Dritte außerhalb des Vereins

Übermittlung an Dachorganisationen und Verbände

Mitgliederdaten werden im Zusammenhang mit dem Mitgliedermeldeverfahren an den Bezirk weitergegeben und dort elektronisch gespeichert und verarbeitet. Diese Übermittlung liegt im berechtigten Interesse des Vereins und des Bayerischen Sportschützenbundes e.V. und ist zur Erfüllung der Vereins- und Verbandszwecke erforderlich und deshalb datenschutzrechtlich zulässig. Trotzdem sollte für die Übermittlung eine satzungsrechtliche Grundlage geschaffen und die Mitglieder über diese Übermittlung unterrichtet werden.

Empfehlung

Die Übermittlung von Daten an den Verband sollte in der Satzung geregelt werden. Zumindest sollte in der Hauptversammlung oder in der Vereinszeitung darauf hingewiesen werden. Zur Information neuer Mitglieder ist ein entsprechender Hinweis im Aufnahmeantrag erforderlich. (siehe Anlage).

Veröffentlichung von Spenderdaten

Häufig wird Spendern öffentlich gedankt oder es wird eine Spenderliste veröffentlicht. Hier ist abzuwägen, ob auf Seiten des Vereins ein berechtigtes Interesse an der Veröffentlichung der Spender besteht und ob auf Seiten der Spender ein schutzwürdiges Interesse an der Wahrung ihrer Anonymität bestehen kann. In Zweifelsfällen muss eine Einwilligung der Spender in die Veröffentlichung dieser Daten eingeholt werden. Die Spendenhöhe darf nur mit Einwilligung der Betroffenen offen gelegt werden.

Empfehlung

Zu empfehlen ist, das beabsichtigte Veröffentlichungsverfahren im Spendenaufruf darzulegen. Erheben die Spender gegen das dargelegte Verfahren keine Einwendungen, kann davon ausgegangen werden, dass sie mit der Veröffentlichung einverstanden sind.

Gruppenversicherungsverträge

Sollen Daten im Rahmen von Gruppenversicherungsverträgen an Versicherungen offenbart werden, ist folgendes zu beachten:

Von Vereinsmitgliedern, die nach Abschluss eines Gruppenversicherungsvertrages in den Verein eintreten, muss die Einwilligung für die Weitergabe der Daten eingeholt werden. Die zu übermittelnden Datenarten müssen angegeben werden. Die Einwilligung wird am zweckmäßigsten mit der Abgabe der Bei-

trittserklärung oder des Aufnahmeantrages eingeholt. Personen, die beim Abschluss des Gruppenversicherungsvertrages bereits Mitglied des Vereins sind, müssen rechtzeitig vor der Übermittlung ihrer Daten schriftlich informiert werden. In dem Schreiben müssen die zu übermittelnden Daten angegeben werden und es muss auf die Möglichkeit eines Widerspruches gegen die Datenübermittlung und auf einen bevorstehenden Vertreterbesuch hingewiesen werden. Widerspricht das Mitglied, dürfen seine Daten nicht übermittelt werden.¹ Für den Widerspruch ist eine Frist von mindestens vier Wochen vorzusehen, damit das Widerspruchsrecht auch wahrgenommen werden kann.²

Empfehlung für einen Einwilligungstext

Der/die <Name des Vereins> hat für seine Mitglieder einen Gruppenversicherungsvertrag abgeschlossen. Um die Vergünstigungen aus dem Gruppenversicherungsvertrag wahrnehmen zu können, willige ich ein, dass hierfür mein Name, meine Anschrift und mein Geburtsjahr an der/die <Name der Versicherung> weitergegeben werden.³

Einige Versicherungen haben zu diesem Thema selbst Datenschutzinformationen verfasst und darin eine weniger strenge Rechtsauffassung vertreten. Im Streitfall kann sich ein Verein aber nur schwerlich auf derartige Aussagen berufen, denn verbindlich sind allein die Regelungen des Datenschutzgesetzes. Als Auslegungshilfen sollten nur Kommentare, Gerichtsurteile und Veröffentlichungen von Aufsichtsbehörden herangezogen werden.

Übermittlungen an die Presse

Aus Gründen des Persönlichkeitsschutzes dürfen Daten über Mitglieder nur dann an die Presse oder andere Medien weitergegeben werden, wenn dem keine schutzwürdigen Interessen der Mitglieder entgegenstehen. Regelmäßig dürfen die Ergebnisse von öffentlichen sportlichen Wettkämpfen oder besondere sportliche Leistungen veröffentlicht werden, wenn die Veröffentlichungen bereits einer ständigen Übung im Verein entsprechen, über die die Mitglieder auch informiert sind. Vorsicht ist jedoch bei Veröffentlichungen über vereinsinterne Wettbewerbe geboten oder wenn mit der Veröffentlichung zusätzliche, nicht allgemein bekannte oder sensible Informationen aus dem persönlichen Bereich der Mitglieder an die Öffentlichkeit gelangen. Dazu gehören z.B. Informationen über Behinderungen oder wenn die Ergebnisse Rückschlüsse auf den

¹⁾ Tätigkeitsbericht Nr. 1 2001/2002 der Aufsichtsbehörde für den Datenschutz Rheinland-Pfalz und Empfehlungen der Aufsichtsbehörde für den Datenschutz Baden-Württemberg

²⁾ Empfehlungen der Aufsichtsbehörde für den Datenschutz Baden-Württemberg

³⁾ Text lt. Tätigkeitsbericht Nr. 1 2001/2002 der Aufsichtsbehörde für den Datenschutz Sachsen

Besitz bestimmter Waffen zulassen. Im Zweifel sollten die betroffenen Mitglieder vorher informiert werden. Unproblematisch ist es, wenn bei Veranstaltungen Pressevertreter anwesend sind und über das Geschen berichten.

Empfehlung

Im Zweifel ist zu empfehlen, bei der Veranstaltung durch Aushang auf die beabsichtigte Veröffentlichung hinzuweisen.

Eine Offenbarung kann auch in Betracht kommen und zulässig sein, wenn im Vereinsinteresse oder in einem öffentlichen Informationsinteresse in der Öffentlichkeit Sachverhalte diskutiert oder richtig gestellt werden müssen. Dabei dürfen aber nur die unbedingt notwendigen persönlichen Angaben offen gelegt werden und es muss das schutzwürdige Interesse der betroffenen Mitglieder beachtet werden.

7. Werbung

Werbeveranstaltungen

Das Ansprechen von Personen zum Zwecke der Mitgliederwerbung ist auf Werbeveranstaltungen (Tag der offenen Tür, Schnupperschießen etc.) zulässig. Werden bei einer derartigen Veranstaltung Daten gezielt erhoben, um sie später für Werbeaktionen zu verwenden, müssen die Betroffenen über die Freiwilligkeit der Angaben und über die beabsichtigte Verwendung der Daten für Werbemaßnahmen unterrichtet werden. Dies gilt auch, wenn bei Sportveranstaltungen Daten für Werbezwecke erhoben werden sollen, z.B. über Verlosungen oder Preisausschreiben. Zulässig ist dagegen die Verteilung oder der Versand von Werbematerial an die Haushalte des Ortes bzw. der Gemeinde.

Telefon-, Fax- und E-Mailwerbung

Mitgliederwerbung per Telefon durch Entnahme von Telefonnummern aus dem Telefonbuch oder Nutzung von Daten aus anderen Quellen, z.B. aus Verlosungen, und Anrufen der Betroffenen (kaltes Telefonmarketing) im Rahmen einer Werbeaktion durch Mitglieder eines Vereins oder im Auftrag eines Vereins durch ein Call Center ist nach deutschem Wettbewerbsrecht nur zulässig, wenn eine Einverständniserklärung der betroffenen Personen eingeholt wurde. Dies gilt auch für Werbung mittels Fax oder E-Mail. Davon zu unterscheiden ist eine gelegentliche Werbung für einen Verein im Freundeskreis gelegentlich eines Gespräches. Sollen aber die gelegentlich eines Gespräches gewonnenen Adressdaten an den Verein zur gezielten Ansprache weitergegeben werden, ist auch hierfür die Einwilligung des Betroffenen erforderlich.

Übermittlung an Sponsoren und Wirtschaftsunternehmen

Sponsoren erwarten z.T. als Gegenleistung für ihre Unterstützung des Vereins die Bekanntgabe von Mitgliederdaten für Werbezwecke. Auch für Wirtschaftsunternehmen, z.B. für Versicherungen, Banken, Zeitschriftenverlage, und für politische Parteien können die Mitgliederdaten eines Vereins von Interesse sein. Das Bundesdatenschutzgesetz spricht hier von Werbung, Markt- und Meinungsforschung. Für diese Zwecke ist eine Übermittlung in listenmäßig zusammengefasster Form grundsätzlich zulässig, wenn kein Grund zur Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung oder Nutzung hat (Listengebot).

Neben der Tatsache der Zugehörigkeit zum Verein umfasst dieses sog. Listenprivileg folgende Datenarten:

- Berufs-, Branchen- oder Geschäftsbezeichnung,
- Name,
- Titel,
- Akademische Grade,
- Anschrift und
- Geburtsjahr.

Da es sich aber bei der Mitgliedschaft in einem Verein um ein personenrechtliches Rechtsverhältnis handelt, aus dem sich für den Verein besondere Rücksichtnahmepflichten im Bezug auf die schutzwürdigen Interessen seiner Mitglieder ergeben, ist bei derartigen Offenbarungen besondere Vorsicht geboten. Insbesondere Mitglieder örtlicher Vereine vertrauen darauf, dass der Verein ihre Daten grundsätzlich nicht für vereinsfremde Zwecke verwendet.

Vor einer Übermittlung der Daten an Sponsoren muss den Mitgliedern die Gelegenheit eingeräumt werden, einer Übermittlung ihrer personenbezogenen Daten zu widersprechen. Widerspricht das Mitglied, dürfen die Daten nicht übermittelt werden. Darüber hinaus muss der Empfänger der Daten schriftlich verpflichtet werden, die Daten nur für die dargelegten Zwecke, z.B. eigene Werbemaßnahme, zu verarbeiten oder zu nutzen. Insbesondere sollte er verpflichtet werden, die überlassenen Daten seinerseits nicht an andere Stellen zu übermitteln. Zulässig ist dagegen die Beifügung von Werbematerial des Sponsors zur Vereinspost oder ein Versand des Materials im Lettershopverfahren.

Empfehlung

Falls ein Verein mit Sponsoren zusammenarbeitet, empfiehlt es sich, im Verein eine Grundsatzentscheidung über das Verfahren herbeizuführen, z.B. durch eine Entscheidung der Mitgliederversammlung. Der Vorstand sollte dann alle Mitglieder darüber unterrichten und jedem einzelnen Mitglied die Möglichkeit einräumen, innerhalb einer angemessenen Frist (ca. vier Wochen) der Weitergabe der eigenen Daten zu widersprechen.

Personenbezogene Daten für Mitglieder- und Spendenwerbung

Adressen von Interessenten und Sponsoren, die diese z.B. bei Anfragen an den Verein, bei Mitgliedern oder bei Vereinsfunktionären angeben, dürfen vom Verein für die Mitglieder- und Spendenwerbung gespeichert und genutzt werden, solange dies sinnvoll ist und der Betroffene keine Verletzung seiner schutzwürdigen Interessen geltend macht bzw. nicht widerspricht.

Werbung durch Vereinsmitglieder

Werben Vereinsmitglieder in ihrem Freundes- und Bekanntenkreis für den Verein oder beschaffen sie Adressen für eine Mitglieder- und Spendenwerbung, ist eine Weitergabe dieser Adressen an den Verein nur nach vorheriger Information der Betroffenen und deren Einverständniserklärung zulässig. Sollen die Betroffenen angerufen oder zuhause besucht werden, müssen sie bei der Einholung der Einverständniserklärung auch hierüber informiert werden.

Werbung mit zugekauften Adressen

Beschafft ein Verein Adressen von Adresshändlern, um damit Mitgliederwerbung zu betreiben, ist dies bei Beschränkung der Daten auf das Listengebot zulässig. Die Betroffenen müssen bei der Ansprache zur Werbung darüber informiert werden, dass sie weiteren Werbemaßnahmen widersprechen können.

Werbung durch professionelle Werbefirmen

Große Vereine beauftragen auch Werbebüros mit Mitglieder- und Spendenwerbung. Dies ist eine Datenverarbeitung im Auftrag und erfordert den Abschluss eines schriftlichen Vertrages. Der Verein bleibt hier für die Einhaltung des Datenschutzes verantwortlich. In dem Vertrag sind Art und Umfang des Auftrages konkret festzulegen. Insbesondere muss die Werbefirma verpflichtet werden, die vom Verein überlassenen Daten nur für die beauftragte Werbe- oder Spendenaktion und nicht auch für andere Zwecke oder Werbemaßnahmen zu verwenden und nach Abschluss der Aktion sämtliche Daten vollständig an den Verein herauszugeben bzw. zu löschen. Wichtig ist auch, Vorkehrungen zu treffen, dass bei der Haustürwerbung kein unangemessener Druck ausgeübt wird, z.B. durch Offenbarung von Spenden der Nachbarn, weil dadurch deren schutzwürdige Interessen verletzt werden. Der Verein muss die Werbefirma nach der besonderen Eignung der bei ihr eingerichteten technischen und organisatorischen Maßnahmen zum Datenschutz sorgfältig auswählen und hat auch die Verpflichtung, diese in angemessener Weise zu überprüfen.

Wahlwerbung

Eine Weitergabe von Mitgliederdaten für Wahlwerbung an politische Parteien oder Gruppen oder an deren Kandidaten ist nur mit Einwilligung der betroffenen Mitglieder zulässig. Die Unterstützung einer Wahlwerbung ist von den Vereinszwecken nicht abgedeckt. Zum anderen ergibt sich ein besonderes schutzwürdiges Interesse der Mitglieder aus den besonderen Schutzpflichten des Vereins auf der Grundlage des personenrechtlichen Rechtsverhältnisses.¹

8. Veröffentlichung im Internet und E-Mailverkehr

Das Internet bietet dem Verein vielfältige Möglichkeiten der Selbstdarstellung und der Öffentlichkeitsarbeit. Allerdings bestehen aufgrund der allgemeinen und weltweiten Zugänglichkeit auch Risiken für die betroffenen Vereinsmitglieder. Die Daten sind im Internet länger veröffentlicht als in der Presse und sind für die Werbewirtschaft auswertbar. Durch die einfache und schnellere Zugriffsmöglichkeit besteht eine größere Missbrauchsgefahr, z.B. in Form von Datenabgleichen durch die Werbewirtschaft oder Profilbildungen.¹ Es sollte deshalb sorgfältig geprüft werden, ob die Veröffentlichung personenbezogener Daten im Internet für die verfolgten Vereinszwecke tatsächlich erforderlich ist und welche Informationen über die Mitglieder veröffentlicht werden sollen.

Wenn im Internet personenbezogene Daten veröffentlicht werden sollen, ist eine vorherige schriftliche Einwilligung der Mitglieder erforderlich. Bei neu eingetretenen Mitgliedern empfiehlt es sich, bereits bei der Datenerhebung für die Mitgliedschaft die Einwilligung einzuholen. Dabei ist darauf zu achten, dass den Betroffenen klar ist, welche Daten zur Veröffentlichung bestimmt sind und dass sie deren Umfang beschränken können. Ebenso ist auf die Freiwilligkeit der Einwilligung und auf ihre jederzeitige Widerrufsmöglichkeit hinzuweisen. Bei Altmitgliedern bietet es sich an, über die Vereinsmitteilungen eine allgemeine Information, die die genannten Punkte berücksichtigt, mit einer zurückzusendenden Zustimmungserklärung zu verteilen.²

Empfehlung

Die Einwilligungserklärung muss über die Internetrisiken informieren, die zu veröffentlichenden Daten enthalten und über die Freiwilligkeit unterrichten. Es empfiehlt sich, den von Seiten der Aufsichtsbehörden für den Datenschutz hierfür zur Verfügung gestellten Mustertext zu verwenden (siehe Anlage).³

¹) Tätigkeitsbericht Nr. 1 der Aufsichtsbehörde für den Datenschutz Bayern

²) 16. Datenschutzbericht des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen

³) Merkblatt des Innenministeriums Baden-Württemberg, „Datenschutz im Verein“, Datenschutz im Verein, Informationen zum Datenschutz: Der Landesbeauftragte für den Datenschutz Bremen, Der Hamburgische Datenschutzbeauftragte, Der Landesbeauftragte für den Datenschutz Niedersachsen, Der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Unabhängiges Landeszentrum für den Datenschutz Schleswig-Holstein

Diese Einwilligung ist eine grundsätzliche Willenserklärung und wirkt für alle in der Zukunft vorgesehenen Veröffentlichungen. Weitere Veröffentlichungen haben aber zu unterbleiben, wenn der Betroffene zu einem späteren Zeitpunkt seine Einwilligung zurücknimmt.

Veröffentlichung von öffentlichen Wettkampfergebnissen, Mannschaftsaufstellungen und Ranglisten

Eine Veröffentlichung mit Name, Disziplin, Klasse/Liga und Platzierung ist zulässig. Ein schutzwürdiges Interesse der Betroffenen am Ausschluss der Veröffentlichung ist in der Regel nicht ersichtlich, weil die Wettkämpfe selbst öffentlich sind und damit auch die Daten öffentlich zugänglich sind bzw. aus öffentlich zugänglichen Quellen stammen. Die Öffentlichkeit ist den Sportlern bekannt. Eine Beeinträchtigung der Sportler durch die Internet-Veröffentlichung ist nicht anzunehmen. Die Veröffentlichung ist aber auf Sportart/Disziplin, Name, Vorname und Altersgruppe zu beschränken.¹ Wichtig ist auch, die Dauer der Veröffentlichung auf den aktuellen Zeitraum zu begrenzen und die Informationen wieder rechtzeitig zu löschen. Weitere Daten wie Anschrift und Geburtsdatum dürfen nicht ohne Einwilligung der Betroffenen veröffentlicht werden.²

Empfehlung

Bei kleineren Meisterschaften oder Wettkämpfen, die zwar auch öffentlich zugänglich sind, aber bei denen die Teilnehmer nicht unbedingt damit rechnen, dass die Ergebnisse mit Personenbezug im Internet veröffentlicht werden sollen, ist eine Information der Teilnehmer durch Aushang am Veranstaltungsort zu empfehlen.

Veröffentlichung von Daten über Verbands- und Vereinsfunktionäre

Um die Aufnahme von Kontakten zum Schützenverein zu ermöglichen bzw. zu erleichtern, werden häufig Daten über Vereinsfunktionäre im Internet veröffentlicht. Diese Praxis ist ohne Einwilligung zulässig, weil von Seiten des Vereins oder Verbandes ein berechtigtes Interesse gegeben und eine Verletzung schutzwürdiger Interessen der Betroffenen nicht ersichtlich ist.²

Die Veröffentlichung sollte aber auf diejenigen Funktionäre beschränkt bleiben, die für Außenstehende für eine Kontaktaufnahme von Interesse sind. Dazu gehören der Schützenmeister und sein bzw. seine Stellvertreter, Sportleiter, Schriftführer, Kassier, Jugendleiter und im Einzelfall weitere Personen wie z.B. der Verantwortliche für den Betrieb und die Bewirtschaftung des Schützenheimes.

¹) 20. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

²) Tätigkeitsbericht Nr. 1 der Aufsichtsbehörde für den Datenschutz Bayern

Auch wenn eine Einwilligung vorher nicht eingeholt werden muss, sollten die Betroffenen im Vorfeld über die beabsichtigte Veröffentlichung informiert werden. Widerspricht der Betroffene, hat eine Veröffentlichung zu unterbleiben. Notwendig ist eine Einwilligung dann, wenn eine Fotografie der Betroffenen oder zusätzliche, für eine Kontaktaufnahme nicht unbedingt erforderliche Daten mit veröffentlicht werden sollen oder wenn durch das Amt Rückschlüsse auf besondere Umstände der betroffenen Person denkbar sind, z.B. bei einem Behindertenvertreter.

Veröffentlichung von Urteilen der Vereinsgerichtsbarkeit

Eine Veröffentlichung von Urteilen der Vereinsgerichtsbarkeit im Internet ist unzulässig. Für Urteile, die im Vereinsordnungsverfahren ergehen und deren Veröffentlichung angeordnet ist, stehen regelmäßig Veröffentlichungsmöglichkeiten über Mitteilungsorgane des Vereins oder des Verbandes zur Verfügung. Es besteht keine Erforderlichkeit für eine weltweite Veröffentlichung im Internet. Darüber hinaus überwiegt das schutzwürdige Interesse des Betroffenen daran, dass seine personenbezogenen Daten wie Name und Inhalt des Gerichtsbeschlusses nicht weltweit bekannt gegeben werden¹.

Veröffentlichung von Daten über Minderjährige

Daten über Kinder, z.B. von Mitgliedern von Schüler- oder Jugendmannschaften, insbesondere mit Adresse, Geburtsdatum oder Foto, dürfen auf der Homepage nur mit vorheriger Einwilligung der Erziehungsberechtigten veröffentlicht werden. Die Einwilligung ist solange erforderlich, solange die Minderjährigen noch nicht die notwendige Einsichts- und Urteilsfähigkeit besitzen, um die Risiken einer Veröffentlichung ihrer personenbezogenen Daten im Internet abzusehen und zu beurteilen.

Soweit es sich um Informationen aus öffentlichen Veranstaltungen handelt, z.B. Ergebnisse von Meisterschaften oder Rundenwettkämpfen, ist eine Veröffentlichung aufgrund der Öffentlichkeit der Veranstaltung zulässig, jedoch sind die Angaben auf das Notwendigste zu beschränken, z.B. Name, Klasse des Wettbewerbes (Schüler, Jugend etc.) und Vereinsname. Weitere Informationen wie Adresse oder Geburtsdatum dürfen auch hier nicht veröffentlicht werden.

Empfehlung

Für eine Veröffentlichung von Bildern und Textbeiträgen im Internet ist zumindest für Minderjährige bis 14 Jahre eine schriftliche Einwilligung der Erziehungsberechtigten einzuholen. Die Erziehungsberechtigten sind über die näheren Umstände der Veröffentlichung zu unterrichten (Muster siehe Anlage).

¹) 20. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten

E-Mailverkehr

Bei einem Versand von E-Mails mit personenbezogenem Inhalt ist zu bedenken, dass E-Mails jederzeit von unbefugten Personen mitgelesen werden können. Sensible personenbezogene Informationen sollten deshalb nicht mit E-Mail versandt werden. Grundsatz ist, was nicht auf einer Postkarte versandt würde, sollte auch nicht per E-Mail versandt werden.

9. Löschung von personenbezogenen Daten

Wenn Mitglieder aus einem Verein ausscheiden, dürfen die personenbezogenen Daten nicht weiter gespeichert werden. Sie müssen gelöscht werden, wenn diese Daten für Vereinszwecke, z.B. Beitragsabrechnungen u.a. nicht mehr benötigt werden. Das Anbringen eines Vermerkes über die Beendigung der Mitgliedschaft im Mitgliederverzeichnis genügt nicht. Gleiches gilt auch, wenn jemand einen Aufnahmeantrag gestellt und diesen später wieder zurückgenommen hat. Von dieser Lösungsverpflichtung unberührt sind personenbezogene sport- und gesellschaftsbezogene Informationen, die für die Vereinsgeschichte von Interesse sind, z.B. Daten über Ehrenmitglieder, Vereinsfunktionäre oder Mitglieder, die für den Verein besondere Leistungen erbracht haben.

Empfehlung

Wenn Mitgliederdaten aus bestimmten Gründen über die Beendigung der Mitgliedschaft hinaus noch für einen gewissen Zeitraum erforderlich sind, sollte die Frist, für die die Daten über die Beendigung der Mitgliedschaft hinaus noch vorgehalten werden sollen, verbindlich festgelegt werden. Es sollen dann aber auch zuverlässige Regelungen geschaffen werden, die eine fristgerechte Löschung dieser Daten gewährleisten.

10. Datenverarbeitung im Auftrag

Die ursprüngliche Form der Datenverarbeitung im Auftrag liegt dann vor, wenn der Verein die Verarbeitung personenbezogener Daten einer anderen Einrichtung oder Stelle überträgt, z.B. wenn das Mitgliederverzeichnis durch eine Bank oder eine Sparkasse geführt oder der Beitragseinzug im Service durchgeführt wird.

Bei einer Datenverarbeitung im Auftrag bleibt der Verein als Auftraggeber für die zu verarbeitenden personenbezogenen Daten datenschutzrechtlich verantwortlich. Für die Vergabe der Datenverarbeitung ist deshalb der Abschluss eines schriftlichen Vertrages oder die Erteilung eines schriftlichen Auftrages erforderlich. Der Vertrag oder Auftrag muss die durchzuführende Datenverarbeitung eindeutig und vollständig beschreiben und den Auftragnehmer auf die Wahrung des Datenschutzes sowie auf die auftragsgemäße Durchführung der Verarbeitung verpflichten.

Eine Datenverarbeitung im Auftrag liegt auch dann vor, wenn durch einen Servicetechniker Wartungs- oder Reparaturarbeiten am Computer oder anderen Datenverarbeitungsgeräten, Softwarepflegearbeiten oder eine Datenrekonstruktion durchgeführt werden und dabei eine Kenntnisnahme von personenbezogenen Daten durch den Techniker nicht ausgeschlossen werden kann.

Der Verein muss im Hinblick auf die Vertraulichkeit der Daten den Auftragnehmer sorgfältig auswählen. Kriterium für die Auswahl ist grundsätzlich die Eignung der beim Auftragnehmer eingerichteten technischen und organisatorischen Maßnahmen. Diese müssen geeignet sein, die Einhaltung des erforderlichen Datenschutzes und der notwendigen Datensicherheit zu gewährleisten.

Häufig werden Hardwarereparatur- und Softwarepflegemaßnahmen oder Programmentwicklungs- und Installationsarbeiten von Mitgliedern des Vereins oder von Personen aus deren Freundes- oder Bekanntenkreis als Gefälligkeitsleistung durchgeführt. Auch hier gilt, dass diese Personen unter Zuverlässigkeitsgesichtspunkten sorgfältig ausgewählt werden müssen und dass ein schriftlicher Auftrag mit den genannten Inhalten und Verpflichtungen abgeschlossen werden muss.

Empfehlung

Der Auftragnehmer sollte zumindest schriftlich auf die Wahrung des Datenschutzes verpflichtet werden (Muster siehe Anlage).

11. Datenschutzgrundsätze und Regelungen für die Datenverarbeitung im Verein

Um die Datenverarbeitung im Verein rechtlich abzusichern und für die Mitglieder Transparenz über die Verarbeitung, Nutzung und Übermittlung von Daten zu schaffen, empfiehlt es sich, Datenschutzgrundsätze zu entwickeln und von den Mitgliedern beschließen zu lassen (Leitfaden siehe Anlage). In diesen Datenschutzgrundsätzen sollte festgelegt und beschrieben werden, welche Daten von den Mitgliedern erhoben und für welche Zwecke sie verarbeitet, genutzt und übermittelt werden sollen. Besonderes Augenmerk sollte dabei auf eine vollständige Darlegung aller Übermittlungs- und Veröffentlichungsvorgänge gelegt werden. Diese Datenschutzgrundsätze sollten genauso wie die Satzung jedem Mitglied zur Verfügung gestellt und bei jeder Neuaufnahme ausgegeben werden. Soweit erforderlich, könnten mit der Herausgabe dieser Datenschutzgrundsätze auch die Einwilligungserklärungen eingeholt werden, wobei in jedem Fall auf die Freiwilligkeit der Einwilligung und die Möglichkeit des jederzeitigen Widerrufs hingewiesen werden muss.

12. Verpflichtung auf das Datengeheimnis

Personen, die im Verein personenbezogene Daten von Mitgliedern verarbeiten oder verwalten, müssen schriftlich auf die Wahrung des Datengeheimnisses verpflichtet werden. Diese Verpflichtung gilt auch über die Beendigung des Ehrenamtes hinaus fort.

Empfehlung

Die Verpflichtung ist schriftlich vorzunehmen und sollte vom Vorsitzenden des Vereins durchgeführt werden (Verpflichtungsmuster siehe Anlage).

13. Bestellung eines Datenschutzbeauftragten

Sind mehr als vier Personen regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten betraut, muss der Verein einen Datenschutzbeauftragten bestellen. Zu berücksichtigen sind hier aber nur Mitarbeiter des Vereins im Sinne des Betriebsverfassungsgesetzes, d.h. Personen, die aufgrund eines Arbeits- oder Anstellungsvertrages angestellt sind. Die Aufsichtsbehörde für den Datenschutz in Rheinland-Pfalz hat hierzu im Tätigkeitsbericht Nr. 1 ebenfalls ausgeführt, dass nur große Vereine, die in ihrer Geschäftsstelle Arbeitnehmer beschäftigen, einen Datenschutzbeauftragten bestellen müssen.

Der Datenschutzbeauftragte muss nicht Mitglied des Vereins sein. Die Aufgaben des Datenschutzbeauftragten können auch von externen Personen wahrgenommen werden. Um Interessenkollisionen zu vermeiden, darf diese Aufgabe nicht vom Vorstand oder von der für die Datenverarbeitung zuständigen Person ausgeübt werden.

14. Technische und organisatorische Maßnahmen

Das Bundesdatenschutzgesetz sieht für jede verantwortliche Stelle die Einführung und ständige Anwendung geeigneter technischer und organisatorischer Maßnahmen vor, die die Ausführung der Vorschriften des Bundesdatenschutzgesetzes und die Erfüllung der in der Anlage zum Gesetz genannten Anforderungen gewährleisten. Diese Auflagen gelten auch für Vereine bezüglich der Erhebung, Verarbeitung und Nutzung der Mitgliederdaten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zum Schutzzweck steht.

In diesem Zusammenhang sollte die vereinsindividuelle Situation der Datenverarbeitung kritisch durchleuchtet werden. Das Bundesdatenschutzgesetz enthält hierzu in einer Anlage einen Katalog von Kontrollbereichen. Zu den ein-

zelen Kontrollbereichen ist zu analysieren, welchen Risiken die personenbezogenen Daten in der jeweiligen Situation (z.B. Speicherung auf einem PC des Vereins im Vereinsheim oder Speicherung auf dem privaten PC eines Ehrenamtsträgers) ausgesetzt sind. Im Anschluss daran müssen angemessene und geeignete Maßnahmen ausgewählt und eingerichtet werden, die geeignet sind, die personenbezogenen Daten je nach dem Grad ihrer Sensibilität ausreichend zu schützen. Dabei werden nur diejenigen Maßnahmen verlangt, deren Aufwand im Hinblick auf den Schutzzweck der Daten angemessen ist. Besitzen die Daten einen relativ geringen Sensibilitätsgrad, genügen auch einfachere Schutzmaßnahmen. Handelt es sich jedoch um Daten mit einem hohen Sensibilitätsgrad, z.B. Daten über Bankverbindungen, müssen diese auch mit erhöhter Sorgfalt behandelt und geschützt werden. Das beigefügte Merkblatt zeigt für die einzelnen Kontrollbereiche die besonderen Risiken und enthält Beispiele für mögliche technische und organisatorische Regelungen. Verantwortlich für die Durchführung dieser Maßnahmen und die Einrichtung geeigneter technischer und organisatorischer Maßnahmen ist der Vorsitzende des Vereins.

Empfehlung

Anhand eines Merkblattes, „Technische und organisatorische Maßnahmen im Schützenverein“ (Leitfaden siehe Anlage) sollte eine Risikobetrachtung durchgeführt und angemessene und geeignete Maßnahmen ausgewählt, eingeführt und in einem Merkblatt beschrieben werden. Das Merkblatt sollte den Mitgliedern bekannt gegeben werden.

15. Bußgeld und Schadensersatz

Das Bundesdatenschutzgesetz enthält einen Bußgeldkatalog, der bestimmte Verstöße gegen den Datenschutz als Ordnungswidrigkeit ahndet und mit Bußgeld bis 25.000 Euro, in besonders schwerwiegenden Fällen bis 250.000 Euro, bewehrt. So wird u.a. mit Bußgeld belegt, wer den Betroffenen bei der Ansprache zur Werbung nicht über die Möglichkeit unterrichtet, weiteren Werbemaßnahmen zu widersprechen.

Entsteht dem Betroffenen aus einer Datenschutzverletzung heraus ein nachweisbarer und berechenbarer Schaden, ist der Verein zum Ersatz des entstandenen Schadens verpflichtet. Dieser Schadensersatz entfällt, wenn der Verein die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

16. Zusätzliche Informationen zum Datenschutz und zur Datensicherheit

Zum Thema Datenschutz und Datensicherheit stehen im Internet umfassende Informationsmöglichkeiten zur Verfügung. Der Bundesbeauftragte für den Da-

tenschutz, die Landesbeauftragten für den Datenschutz und die zuständigen Aufsichtsbehörden bieten kostenloses Informationsmaterial zu allen Themen des Datenschutzes an. Ferner steht Informationsmaterial zum Download zur Verfügung. Zum Thema Datensicherheit bietet das Bundesamt für Sicherheit in der Informationstechnik ebenfalls wertvolles Informationsmaterial an. Stellvertretend für viele andere Informationsquellen werden im Folgenden einige Adressen genannt.

www.bfdi.bund.de	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
www.im.bwl.de	Innenministerium Baden-Württemberg
www.datenschutzzentrum.de	Unabhängiges Landeszentrum für den Datenschutz Schleswig-Holstein
www.bsi.de	Bundesamt für Sicherheit in der Informationstechnik

Auf diesen Internetseiten werden zusätzlich Links zu den weiteren Aufsichtsbehörden, den Landesdatenschutzbeauftragten und sonstigen Stellen angeboten, die Informationen zum Datenschutz und zur Datensicherheit bereithalten.

Anschrift des Verfassers:

Helmut Bartels
Dorfstraße 45
85232 Bergkirchen

Der Verfasser ist Pistolenreferent im Schützengau Dachau und Fachberater für Datenschutz und Datensicherheit.

Einwilligung für eine Veröffentlichung personenbezogener Daten im Internet

Der Vereinsvorstand weist hiermit darauf hin, dass ausreichende technische Maßnahmen zur Gewährleistung des Datenschutzes getroffen wurden. Dennoch kann bei einer Veröffentlichung personenbezogener Daten im Internet ein umfassender Datenschutz nicht garantiert werden. Daher nimmt das Vereinsmitglied die Risiken für eine eventuelle Persönlichkeitsrechtsverletzung zur Kenntnis und ist sich bewusst, dass

- die personenbezogenen Daten auch in Staaten abrufbar sind, die keine der Bundesrepublik Deutschland vergleichbaren Datenschutzbestimmungen kennen,
- die Vertraulichkeit, die Integrität (Unverletzlichkeit), die Authentizität (Echtheit) und die Verfügbarkeit der personenbezogenen Daten nicht garantiert ist.

Das Vereinsmitglied trifft die Entscheidung zur Veröffentlichung seiner Daten im Internet freiwillig und kann seine Einwilligung jederzeit widerrufen.

Erklärung

Ich bestätige, das Vorstehende zur Kenntnis genommen zu haben, und willige ein, dass der Verein <Name des Vereins> folgende Daten zu meiner Person (unzutreffende Daten streichen bzw. weitere Daten ergänzen) auf folgender Internetseite des Vereins veröffentlichen darf:

Onlinedienst/Internet; Zugangsadresse

Allgemeine Daten

Vorname: _____

Zuname: _____

Fotografische Aufnahmen

Sonstige Daten (z.B. Mannschaftsaufstellungen, Ergebnisse von Wettkämpfen und Meisterschaften)

Zusätzliche Daten von Funktionsträgern

Anschrift: _____

Telefonnummer: _____

Faxnummer: _____

E-Mailadresse: _____

Ort und Datum

Unterschrift

Text lt. Merkblatt des Innenministeriums Baden-Württemberg „Datenschutz im Verein“,

Verpflichtung auf das Datengeheimnis

Nach den Vorschriften des Bundesdatenschutzgesetzes (§ 5 BDSG) dürfen personenbezogene Daten nur im Rahmen der Vereinszwecke und nur zu dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck erhoben, verarbeitet, bekannt gegeben, zugänglich gemacht oder auf sonstige Weise genutzt werden. Personenbezogene Daten sind hierbei alle zu einer Person gehörenden oder auf eine Person beziehbaren Einzelangaben über persönliche und sachliche Verhältnisse.

Sie werden hiermit verpflichtet, personenbezogene Daten jeder Art nur im erforderlichen Umfang und nur zu dem jeweiligen satzungsmäßigen oder sonstigen berechtigten Vereinszweck zu erheben, zu verarbeiten, bekannt zu geben, zugänglich zu machen oder auf sonstige Weise zu nutzen. Diese Verpflichtung bleibt auch nach Beendigung des Ehrenamtes, der Tätigkeit oder Mitgliedschaft im Verein bestehen. Verletzungen des Datengeheimnisses können strafrechtliche Konsequenzen oder Schadensersatzansprüche nach sich ziehen.

Sonstige Geheimhaltungsverpflichtungen bleiben von dieser Verpflichtung unberührt.

Meine Verpflichtung auf das Datengeheimnis gemäß § 5 Bundesdatenschutzgesetz habe ich zur Kenntnis genommen.

Datum Unterschrift

Datenschutzverpflichtung über Datenverarbeitung im Auftrag

Der Auftragnehmer verpflichtet sich,

das Datengeheimnis im Sinne des Bundesdatenschutzgesetzes zu wahren und alle ihm bei der Erbringung der Leistungen bekannt werdenden personenbezogenen Daten und sonstige Informationen vertraulich zu behandeln und nicht unbefugt zu offenbaren,

die personenbezogenen und sonstigen Daten/Informationen nur nach Weisung des Auftraggebers und nicht zu einem anderen als den vereinbarten Vertragszweck zu verarbeiten oder zu nutzen,

die personenbezogenen und sonstigen Daten/Informationen vor Missbrauch oder Verlust zu schützen und dazu ausreichende technische und organisatorische Maßnahmen zu treffen, welche dem Schutzzweck angemessen sind und den Forderungen des Bundesdatenschutzgesetzes gerecht werden,

Subunternehmer nur mit Zustimmung des Auftraggebers und nur in dem vom Auftraggeber gestatteten Umfang einzusetzen.

Der Auftragnehmer stellt ferner sicher, dass bestehende Datenschutzbestimmungen, soweit sie für ihn zutreffen, beachtet und eingehalten werden.

Diese Verpflichtungen gelten für den Auftragnehmer und seine Erfüllungsgehilfen sowie für eventuelle Subunternehmer und bestehen auch nach Beendigung dieses Vertrages/Auftrages auf unbegrenzte Dauer fort.

Name/Firmenbezeichnung

Datum Unterschrift

Merkblatt

Technische und organisatorische Maßnahmen im Schützenverein

Das Bundesdatenschutzgesetz enthält in der Anlage zu § 9 acht Kontrollbereiche, die als Leitfaden für die Ausgestaltung der technischen und organisatorischen Maßnahmen herangezogen werden können. In diesem Merkblatt werden diese Kontrollbereiche sowie die Risikokriterien beschrieben und geeignete Maßnahmen vorgestellt. Je nach der individuellen Situation im Verein müssen zu den einzelnen Risiken geeignete Schutzmaßnahmen eingerichtet und unterhalten werden. Soweit erforderlich, sind zu den einzelnen Schutzmaßnahmen die Verantwortlichen Personen zu benennen.

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die vereinsinterne Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogenen Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbei-

tet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragsskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungsgebot).

Risiken und Maßnahmen zu den einzelnen Kontrollbereichen

Zutrittskontrolle

Die Zutrittskontrolle betrifft die Sicherung von Gebäuden und Räumen, in denen Computer und Datenträger untergebracht sind, auf denen personenbezogene Daten von Mitgliedern verarbeitet oder gespeichert werden.

Hier ist zu prüfen, in welchen Lokalisationen und Räumen Computer und Datenträger untergebracht sind. Dies kann z.B. im Schützenheim, in Nebenräumen von Gastwirtschaften, Schießständen oder in den Privaträumen von Vorstandsmitgliedern der Fall sein. Häufig werden Daten auf verschiedenen Computern, z.B. im Schützenheim und auf privaten Computern, gespeichert und verarbeitet und nicht überall unterliegt die Zutrittskontrolle der Entscheidungs- und Kontrollbefugnis des Vereins, z.B. wenn der Verein in einer Gastwirtschaft oder in einem öffentlichen Gebäude untergebracht ist, das auch von anderen Einrichtungen und Vereinen genutzt wird. Auch wenn der Verein über ein eigenes Schützenheim verfügt, ist zu hinterfragen, ob und welche vereinsfremde Personen Zutritt zum Schützenheim besitzen bzw. im Schützenheim verkehren, z.B. wenn das Vereinsheim auch für private Feiern überlassen wird, im Rahmen von Wettkämpfen und Meisterschaften auch Mitglieder anderer Vereine verkehren oder das Vereinsheim auch anderen Vereinen genutzt wird.

In Abhängigkeit von diesen Verhältnissen und der Art und Sensibilität der auf den jeweiligen Computern gespeicherten Daten ist zu prüfen, ob die Räumlichkeiten vor unbefugtem Zutritt ausreichend geschützt und ob Computer und Datenträger sicher verwahrt sind (Schutz vor Diebstahl und unbefugter Benutzung) und ob bzw. welche Sicherheitsmaßnahmen erforderlich sind. Zu den Sicherheitsmaßnahmen gehören alle Maßnahmen der Gebäude- und Raumsicherung wie Alarmanlagen, sichere Verwahrung der Datenträger, abgesperrter Büroraum für den Computer etc. Ebenso einzubeziehen sind Regelungen zur kontrollierten Schlüsselvergabe und zur sicheren Schlüsselverwahrung, denn jede Schließanlage verliert ihre Sicherungsfunktionen, wenn die zugehörigen Schlüssel unkontrolliert und ohne Wissen der Verantwortlichen weitergereicht werden oder der Schlüssel zum abgesperrten Büroraum im Vereinsheim offen am Schlüsselbrett hängt.

Wo sich die Maßnahmen der Zutrittskontrolle den Befugnissen des Vereins entziehen, z.B. in Gastwirtschaften oder anderen öffentlich zugänglichen Gebäuden, muss u.U. auf einen stationären Computer verzichtet und ein Notebook eingesetzt werden, das nach dem Vereinsabend an einem anderen Ort sicher verwahrt werden kann.

Werden die personenbezogenen Daten der Mitglieder auf einem privaten Computer eines Vorstandsmitgliedes gespeichert und verarbeitet, sind die beschriebenen Verfahren der Zutrittskontrolle z.T. so nicht umzusetzen. Hier müssen dann andere, unter den folgenden Kontrollbereichen beschriebene Maßnahmen greifen.

Zugangskontrolle

Die Zugangskontrolle betrifft die Sicherung des Computers vor unbefugter Benutzung. Regelmäßig werden zu diesem Zweck Benutzererkennung und Passwort eingesetzt. Wenn im Verein mehrere Personen einen Computer benutzen, ist es zweckmäßig, für jeden Berechtigten eine Benutzererkennung einzurichten. Mit dieser Benutzererkennung können bestimmte Rechte verknüpft werden, die der Benutzer im System haben soll, z.B. Zugriffsrechte nur auf bestimmte Datenarten (für den Kassier auf die Bankdaten, für den Sportleiter auf die Sportdaten etc.). Mit einem Passwort identifiziert sich der Benutzer gegenüber dem System.

Das Passwort soll eine bestimmte Mindestlänge besitzen (mindestens sechs Stellen), es sollen keine sprechenden Begriffe oder Wörter aus dem Wörterbuch benutzt werden, soll kryptisch sein und aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Das Passwort muss vertraulich behandelt und auch in regelmäßigen Abständen (z.B. alle drei Monate) geändert werden.

Gerade wenn die Mitgliederdaten auf privaten Computern gespeichert werden, ist die Einrichtung eines sicheren Passwortes wichtig, um eine unbefugte Benutzung des Computers zu vermeiden.

Zugriffskontrolle

Die Zugriffskontrolle betrifft den Schutz der personenbezogenen Daten in einem IT-System, wenn mehrere Personen auf den Computer zugriffsberechtigt sind, aber nicht jeder auf den Computer Zugriffsberechtigte auch auf alle Daten Zugriff besitzen soll. Dies ist z.B. bei einem Vereinscomputer der Fall, auf dem sowohl die Mitgliedschafts-, Sport- und Bankeinzugsdaten gespeichert sind. Hier soll der Sportbereich nicht auf die Bankeinzugsdaten zugreifen können, weil es sich bei diesen Daten einerseits um sensiblere Daten handelt und andererseits diese Daten auch nur vom Kassier benötigt werden.

Durch die Regelung von Benutzerrechten, in denen abgebildet ist, wer auf welche Daten zugreifen können soll und auf welche Daten einzelne Mitglieder der Vorstandschaft keine Zugriffsberechtigung besitzen sollen (z.B. auf die Bankeinzugsdaten nur der Kassier), ist der Kreis der zugriffsberechtigten Personen auf das notwendige Maß zu beschränken.

Von besonderer Bedeutung sind diese Regelungen, wenn personenbezogene Vereinsdaten auf dem privaten Computer eines Vorstandsmitgliedes gespeichert sind und auch Familienmitglieder auf den Computer zugreifen können. Hier müssen zwingend durch Einrichtung von entsprechenden Leseberechtigungen Zugriffsschutzmaßnahmen eingerichtet werden, die eine unbefugte Kenntnisnahme der Daten durch Familienmitglieder verhindern. Alternativ können personenbezogene Vereinsdaten auch auf externen Datenträgern wie USB-Sticks oder mobilen Plattenlaufwerken gespeichert und verarbeitet werden. Diese Datenträger können nach der Verarbeitung gesondert verwahrt werden und so vor unbefugtem Zugriff geschützt werden.

Externe Datenträger besitzen auch den Vorteil, dass bei einem Wechsel im Ehrenamt mit dem Datenträger die Vereinsdaten unkompliziert an den Nachfolger übergeben werden können und auf dem privaten Computer des Vorgängers keine Restdaten verbleiben.

Weitergabekontrolle

Mit den Maßnahmen der Weitergabekontrolle sollen die personenbezogenen Daten während ihrer Speicherung oder Übermittlung vor einer Weitergabe an unbefugte Personen geschützt werden. Die Schutzvorkehrungen müssen auf jedem Computer, unabhängig davon, ob es sich um einen Vereinscomputer oder um einen privaten Computer handelt, eingerichtet werden.

Folgende Risiken müssen hier unterschieden werden:

Unbefugte Kenntnisnahme bei Übermittlungen

Werden Daten auf Datenträgern übermittelt, ist zu gewährleisten, dass die Datenträger nicht in unbefugte Hände geraten können. Die Datenträger sollten deshalb z.B. mit der Post versandt oder nur dem berechtigten Empfänger persönlich ausgehändigt werden.

Elektronischer Versand von personenbezogenen Daten

Werden personenbezogene Daten mittels E-Mail versandt, ist zu bedenken, dass das E-Mail-System kein vertrauliches Transportmedium ist, weil die Inhalte von E-Mails beim Versand von Unbefugten mitgelesen und ausgewertet werden können. Personenbezogene Daten sollten deshalb per E-Mail nur verschlüsselt versandt werden.

Viren- und Internetsicherheit

Grundsätzlich muss jeder Computer mit einem aktuellen Virens Scanner ausgerüstet werden. Wenn ein Computer, auf dem personenbezogene Vereinsdaten gespeichert und verarbeitet werden, über einen Internetanschluss verfügt, muss der Computer zusätzlich durch geeignete Sicherheitssoftware (Firewall/Internet-Security-Software) vor den Internetrisiken geschützt werden. Dabei ist auch darauf zu achten, dass der Virens Scanner und die Sicherheitssoftware ständig auf dem aktuellen Stand gehalten werden und die Firewall sowohl den eingehenden als auch den ausgehenden Datenverkehr kontrolliert, um die personenbezogenen Daten auch vor einem unbemerkten Versand an unbefugte Empfänger zu schützen.

Vernichtung von Datenträgern

Wenn Magnetdatenträger ausgedondert werden (Verkauf oder Verschrottung) müssen die darauf gespeicherten Daten sicher, d.h. mit einem speziellen Löschmodprogramm, gelöscht werden. Eine Formatierung des Datenträgers ist nicht ausreichend, weil nach einer Formatierung die Daten mit einer Datenrettungssoftware wieder lesbar gemacht werden können. Ist eine derartige Löschung nicht möglich, z.B. weil der Datenträger defekt ist, muss er mechanisch zerstört oder z.B. in einem starken Magnetfeld gelöscht werden. Ebenso ist bei der Entsorgung von Papier darauf zu achten, dass personenbezogene Daten nicht in unbefugte Hände geraten können. Mitgliederlisten und andere Papierunterlagen mit personenbezogenen Daten sind deshalb mit einem geeigneten Aktenvernichter zu zerkleinern.

Eingabekontrolle

Die Eingabekontrolle ist i.d.R. im Bereich der Vereinsdatenverarbeitung nicht relevant.

Auftragskontrolle

Wenn personenbezogene Vereinsdaten im Auftrag durch eine andere Stelle verarbeitet werden (z.B. Bank erledigt für den Verein die Mitgliederbestandsführung und den Beitragseinzug) muss mit dem Auftragnehmer ein Vertrag über die Datenverarbeitung im Auftrag abgeschlossen oder zumindest ein schriftlicher Auftrag mit einer Datenschutzverpflichtung erteilt werden. Eine Datenschutzverpflichtung ist auch erforderlich, wenn ein Techniker mit der Reparatur eines Computers, einer Softwareinstallation oder mit einer Datenrekonstruktion beauftragt wird, wenn dabei eine Kenntnisnahme von personenbezogenen Daten durch den Techniker nicht ausgeschlossen werden kann.

Verfügbarkeitskontrolle

Personenbezogene Daten müssen auch vor einem zufälligen Verlust oder einer zufälligen Zerstörung geschützt werden.

Es ist deshalb erforderlich, die personenbezogenen Vereinsdaten regelmäßig auf einem anderen Trägermedium (z.B. CD-ROM, USB-Stick oder externe Magnetplatte) zu sichern, um im Fall einer Zerstörung der Daten den Datenbestand wieder rekonstruieren zu können.

Trennungsgebot

Beitrags- und Bankdaten einerseits und Mitgliedschafts- und Sportdaten andererseits dienen unterschiedlichen Zwecken und müssen zumindest logisch voneinander getrennt sein. Dies bedeutet nicht, dass sie auf unterschiedlichen Computern oder Datenträgern gespeichert werden müssen. Es genügt, wenn sie logisch so voneinander getrennt sind, sodass sie für die unterschiedlichen Zwecke getrennt voneinander verarbeitet werden können. Insbesondere müssen entsprechende Zugriffsstrukturen geschaffen werden können, die gewährleisten, dass nur diejenigen Personen auf die Daten zugreifen können, die die Daten für ihre Aufgaben auch benötigen.

Datenschutzgrundsätze und Regelungen für die Datenverarbeitung im Verein

Die Datenschutzgrundsätze regeln die grundsätzlichen Fragen zum Datenschutz im Verein. Sie sind für die Erhebung, Verarbeitung, Nutzung und Übermittlung personenbezogener Daten verbindlich und dienen auch der Information der Vereinsmitglieder.

Folgende Bereiche sollten geregelt werden:

1. Führung der Mitgliederdaten

Hier sind die Sachverhalte und Grundsätze zur Führung der Mitgliederdaten zu beschreiben. Dazu gehören folgende Fragen:

- Werden die Mitgliederdaten in automatisierten oder nicht automatisierten Verfahren geführt?
- Wer ist für die Verwaltung der Daten verantwortlich?
- Von welchen Stellen im Verein (Bezeichnung des Ehrenamtes) werden welche Daten verwaltet?
- Werden die Daten im Auftrag verarbeitet?

2. Erhebung von personenbezogenen Daten

Hier sollten folgende Grundsätze formuliert werden:

- Erhebung nur, soweit die personenbezogenen Daten für die Verfolgung der Vereinszwecke erforderlich sind.
- Beachtung der Hinweise auf eine eventuelle Freiwilligkeit der Angaben.
- Datenerhebung nur von den Mitgliedern.

3. Übermittlungen

Hier ist zu beschreiben, an welche Stellen oder Einrichtungen welche personenbezogenen Daten für welche Zwecke übermittelt werden, z.B. Bayerischer Schützenbund e.V., Banken für den Beitragseinzug, Sponsoren und Förderer des Vereins.

4. Offenbarung von Daten innerhalb des Vereins

Hier ist zu beschreiben, welche Datenkategorien über welche Trägermedien offenbart werden, z.B.:

- Werden Mitgliederlisten zur allgemeinen Einsicht zur Verfügung gestellt?
- Welche Aushänge werden am schwarzen Brett ausgehängt?
 - Sportergebnisse (Meisterschaften, Rundenwettkämpfe, Preisschießen etc.),

- Vereinsmeisterschaften und sonstige interne Wettbewerbe,
- Meldungen, Mannschaftsaufstellungen, Starterlisten,
- Persönliche Jubiläen, Geburtstage usw.,
- vereinsinterne Mitteilungen.

5. Veröffentlichung in der Presse

Hier sind die Verantwortlichen zu benennen und die Grundsätze über Anlässe und Inhalte von Veröffentlichungsverfahren zu beschreiben, z.B.:

Die Vorstandschaft < Pressestelle > des Vereins veröffentlicht in der örtlichen Presse nach eigenem Ermessen Beiträge in Wort und Bild über das Vereinsleben und das Sportgeschehen, soweit es sich um Informationen von allgemeinem Interesse handelt. Soweit erforderlich, insbesondere bei Bildveröffentlichungen über einzelne Personen, wird die Einwilligung der Betroffenen eingeholt.

6. Veröffentlichung im Internet

Hier ist zu beschreiben, ob und welche personenbezogenen Informationen im Internet veröffentlicht werden, z.B.

- Kontaktdaten von Vorstandsmitgliedern (Fotos nur mit Einwilligung),
- Ergebnisse von öffentlichen Wettbewerben,
- Mannschaftsaufstellungen (Fotos nur mit Einwilligung).

Sonstige personenbezogene Informationen nur mit Einwilligung der Betroffenen bzw. der Erziehungsberechtigten.

7. Rechte der Mitglieder

Hier sind die Rechte der Mitglieder zu beschreiben, z.B.:

Die Mitglieder haben das Recht, jederzeit Auskunft über die zu ihrer Person gespeicherten personenbezogenen Daten einschließlich deren Herkunft, Art der Nutzung und Übermittlung, ggf. auch über die Empfänger, zu verlangen. Falls Daten unrichtig sind, kann jedes Mitglied die Berichtigung seiner Daten und falls bestimmte Daten für die Erreichung der Vereinszwecke nicht mehr erforderlich sind, auch deren Löschung verlangen.

Soweit die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten der Freiwilligkeit unterliegt, wird die freiwillige Einwilligung der Mitglieder eingeholt. Das Mitglied kann jederzeit widersprechen, ohne dass ihm dadurch irgendwelche Nachteile entstehen.

Datenschutzregelung in der Vereinssatzung

5 ..Mitgliedschaft - Datenschutz

(1) Mit dem Beitritt erklärt sich das Mitglied einverstanden, dass die im Zusammenhang mit der Mitgliedschaft benötigten personenbezogenen Daten unter Berücksichtigung der Vorgaben des Bundesdatenschutzgesetzes für den Verein erhoben und in einem DV-gestützten Verfahren verarbeitet und genutzt werden. Dabei handelt es sich um folgende Angaben:

Name, Vorname, Geburtsdatum,

Anschrift, Telefon,

Erstverein,

Bankverbindung (freiwillig).

Zusätzliche Daten, die im Zusammenhang mit sportlichen Aktivitäten, einem eventuellen Ehrenamt oder sonstigen Vereinsaktivitäten zur Erfüllung der Vereinszwecke anfallen bzw. erforderlich sind.

Ohne dieses Einverständnis kann eine Mitgliedschaft zum Verein nicht begründet werden.

(2) Die überlassenen personenbezogenen Daten dürfen ausschließlich für Vereinszwecke verwendet werden. Hierzu zählen insbesondere die Mitgliederverwaltung, die Durchführung des Sport- und Spielbetriebes, die Veröffentlichung in der Vereinszeitung sowie interne Aushänge am "Schwarzen Brett". Eine anderweitige Verarbeitung oder Nutzung (z. B. Übermittlung an Dritte) ist – mit Ausnahme der erforderlichen Mitgliedermeldung an den Bayerischen Sportschützenbund e.V. und der Meldungen zur Erlangung von Startberechtigungen bei Meisterschaften, Rundenwettkämpfen und sonstigen schießsportlichen Veranstaltungen – nicht zulässig.

Datenschutzhinweis in der Beitrittserklärung

Datenschutzhinweis: Ich erkläre mich damit einverstanden, dass vorstehende Daten für vereinsinterne Zwecke in einer EDV-gestützten Mitglieder- und Beitragsdatei gespeichert und verarbeitet werden. Im Rahmen des vorgeschriebenen Mitgliedermeldeverfahrens werden personenbezogene Daten an den Bayerischen Sportschützenbund e.V. übermittelt.

Ohne dieses Einverständnis kann eine Mitgliedschaft nicht begründet werden. Die Regelungen zum Datenschutz in der Vereinssatzung habe ich zur Kenntnis genommen.

*Texte auf der Grundlage eines Musters des Unabhängigen Landesentrums
für den Datenschutz Schleswig-Holstein*

Einwilligungserklärung der Erziehungsberechtigten zur Internetpräsentation auf der Vereinshomepage

Aufklärung und Einwilligungserklärung zur Internetpräsentation auf der Homepage des Schützenvereins < Name des Vereins > im Internet

Liebe Eltern, wir möchten gerne Bilder und Textbeiträge von Ihrem Sohn/Ihrer Tochter.....für die Internetseite unseres Vereines verwenden. Bilder und Texte verfolgen ausschließlich den Zweck, den Verein und insbesondere unsere Schützen mit ihren Aktivitäten in der Öffentlichkeit darzustellen.

Die Darstellung wird unter der Verantwortung von.....erstellt und laufend überarbeitet. Sicherlich ist Ihnen bekannt, dass über das Internet eine weltweite Abrufbarkeit und Veränderbarkeit der Bilder möglich ist. Nach dem Kunst- und Urheberrechtsgesetz hat jeder Mensch ein Recht am eigenen Bild. Daher dürfen grundsätzlich keine Bilder ohne sein ausdrückliches Einverständnis verbreitet werden. Gleiches gilt für Textdarstellungen, sofern sie auf einzelne Personen Bezug nehmen.

Wir möchten Sie darum fragen, ob Sie damit einverstanden sind, dass Bilder Ihres Kindes ohne Anschriftenangabe für diese Zwecke verwendet werden, und ob wir über Ihr Kind ebenfalls ohne Anschriftenangabe in sport- und vereinsbezogenen Bild- und Textdarstellungen berichten dürfen.

Die Abgabe dieser Erklärung ist selbstverständlich freiwillig. Ihr Kind wird keine Nachteile erleiden, wenn Sie Ihre Einwilligung nicht erteilen. Die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden. Selbstverständlich werden dann alle Daten gelöscht.

Ich bin damit einverstanden, dass Bilder meiner Tochter/meines Sohnes auf der Internetseite www.....de veröffentlicht werden

Name, Anschrift

Datum, Unterschrift
des/der Erziehungsberechtigten

Text auf der Grundlage eines Musters des Unabhängigen Landeszentrums für den Datenschutz Schleswig-Holstein. Geeignet für die Stellvertretung von Minderjährigen bis 14 Jahre.