

Fragekatalog der Q&A Session zum Thema Datenschutz im Sportverein- und verband

Die vorliegenden Antworten zu den entsprechenden Fragen sind als Hinweise und Wegleitung allgemeiner Art zu verstehen und stellen keine Rechtsberatung dar. Der ZKS übernimmt keine Haftung.

Organisation

1) Muss ein/e Datenschutzverantwortliche/r im Verein bestimmt werden oder reicht es, die Bestimmungen zu formulieren und zu veröffentlichen?

Das Schweizer Datenschutzgesetz (DSG) sieht in Art. 10 die Möglichkeit der Ernennung eines sog. Datenschutzberaters vor. Diese Funktion ist jedoch freiwillig. Folglich sind Vereine nicht verpflichtet, einen Datenschutzberater zu benennen.

Dennoch empfiehlt es sich zu Organisationszwecken, eine verantwortliche Person zu definieren, die für den Datenschutz im Verein zuständig ist, selbst wenn es sich bei dieser Person nicht um einen Datenschutzberater im Sinne des Gesetzes handelt. Diese Person sollte über das notwendige Fachwissen verfügen und insbesondere folgende Aufgaben erfüllen:

- Ansprechperson für Datenschutzfragen innerhalb des Vereins
- Ansprechperson für Anfragen von betroffenen Personen und Behörden
- Überwachung der Einhaltung der Datenschutzvorschriften im Verein
- Führung des Inventars der Bearbeitungstätigkeiten

Es gilt aber zu betonen, dass Datenschutz Teamarbeit ist und die Einhaltung der datenschutzrechtlichen Vorschriften sämtlichen im Verein tätigen Personen obliegt.

2) Welche Anpassungen müssen in den Vereins-Statuten vorgenommen werden?

Die Statuten dienen der Gründung des Vereins und regeln die Aufgaben sowie die Rollen der einzelnen Organe. Eine Integration von Datenschutzrichtlinien in den Statuten erscheint übermässig und untypisch. Hingegen ist es sinnvoll, interne Richtlinien zu erarbeiten, die bestimmte Grundprinzipien für den Umgang mit Personendaten festlegen. Diese können in einem separaten Dokument festgehalten oder beispielsweise im Vereinsreglement ergänzt werden.

3) Dürfen Trainerinnen und Trainer die Daten der eigenen Riegenmitglieder bearbeiten? Bisher habe ich nur immer über eine verantwortliche Person im Verein gelesen.

In diesem Zusammenhang ist zwischen dem Verantwortlichen im Sinne des Gesetzes und der für Datenschutz verantwortlichen Person in der Organisation zu unterscheiden. Beim Verantwortlichen im Sinne des Gesetzes handelt es sich um diejenige Person, die über den Zweck und die Mittel der Datenbearbeitung entscheidet. Hierbei handelt es sich nicht um eine einzelne Person, sondern um den Verein als Ganzes.

Trainerinnen und Trainer dürfen als im Verein tätige Personen die Daten ihrer eigenen Riegenmitglieder bearbeiten. Dies ist im Rahmen der notwendigen Aufgaben zur Organisation und Durchführung der sportlichen Aktivitäten erforderlich.

Weitergabe von Daten

4) Was muss bei der Weitergabe von Personendaten an Dritte beachtet werden? (z.B. an den Verband, Gemeinde für Sportlerehrungen, etc.)

Eine Weitergabe von Personendaten ist gegeben, wenn die Personendaten einer anderen Person, als derjenigen, die sie bisher bearbeitet hat, zugänglich gemacht werden. Bei einer solchen Weitergabe müssen immer die folgenden vier Thematiken beachtet werden:

1. Allgemeine Grundsätze des Datenschutzes

Rechtmässigkeit, Treu & Glauben, Erkennbarkeit, Zweckbindung, Verhältnismässigkeit, Speicherbegrenzung, Richtigkeit, Datensicherheit

Bei der Weitergabe von Personendaten handelt es sich um eine Bearbeitungstätigkeit. Entsprechend sind wie bei jeder Bearbeitungstätigkeit die Bearbeitungsgrundsätze einzuhalten:

<i>Rechtmässigkeit:</i>	Gibt es gesetzliche Vorschriften, die die Weitergabe verbieten, z.B. Geheimhaltungspflichten?
<i>Treu & Glauben:</i>	Hat die betroffene Person der Weitergabe widersprochen?
<i>Erkennbarkeit:</i>	Ist die Weitergabe für die betroffene Person ersichtlich, z.B. indem diese in der Datenschutzerklärung vorgesehen ist?
<i>Zweckbindung:</i>	Ist die Weitergabe vom kommunizierten Zweck gedeckt?
<i>Verhältnismässigkeit:</i>	Werden nicht mehr Daten weitergegeben als notwendig?
<i>Speicherbegrenzung:</i>	Werden die Daten vom Dritten nicht länger aufbewahrt als nötig?
<i>Richtigkeit:</i>	Sind die weitergegebenen Daten korrekt?
<i>Datensicherheit:</i>	Ist die Datensicherheit gewährleistet?

Falls diese Grundsätze nicht eingehalten werden, ist ein Rechtfertigungsgrund erforderlich. Es gibt drei mögliche Rechtfertigungsgründe: überwiegendes privates oder öffentliches Interesse, gesetzliche Bestimmungen und Einwilligung.

2. **Auslandbezug**

Werden Personendaten ins Ausland weitergegeben, ist zu prüfen, ob das Empfängerland über ein angemessenes Datenschutzniveau verfügt. Welche Länder über einen angemessenen Datenschutz verfügen, ist aus Anhang 1 der Datenschutzverordnung ersichtlich – grundsätzlich kann festgehalten werden, dass Länder innerhalb des Europäischen Wirtschaftsraums (EWR) über ein angemessenes Datenschutzniveau verfügen. Falls dies nicht der Fall ist (bspw. USA), müssen zusätzliche Garantien vorgesehen werden, wie z.B. Standardvertragsklauseln (Standard Contractual Clauses, in Einzelfällen die Einwilligung). Ausserdem ist eine sog. Datenschutz-Folgenabschätzung durchzuführen.

Unabhängig vom Datenschutzniveau ist die betroffene Person über das oder die spezifische(n) Empfängerland bzw. -länder zu informieren.

Die Datenschutzerklärung sollte folglich einen Absatz enthalten, aus dem ersichtlich ist, an wen (Namen oder auch nur Kategorien wie z.B. IT-Provider) Personendaten weitergegeben werden und in welchem Land oder welchen Ländern sich diese befinden. Sollten zusätzliche Garantien notwendig sein, so sind diese ebenfalls zu nennen.

3. **Art von Personendaten**

Werden besonders schützenswerte Personendaten (beispielsweise Gesundheitsdaten) an Dritte weitergegeben, handelt es sich um eine Persönlichkeitsverletzung, weshalb es zwingend eines Rechtfertigungsgrundes bedarf.

4. **Involvierte Parteien**

Schliesslich ist die Beziehung zwischen den involvierten Parteien zu analysieren. Es wird zwischen Auftragsbearbeitern und eigenständigen Verantwortlichen unterschieden.

Beim Auftragsbearbeiter (z.B. IT-Provider) handelt es sich um eine (natürliche oder juristische) Person, die im Auftrag des Verantwortlichen, also dem Verein, Personendaten bearbeitet. Eine derartige Auslagerung von Bearbeitungstätigkeiten ist möglich, wenn die Daten so bearbeitet werden, wie der Verantwortliche es selbst tun dürfte und wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. Es empfiehlt sich, in derartigen Konstellationen einen schriftlichen Auftragsbearbeitungsvertrag abzuschliessen und die jeweiligen Pflichten klar zu definieren.

Ein eigenständiger Verantwortlicher (z.B. Dachverband) bearbeitet die Personendaten in Abgrenzung zum Auftragsbearbeiter nicht im Auftrag des Verantwortlichen, sondern zu eigenen

neuen Zwecken. Diesfalls ist jeder Verantwortliche selbst für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. In den Verträgen mit eigenständigen Verantwortlichen empfiehlt sich festzuhalten, dass sich die Parteien an die einschlägigen Datenschutzvorschriften halten müssen.

5) Was muss bei der Verwendung von Clouddiensten beachtet werden? (z.B. Google Drive, Clubdesk, etc.)?

Hier braucht es eine Einzelfallanalyse, deren Resultat vom jeweiligen Dienst abhängt. Es geht jedoch letztlich um die gleichen vier Themenbereiche (siehe Frage 3), da es sich dabei um eine Weitergabe von Personendaten handelt.

Da sich die meisten Cloudanbieter im Ausland befinden, ist insbesondere der Auslandsbezug zu beachten. Hierbei sollten Sie die zur Verfügung gestellten Unterlagen des Anbieters prüfen, vor allem, ob die jeweiligen Server sich im Ausland befinden und welche Garantien vorgesehen sind, falls es sich dabei um ein Empfängerland ohne angemessenes Datenschutzniveau handelt. Diese Informationen sind anschliessend in Ihrer Datenschutzerklärung zu ergänzen.

Im Zusammenhang mit Cloud-Anwendungen sind zudem folgende Hinweise zu beachten:

- Verwenden Sie immer die Businessversionen der Clouddienste, denn diese sind eher auf Nutzende ausgerichtet, die Personendaten Dritter bearbeiten und dem Datenschutzgesetz unterliegen.
- Einige Anbieter bieten die Möglichkeit, dass Daten nur im EWR bearbeitet werden. Von dieser Option sollten Sie Gebrauch machen.
- Die datenschutzrelevanten Dokumente sollten sorgfältig gelesen werden, bevor Sie sie akzeptieren, insbesondere den Auftragsbearbeitungsvertrag (in Englisch «Data Processing Agreement»).
- Es ist zu prüfen, wo sich die Server befinden. Dies sollte aus den Unterlagen des Anbieters entnommen werden können.
- Es ist zu prüfen, ob die Datensicherheit gewährleistet ist, bzw. ob der Anbieter vertrauenswürdig ist, beispielsweise indem er über Datenschutzzertifizierungen verfügt.
- Bei Unklarheiten empfehlen wir, einen Experten beizuziehen.

6) In unserem Verein werden unzählige WhatsApp-Chats eingesetzt. Welche datenschutzrechtlichen Bestimmungen gilt es zu beachten? Gibt es Verhaltensempfehlungen für Gruppen-Administrator:innen?

Es existieren zwei verschiedene WhatsApp-Applikationen. Namentlich gibt es neben der gewöhnlichen «WhatsApp»-Applikation die «WhatsApp Business»-Applikation. Diese ist im Gegensatz zum

gewöhnlichen Messenger auf Unternehmen ausgerichtet, folglich auf Personen, die dem Datenschutzgesetz unterliegen. Aufgrund dieses Umstands ist zunächst darauf hinzuweisen, dass Vereine und Verbände die Business-Version herunterladen und diese verwenden sollten, damit sie ihren datenschutzrechtlichen Verpflichtungen gegenüber ihren Mitgliedern nachkommen können. Diese Version funktioniert technisch wie der gewöhnliche Messenger, und es ist auch möglich, bisherige WhatsApp-Chats in die WhatsApp Business App zu überführen.

In den «[WhatsApp Business Nutzungsbedingungen](#)» wird unter anderem auf die «WhatsApp Business Datenverarbeitungsbedingungen» verwiesen. Diese stellen rechtlich einen Auftragsdatenbearbeitungsvertrag dar und gelten, sofern WhatsApp die vom Verein zur Verfügung gestellten Personendaten (bspw. Telefonnummern der Mitglieder) als Auftragsbearbeiter bearbeitet. Folglich liegt vorliegend eine Weitergabe von Personendaten vor und es sind die entsprechenden Regeln zu beachten (vgl. Ausführungen unter Fragen 3 und 4).

Prüfschema

Prüfschritte	Erklärung	To do
1. Grundsätze	Bei der Weitergabe von Personendaten handelt es sich um eine Bearbeitungstätigkeit. Folglich sind sämtliche Bearbeitungsgrundsätze einzuhalten, insb. Zweckgebundenheit und Verhältnismässigkeit.	In der Datenschutzerklärung ist darauf hinzuweisen, dass die zur Verfügung gestellten Personendaten zum Zweck der Organisation des Vereinsalltags bearbeitet und an einen Messenger-Dienst übermittelt werden. Im Sinne der Verhältnismässigkeit und falls dies zur Organisation genügt, sollte von der Funktion Gebrauch gemacht werden, wonach nur der Verein selbst Nachrichten schreiben kann. Auch ist darauf zu achten, dass nicht mehr Informationen als nötig zur Zweckerreichung übermittelt werden.

<p>2. Auslandsbezug</p>	<p>WhatsApp hält im Rahmen seiner «Datenverarbeitungsbedingungen» fest, dass Personendaten auch ins Ausland, insb. dem EWR und die USA übermittelt werden können und dass auch sog. Unterauftragsbearbeiter engagiert werden können, welche sich ebenfalls im Ausland befinden (vgl. die zur Verfügung gestellte Liste der «Unterauftragsverarbeiter», welche insbesondere die USA, Dänemark, Schweden und Irland umfasst).</p> <p>Im Dokument «Ergänzung für WhatsApp Business Datenübermittlungen» wird sodann festgehalten, dass WhatsApp für die Übermittlung von Personendaten in Länder ohne angemessenen Datenschutz Standardvertragsklauseln verwendet.</p>	<p>In der Datenschutzerklärung ist festzuhalten, dass Personendaten auch ins Ausland übermittelt werden, namentlich in die USA, Dänemark, Schweden, Irland. Für die Übermittlung in die USA gelten die Standardvertragsklauseln als Garantie.</p>
<p>3. Art der Personendaten</p>	<p>Die Übermittlung von besonders schützenswerten Personendaten an Dritte stellt eine Persönlichkeitsverletzung dar, welche gerechtfertigt werden muss.</p>	<p>Verzichten Sie auf die Übermittlung von besonders schützenswerten Personendaten via WhatsApp.</p>
<p>4. Beziehung zwischen den Parteien</p>	<p>WhatsApp bearbeitet die Personendaten der Nutzer als Auftragsbearbeiter – die entsprechenden Verträge/Nutzungsbedingungen müssen beim Herunterladen der App akzeptiert werden.</p>	<p>Keine weiteren Vorkehrungen erforderlich.</p>

Einwilligung

Die Einwilligung ist einer von drei Rechtfertigungsgründen, welche vorausgesetzt werden zur Rechtfertigung von Persönlichkeitsverletzungen. Eine Einwilligung ist somit nur erforderlich, wenn eine Persönlichkeitsverletzung gegeben ist und kein anderer Rechtfertigungsgrund vorliegt. Neben der

Einwilligung gelten das überwiegende private oder öffentliche Interesse sowie gesetzliche Bestimmungen als Rechtfertigungsgründe.

Eine Persönlichkeitsverletzung ist gegeben, wenn Personendaten wie folgt bearbeitet werden:

- Personendaten werden entgegen den allgemeinen Grundsätzen (*Rechtmässigkeit, Treu & Glauben, Erkennbarkeit, Zweckbindung, Verhältnismässigkeit, Speicherbegrenzung, Richtigkeit, Datensicherheit*) bearbeitet.
- Personendaten werden entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet.
- Dritten werden besonders schützenswerte Personendaten bekanntgegeben.

In allgemeiner Hinsicht ist die Einwilligung stets mit organisatorischem Aufwand verbunden und kann von der einwilligenden Person jederzeit zurückgezogen werden. Entsprechend ist es meist nicht ratsam, eine Persönlichkeitsverletzung mittels Einwilligung zu rechtfertigen.

7) Ist es zulässig, ein Einverständnis einmalig abzuholen, so dass nicht bei jedem Mal wieder separat nachgefragt werden muss?

Nein. Eine Einwilligung muss immer für eine oder mehrere **bestimmte** Bearbeitungen erfolgen. Eine pauschale Einwilligung für sämtliche möglichen Bearbeitungstätigkeiten ist daher nicht möglich. Darüber hinaus kann eine Einwilligung nur nach angemessener Information gültig erteilt werden. Auch dies verunmöglicht eine pauschale Einwilligung. Eine einmalige Einwilligung für mehrere Bearbeitungen ist nur zulässig, sofern diese Bearbeitungen genügend eingegrenzt werden können, so dass für die betroffene Person zweifelsfrei ersichtlich und bestimmt ist, in welche Bearbeitungstätigkeiten sie einwilligt.

Der guten Ordnung halber sei erneut darauf hingewiesen, dass eine Einwilligung nur selten erforderlich sein sollte. Namentlich ist sie nur erforderlich, wenn eine Persönlichkeitsverletzung gegeben ist, die nicht durch Gesetz oder überwiegende Interessen gerechtfertigt ist.

8) Was ist im Zusammenhang mit Kindern und Jugendlichen zu beachten? Inwiefern sind die Eltern einzubeziehen?

Das Datenschutzgesetz unterscheidet grundsätzlich nicht zwischen Kindern und Erwachsenen. Handelt es sich aber um ein Kind, sollte die Kommunikation angepasst werden. So sollte bei der Erfüllung der Informationspflicht auf eine einfache Sprache geachtet werden.

Sollte eine Einwilligung notwendig sein, gilt, dass Kinder selbst einwilligen können, sofern sie urteilsfähig sind, d.h. sofern sie die Tragweite der Einwilligung verstehen. Als durch die Rechtsprechung

entwickelter Richtwert gilt, dass ab einem Alter von 13 Jahren von der Urteilsfähigkeit ausgegangen werden kann, vorausgesetzt, es sind keine Indizien gegeben, welche gegen die Urteilsfähigkeit sprechen (bspw. kognitive Einschränkungen). Unter 13 Jahren sollte deshalb die Einwilligung der Eltern eingeholt werden. Hier ist wiederum zu beachten, dass eine Einwilligung nur für bestimmte Bearbeitungstätigkeiten und nach angemessener Information erfolgen kann.

9) Jahresberichte für die GV: Muss von Personen eine Einwilligung eingeholt werden, wenn Sie darin erwähnt sind?

Wie bereits ausgeführt, ist eine Einwilligung der betroffenen Personen nur erforderlich, sofern eine Persönlichkeitsverletzung vorliegt, welche nicht durch einen anderen Rechtfertigungsgrund gerechtfertigt ist.

Sofern vorliegend eine Persönlichkeitsverletzung gegeben wäre, wäre eine solche entweder durch das Gesetz gerechtfertigt, da dieses die Verfassung von Jahresberichten und deren Aufbewahrung vorsieht oder ggf. durch das überwiegende Interesse des Vereins.

10) Wir haben bis jetzt eine Liste mit Namen, Adresse, Mail, Telefon, Geburtsdatum aller Mitglieder an jedes Mitglied verteilt / gemailt. Ist das weiterhin zulässig? Wenn nein, kann eine spezielle Bewilligung von den Mitgliedern eingeholt werden?

Bei dieser Frage sind insbesondere die Grundsätze der Zweckgebundenheit und der Verhältnismässigkeit zu beachten. Namentlich ist darauf zu achten, dass der Zweck der Übermittlung der erwähnten Liste in der Datenschutzerklärung ersichtlich ist und dass nicht mehr Informationen weitergegeben werden als zur Zweckerreichung notwendig.

Sofern die Übermittlung den erwähnten Datenbearbeitungsgrundsätzen widerspricht, stellt sie eine Persönlichkeitsverletzung dar, welche durch einen Rechtfertigungsgrund gerechtfertigt werden kann, wie beispielsweise mittels Einwilligung.

- 11) Im [Podcast](#) wird erwähnt, dass die Einwilligung für die Bearbeitung der Daten (z.B. Aufnahme in einen WhatsApp-Chat) nicht von der Aufnahme in den Verein abhängig gemacht werden darf. In der Praxis würde dies zu Mehraufwand führen, da dieser Kommunikationskanal nicht mehr alle Mitglieder erreichen würde. Es ist nicht realistisch, bestimmte Personen jeweils separat noch anzuschreiben bzw. zu informieren. Was empfehlen Sie?

Bitte beachten Sie, dass für die Aufnahme in den Chat nicht in jedem Fall eine Einwilligung erforderlich ist (vgl. Ausführungen unter der Frage 5).

Sofern eine Person dem Chat nicht beitreten möchte oder von diesem austritt, ist eine andere Lösung zu finden. Namentlich hat eine Einwilligung immer freiwillig zu erfolgen, d.h. ohne Druck oder Zwang. Andernfalls wäre die Einwilligung nicht rechtsgültig. Es bleibt nichts anderes übrig, als einen alternativen Kommunikationskanal anzubieten.

Informationspflicht

- 12) Ist das Inventar/Verzeichnis der Bearbeitungstätigkeit ein internes oder öffentliches Dokument?

Das Bearbeitungsverzeichnis ist ein internes Dokument, welches jedoch im Falle einer Überprüfung von der zuständigen Datenschutzaufsichtsbehörde, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), eingesehen werden kann.

Die Erstellung eines Bearbeitungsverzeichnisses ist nur bei Organisationen obligatorisch, die mindestens 250 Mitarbeitende beschäftigen (Personen, die in einem Anstellungsverhältnis zum Verein stehen) oder welche in grossem Umfang besonders schützenswerte Personendaten bearbeiten oder Profiling mit hohem Risiko durchführen. In der Regel sind kleine und mittlere Sportvereine folglich nicht von dieser Pflicht erfasst.

Trotzdem empfiehlt es sich ein Verzeichnis bzw. Inventar der Bearbeitungstätigkeiten des Vereins zu erstellen, denn ein solches dient als Grundlage für die Implementierung aller weiteren Massnahmen zur Einhaltung des Datenschutzgesetzes. Es ist ein sehr gutes Werkzeug, um einen Überblick über die Bearbeitungen von Personendaten im Verein zu erhalten und auf dieser Basis die notwendigen Dokumente zu erstellen (z.B. Datenschutzerklärung) oder Auskunftsanfragen und Löschanträge zu bearbeiten.

13) Müssen Personen, die bereits vor der Revision in unserer Datenbank waren, direkt informiert werden? In welcher Form müsste das mindestens geschehen?

Die Informationspflicht gilt für sämtliche Bearbeitungstätigkeiten – unabhängig davon, wann die betroffenen Personen in die Datenbank aufgenommen wurden. Zudem ist darauf hinzuweisen, dass die Informationspflicht bereits vor der Revision des Datenschutzgesetzes galt.

Der betroffenen Person sind sämtliche Informationen mitzuteilen, die erforderlich ist, damit diese ihre Rechte geltend machen kann und um eine transparente Datenbearbeitung gewährleisten.

Dies umfasst mindestens:

- Identität und Kontaktdaten des Verantwortlichen (d.h. des Vereins)
- Bearbeitungszweck
- Allfällige Empfänger/Kategorien von Empfängern, denen Personendaten bekanntgegeben werden
- Kategorien der bearbeiteten Personendaten, sofern die Personendaten nicht bei der betroffenen Person beschafft werden
- Staat oder Organisation, sofern die Personendaten ins Ausland bekanntgegeben werden und gegebenenfalls die zusätzlichen Garantien.

Es gibt keine Formvorschriften, welche z.B. die Schriftlichkeit der Information voraussetzen. Die Informationspflicht wird in der Praxis aber meist durch eine Datenschutzerklärung (i.d.R. auf der Website) erfüllt. Wird die Datenschutzerklärung geändert, sollten die betroffenen Personen über die Änderung informiert werden, bspw. indem darauf hingewiesen wird, dass der Verein seine Datenschutzerklärung geändert hat und diese auf der Website ersichtlich ist.

In gewissen Situationen entfällt die Informationspflicht, insbesondere wenn:

- Die betroffene Person bereits über die Information verfügt
- Die Bearbeitung gesetzlich vorgesehen ist
- Der Verantwortliche einer gesetzlichen Geheimhaltungspflicht unterliegt
- Die Information nicht möglich ist oder einen unverhältnismässigen Aufwand erfordert und die Personendaten nicht bei der betroffenen Person beschafft werden.

14) Gehe ich richtig in der Annahme, dass die Datenschutzerklärung lediglich zur Kenntnis genommen werden muss?

Genau. Bei einer Datenschutzerklärung handelt es sich um eine einseitige Kommunikation. Es geht ausschliesslich darum, zu informieren. Eine Einwilligung oder Zustimmung zur Datenschutzerklärung ist nicht notwendig.

Speicherbegrenzung

15) Man soll die Daten nach Austritt aus dem Verein löschen. Ist das erlaubt, die Daten für das Vereinsarchiv zu behalten?

Bei der Aufbewahrung bzw. Löschung müssen vier Themengebiete beachtet werden: die Aufbewahrungspflicht, die Löschpflicht, das überwiegende Interesse und die Einwilligung.

1. Aufbewahrungspflicht

Das Gesetz sieht unterschiedliche Aufbewahrungspflichten für Dokumente und darin enthaltene Personendaten vor. Die wichtigste gesetzliche Aufbewahrungspflicht gilt für Geschäftsbücher, Geschäftsberichte und Buchungsbelege (10 Jahre). Entsprechend sollte man sich in diesem Zusammenhang stets die Frage stellen, ob eine gesetzliche Aufbewahrungspflicht besteht. Falls ja, müssen die Daten im Archiv bleiben.

2. Löschpflichten

Vorbehaltlich der erwähnten gesetzlichen Aufbewahrungspflichten dürfen Personendaten nur zu einem bestimmten, für die betroffene Person erkennbaren Zweck bearbeitet werden; sie dürfen nur so lange aufbewahrt werden, als der Zweck noch nicht erfüllt ist resp. noch erfüllt werden kann. Entsprechend sollte man sich in diesem Zusammenhang die Frage stellen, ob die Personendaten zur Zweckerreichung noch benötigt werden. Hier kann beispielsweise die Vereinshistorie als Zweck angegeben werden in der Datenschutzerklärung. Es sollte aber auch der Grundsatz der Verhältnismässigkeit beachtet werden. So stellt sich etwa die Frage, ob bspw. die Adresse der betroffenen Person für die Vereinshistorie relevant ist. Zudem ist es wichtig sicherzustellen, dass die gespeicherten Daten in Erfüllung des Grundsatzes der Datenrichtigkeit korrekt und aktuell sind; beispielsweise ist davon auszugehen, dass eine Wohnadresse, die vor 20 Jahren erfasst wurde, häufig nicht mehr aktuell ist

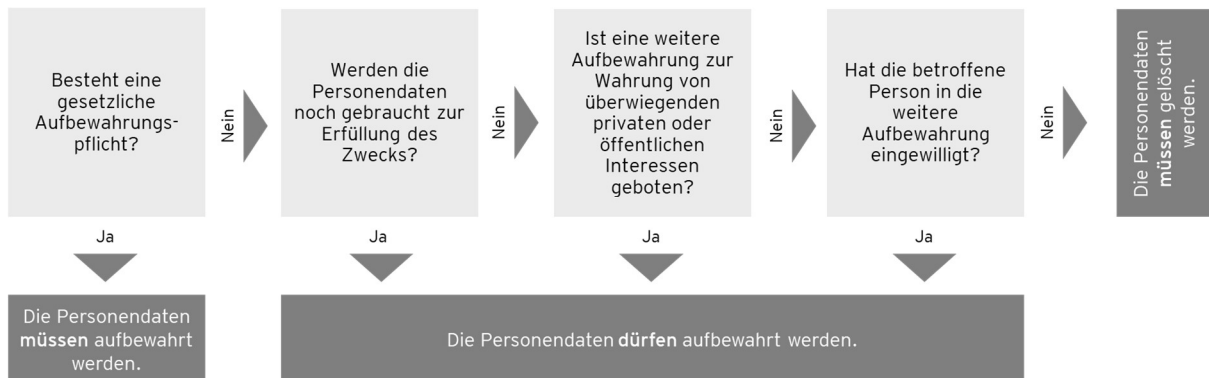
3. Überwiegendes Interesse

Die Aufbewahrung kann gegebenenfalls geboten sein, wenn überwiegende private oder öffentliche Interessen gegeben sind. Hier ist eine Interessenabwägung durchzuführen, in der das Interesse der betroffenen Person auf ihre Privatsphäre und ihr Selbstbestimmungsrecht hinsichtlich ihrer Personendaten den Interessen des Vereins gegenübergestellt werden. Es ist davon auszugehen, dass das Interesse des Vereins, für immer **alle** Daten einer Person aufzubewahren, nicht überwiegend ist.

4. Einwilligung

Eine Einwilligung kann eine weitere Aufbewahrung trotz grundsätzlicher Löschpflicht rechtfertigen. Folglich sollte man sich die Frage stellen, ob die betroffene Person in die Aufbewahrung über die Mitgliedschaft hinweg eingewilligt hat.

Überblick:



- 16) Wir dokumentieren wichtige Ereignisse zu einer Person. Beispiele sind Wettkampfergebnisse oder die Übernahme von Ämtern. Müssen auch solche Informationen bei Austritt gelöscht werden? Personen treten später gegebenenfalls wieder in den Verein ein. Sollte die Person später für langjährige Tätigkeit geehrt werden, fehlen nun relevante Informationen.**

Es gelten die gleichen Regeln, die unter Frage 15 erläutert wurden. Als Zweck für die weitere Aufbewahrung von Personendaten wird vorliegend die Führung von Wettkampfergebnissen genannt und das Dokumentieren von der Übernahme von Ämtern. Es ist davon auszugehen, dass dies ebenfalls unter den zulässigen Zweck der Vereinshistorie fällt, sofern weiterhin sämtliche Datenbearbeitungsgrundsätze eingehalten werden.

- 17) Gelten die Bestimmungen rückwirkend? Seit ca. 2 Jahren erwähnen wir bei Wettkampfanmeldungen, dass Daten in Ranglisten veröffentlicht werden und Bilder auf dem Wettkampfbereich zwecks Berichterstattung gemacht werden. Müsste älteres Material gelöscht werden?**

Hierbei sind zwei verschiedene Themengebiete zu unterscheiden:

Hinsichtlich der Ranglisten ist darauf hinzuweisen, dass die Informationspflicht schon vor der Revision des Datenschutzgesetzes bestand und für sämtliche Bearbeitungstätigkeiten gilt. Die Aufbewahrung stellt eine Datenbearbeitung dar und unterliegt folglich der Informationspflicht. Der Zweck der Erstellung von Ranglisten ist in der Datenschutzerklärung zu ergänzen. Grundsätzlich ist aber darauf

hinzuweisen, dass der Zweck bei diesem Beispiel bereits durch die Umstände ersichtlich ist – bei Wettkämpfen wird in der Regel auch eine Rangliste erstellt. Damit ist der Bearbeitungszweck ersichtlich und folglich entfällt grundsätzlich eine spezifische Informationspflicht. Trotzdem ist es ratsam, die eigene Datenschutzerklärung zu aktualisieren und dieses Thema aufzunehmen.

Im Zusammenhang mit den Fotos zwecks Berichterstattung ist zu erwähnen, dass dies einerseits den Datenschutz und andererseits das Recht am eigenen Bild berührt. Sofern auf dem Bild Personen mindestens bestimmbar sind, handelt es sich um Personendaten und es gilt das zuvor erläuterte. Zum Recht am eigenen Bild wird auf die Ausführungen unter dem Titel «Recht am eigenen Bild» verwiesen.

Schutzmassnahmen

18) Dürfen Personendaten per E-Mail versendet werden? Oder müssen spezielle Vorkehrungen getroffen werden (beispielsweise durch Verschlüsselung)? Gibt es dabei einen Unterschied zwischen «normalen» und «besonders schützenswerten» Personendaten?

Personendaten müssen durch geeignete technische und organisatorische Massnahmen gesichert sein. Was geeignet ist, hängt einerseits vom Risiko und Schutzbedarf der Personendaten ab. Dies beurteilt sich nach der Art der bearbeiteten Personendaten, dem Zweck, der Art, dem Umfang und der Umstände der Bearbeitung. Bei der Festlegung der technischen und organisatorischen Massnahmen werden andererseits auch der Stand der Technik und die Implementierungskosten berücksichtigt. Im Kontext einer gewöhnlichen Mitgliederliste ist der Schutzbedarf als eher gering einzustufen. Werden dagegen besonders schützenswerte Personendaten oder bspw. Kreditkarteninformationen versendet, so ist der Schutzbedarf höher. Damit kann festgehalten werden, dass bei einer gewöhnlichen Mitgliederliste mit Namen und Adressen keine Verschlüsselung notwendig sein sollte.

19) Dürfen Excel Listen mit Mitglieder Daten auf einem Passwort-geschützten PC aufgehoben werden? Gilt das als genügend geschützt?

Wenn es sich um nicht besonders schützenswerte Personendaten handelt und deren Schutzbedarf als gering einzustufen ist, sollte der Umstand, dass diese auf einem Passwort-geschützten Computer aufbewahrt werden, als Sicherheitsmassnahme genügen.

Haftung

20) Der Datenschutzverantwortliche haftet ja mit seinem Privatvermögen, wenn eine Datenschutzverletzung vorliegt und es eine Busse geben wird (die kann ja bis CHF 250'000 sein). Nun wollte ich fragen, wie wir dies umgehen können, denn so möchte ja niemand mehr Datenschutzverantwortlicher sein. Kann man das einfach in einer Vorstandssitzung definieren, dass der Verein die Busse und die Haftung übernehmen würde? So würde sich auch jemand zur Verfügung stellen.

Die Strafbestimmungen des Datenschutzgesetzes richten sich an die für die Datenschutzverletzung verantwortliche natürliche Personen. Bei dieser Person handelt es sich jedoch nicht um die für Datenschutz verantwortliche Person im Verein, sondern um diejenige Person, welche eine Datenschutzverletzung zu verantworten hat, und sich folglich strafbar gemacht hat, indem sie die mit Strafe bedrohten Pflichten nicht eingehalten hat. Die für die Datenschutzverletzung verantwortliche Person in einem Verein kann ein Mitglied des Vorstands sein, da diesen in der Regel die Pflicht obliegt, die Einhaltung der geltenden Gesetze durch den Verein sicherzustellen. Aber auch jemand, der nicht dem Vorstand angehört, aber dennoch den entsprechenden Prozess leitet, kann strafrechtlich verfolgt werden.

Die strafrechtlichen Bussen, die gegen die für die Datenschutzverletzung verantwortliche Person gerichtet sind, dürfen weder vom Verein selbst übernommen werden, noch sind sie versicherbar. Es ist wichtig anzumerken, dass nicht alle datenschutzrechtlichen Verpflichtungen mit Strafe bedroht sind. Strafbar sind insbesondere die **vorsätzliche** Verletzung von Informations- und Auskunftspflichten, von Mitwirkungspflichten mit dem EDÖB, der Grundsätze für Datentransfers ins Ausland sowie der Vorgaben zur Datensicherheit. Vorsätzlich handelt, wer mit Wissen und Wollen handelt resp. die Datenschutzverletzung für möglich hält und in Kauf nimmt. Darüber hinaus erfordert die strafrechtliche Verfolgung einen entsprechenden **Strafantrag** der betroffenen Person.

Recht am eigenen Bild

Das Recht am eigenen Bild besagt, dass jeder Mensch selbst darüber bestimmen darf, ob ein Bild von ihm aufgenommen wird und was damit geschieht. Daraus folgt, dass grundsätzlich bereits für die Aufnahme eines Bildes die Einwilligung der abgebildeten Person erforderlich ist. Die Einwilligung für eine Aufnahme kann formfrei erfolgen, somit auch konkludent. Wenn also jemand ausdrücklich für ein Foto posiert, kann davon ausgegangen werden, dass er in die Aufnahme des Fotos eingewilligt hat. Wenn das Foto auf der Website publiziert werden soll, muss die betroffene Person über diese Absicht

informiert werden und ihre Einwilligung dazu geben. Hierzu gibt es aber zwei wichtige Ausnahmen.

Namentlich ist keine Einwilligung erforderlich, wenn:

- Die abgebildete Person als Teil der Landschaft, der Umgebung oder des Ereignisses erscheint, z.B. bei öffentlichen Sportveranstaltungen, bei der viele Leute abgebildet sind. Diese Ausnahme greift allerdings nur, wenn keine Person besonders hervorgehoben bzw. isoliert wird.
- Die abgebildete Person eine sog. Person der Zeitgeschichte ist (z.B. prominente Profisportler wie Marco Odermatt oder Roger Federer).

Wenn keine Ausnahme greift, ist grundsätzlich eine Persönlichkeitsverletzung gegeben. Diese kann aber gerechtfertigt werden durch:

- **Gesetzliche Grundlagen**
- **Höherrangige überwiegende Interessen des Vereins/Verbands**

Dies kann zum Beispiel das Interesse beinhalten, die Gewinnerinnen und Gewinner eines Wettkampfes darzustellen. Dabei ist jedoch Vorsicht geboten. Man kann nicht pauschal ein höher-rangiges Interesse annehmen. Es sollte eine Abwägung zwischen dem berechtigten Interesse des Vereins und dem Interesse der betroffenen Person stattfinden: Welches Interesse wiegt schwerer – das der abgebildeten Person, die das Recht hat zu bestimmen, was mit ihrem Foto geschieht, oder das Interesse des Vereins an der Aufnahme bzw. Veröffentlichung? Im Zweifelsfall wird empfohlen, eine Einwilligung einzuholen.

Der guten Ordnung halber ist darauf hingewiesen, dass sofern einzelne Personen auf einem Bild mindestens bestimmbar sind, es sich dabei um Personendaten handelt und entsprechend sämtliche Regeln des Datenschutzes einzuhalten sind.

21) Kann eine generelle Einverständniserklärung für die Aufnahme und Veröffentlichung von Fotos eingeholt werden?

Nein. Eine pauschale Einwilligung in alle möglichen künftigen Aufnahmen und Veröffentlichungen, beispielsweise im Beitrittsblatt, ist nicht möglich. Eine Einwilligung muss immer für bestimmte Bearbeitungstätigkeiten erfolgen. Eine einmalige Einwilligung für mehrere Aufnahmen und Veröffentlichungen ist nur zulässig, sofern diese genügend eingegrenzt werden können, so dass für die betroffene Person zweifelsfrei ersichtlich und bestimmt ist, in welchen Situationen von ihr Aufnahmen gemacht und publiziert werden dürfen. Die Einwilligung kann formfrei erfolgen (z.B. mündlich, schriftlich, durch Nicken oder auch konkludent). Der guten Ordnung halber wird darauf hingewiesen, dass nicht in jedem Fall eine Einwilligung tatsächlich notwendig ist (vgl. vorangehende einleitende Bemerkungen unter dem Titel «Recht am eigenen Bild»).

22) Wenn ein Vereinsmitglied keine Veröffentlichung von Fotos/Video/Ton wünscht, müssen dann bereits bestehende Dokumente gelöscht werden, auch wenn sie nur aufbewahrt werden?

Zunächst ist vorliegend zu prüfen, ob die abgebildete Person lediglich der Veröffentlichung oder auch der Aufbewahrung widersprochen hat. Ist nur ersteres der Fall, so kann das Bild weiterhin aufbewahrt werden. Hat die betroffene Person auch der Aufbewahrung widersprochen resp. wünscht sie die Löschung, ist dieser Wunsch grundsätzlich zu respektieren, z.B. indem die Personen aus den Bildern herausgeschnitten werden oder durch Verpixelung oder Retouchierung unkenntlich gemacht werden, andernfalls liegt eine Persönlichkeitsverletzung vor. Eine solche kann gerechtfertigt sein durch Gesetz oder überwiegende Interessen. Vergleichen Sie hierzu die allgemeinen Ausführungen unter dem Titel «Recht am eigenen Bild».

Diverses

23) Gilt die Erhebung der genutzten Krankenkasse als besonders schützenswert?

Nein. Der Begriff der besonders schützenswerten Personendaten ist im Gesetz abschliessend definiert und umfasst:

- Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten
- Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie
- Genetische Daten
- Biometrische Daten, die eine natürliche Person eindeutig identifizieren
- Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen
- Daten über Massnahmen der sozialen Hilfe.

erstellt mit Unterstützung der Datenschutz-Experten von Ernst & Young AG