**Datenschutz im Verein: die zwölf wichtigsten Fragen** (HI2326697)

**Zusammenfassung**

Auch wenn man anderes vermuten könnte: Datenschutz schützt Menschen, nicht Daten. Menschen sollen geschützt werden vor falschem oder fahrlässigem Umgang mit Daten, die sie betreffen. Dadurch sollen sie vor Schäden, Missbrauch und Manipulation bewahrt werden.

Im Übrigen ist es ein Grundrecht zu wissen, wer welche Angaben wann über einen kennt. Deshalb gewährt Datenschutz unter anderem auch Korrektur- und Einspruchsrechte.

Besondere Brisanz erhält das Thema Datenschutz auch durch die gesetzliche Neuordnung: Zum 25. Mai 2018 tritt in allen EU-Mitgliedstaaten die EU-Datenschutz-Grundverordnung (DSGVO) in Kraft.[1] Mit ihr erhöhen sich die Anforderungen an Vereine und alle anderen Datenverarbeiter. Bei Nichtbeachtung können Bußgelder in Höhe von bis zu 20 Mio. Euro drohen.

**Die 7 häufigsten Fallen**

**1. Den Kopf in den Sand stecken – "Es wird schon nichts passieren"**

Das Thema Datenschutz aussitzen zu wollen, ist keine gute Idee. Jeder Datenverarbeiter muss sich eine Strategie überlegen, wie er die (neuen) gesetzlichen Anforderungen des Datenschutzrechts umsetzen kann. Diese Umsetzung muss er auch belegen können (Stichwort "Rechenschaftspflicht"). Die Datenschutz-Aufsichtsbehörden besitzen das Recht, dies zu überprüfen.

**2. Keine Datenschutz-Organisation**

Jede Stelle, die personenbezogene Daten verarbeitet, muss sich mit den Datenschutz-Anforderungen proaktiv auseinandersetzen und eine entsprechende Organisation aufbauen: Die Daten sind auf organisatorischer und technischer Ebene wirkungsvoll zu schützen. Die Mitarbeiter müssen Bescheid wissen, was sie mit Daten tun dürfen und was nicht. Es sollte entsprechende Prozessbeschreibungen, Handlungs- oder Arbeitsanweisungen geben. Es ist sicherzustellen, dass der Datenschutzbeauftragte, wenn es einen gibt, in alle Datenschutzfragen eingebunden wird.

**3. Betroffene werden nicht informiert**

Immer wenn der Verein personenbezogene Daten erhebt (z. B. bei der Entscheidung über einen Mitgliedschaftsantrag), müssen die davon Betroffenen informiert werden (Art. 13 und 14 DSGVO). Das Gesetz sieht eine Reihe von Pflichtangaben vor, u. a. etwa, welche Daten zu welchem Zweck erhoben werden, wie lange sie gespeichert werden, an wen die Daten ggf. weitergegeben werden, wo sich die Betroffenen beschweren können, welches die zuständige Aufsichtsbehörde ist. Diese Informationen können über ein zusätzliches Formblatt oder eine Internetseite mitgeteilt werden.

**4. Kein Datenschutzbeauftragter bestellt**

Immer wenn die gesetzlichen Voraussetzungen für die Bestellung eines Datenschutzbeauftragten vorliegen, muss eine Person dazu ernannt werden. In allen anderen Fällen sollte überlegt werden, ob ein Datenschutzbeauftragter auf freiwilliger Basis bestellt wird.

**5. Auftragsverarbeitung ohne datenschutzrechtliche Vereinbarung**

Wenn ein Dienstleister beauftragt wird und er Einblick in personenbezogene Daten erhält (z. B. IT-Systemadministrator, Cloud-Anbieter, Callcenter), muss mit diesem eine datenschutzrechtliche Vereinbarung im Sinne des Art. 28 DSGVO abgeschlossen werden. Darin sind eine Reihe von Punkten zu regeln, die den Umgang und den Schutz der personenbezogenen Daten festlegen.

**6. Keine Meldung nach einer Datenpanne**

Falls der Schutz von personenbezogenen Daten beeinträchtigt wird, muss dies der Datenschutz-Aufsichtsbehörde und in manchen Fällen auch den Betroffenen mitgeteilt werden. Das ist der Fall, wenn etwa die Mitgliederdatenbank gehackt wird oder auch schon dann, wenn eine E-Mail oder ein Fax mit personenbezogenen Daten aus Versehen an einen falschen Adressaten geschickt wird.

**7. Datenschutz-Folgenabschätzung wird nicht durchgeführt**

Wenn personenbezogene Daten auf risikoreiche Art und Weise verarbeitet werden (z. B., weil eine neue Technologie zum Einsatz kommt oder besonders große Datenmengen verarbeitet werden), ist vorab eine Folgenabschätzung durchzuführen. Sie besteht in einer Bewertung und Dokumentation der Datenverarbeitung, der Zwecke und der Risiken. Können die Datenschutzrisiken nicht vorab gemildert werden, muss zwingend die Datenschutz-Aufsichtsbehörde eingeschaltet werden.

**1 Welche Vereine müssen die Datenschutzregeln beachten?** (HI11406684)

Grundsätzlich alle – und zwar ohne Ausnahme. Denn die DSGVO trifft EU-weit Vorgaben für alle Stellen, die personenbezogene Daten verarbeiten, egal welcher Rechtsform oder Größe. Nur private und familiäre Datenverarbeitungen fallen nicht darunter.

Daran schließt sich die Frage an, wann Daten personenbezogen sind? Personenbezogen sind sie immer dann, wenn sie sich auf eine identifizierte oder identifizierbare Person beziehen. Im Verein betrifft das vor allem Mitglieder (mit Angaben etwa zur Adresse, Mitgliedsnummer, zum Mitgliedskonto, Fotos), es fallen aber auch Mitarbeiter und Helfer aller Art darunter (etwa mit Angaben zur Funktion im Verein, betreute Mitglieder, Aufwandsentschädigung oder Gehaltsgruppe, Art der Tätigkeit und Einsatzgebiete, Sozialversicherungsnummer, Urlaubstage, Anzahl der Kinder, Schwerbehinderung etc.), oder auch Kunden und (Geschäfts-)Partner (etwa mit Anschrift, Telefonnummer, Arbeitgeber, Interessen).

Nicht personenbezogen sind dagegen Angaben über juristische Personen, also z. B. die Anschrift oder Kontoverbindung einer GmbH oder AG – wenn solche Daten verarbeitet werden, müssen die Datenschutzgesetze nicht beachtet werden.

**2 Wer im Verein ist zuständig für den Datenschutz?** (HI11406685)

Letztlich verantwortlich für die Einhaltung aller gesetzlichen Regelungen und damit auch der Datenschutzvorgaben ist immer der gesetzliche Vertreter, im Verein also der **Vorstand.** Er muss eine Organisation schaffen, um den Datenschutz systematisch und strukturell umzusetzen. Dass eine solche Organisation besteht, muss auch nachgewiesen werden können (etwa durch Dokumente und Protokolle). Dies stellt Art. 5 Abs. 2 DSGVO fest ("Rechenschaftspflicht").

Der Vorstand kann (und in einigen Fällen: muss) einen Datenschutzbeauftragten bestellen, der ihn bei der praktischen Durchführung dieser Vorgaben unterstützt.

**2.1 In welchen Fällen muss ein Datenschutzbeauftragter bestellt werden?** (HI11406686)

Ein Verein *muss* einen Datenschutzbeauftragten bestellen, wenn mindestens eine der folgenden Voraussetzungen erfüllt ist:

* Wenn in der Regel **mindestens zehn Personen** ständig mit der automatisierten Verarbeitung von personenbezogenen Daten im Verein beschäftigt sind (§ 38 Bundesdatenschutzgesetz in der Fassung ab dem 25.05.2018, welches die DSGVO in Deutschland ergänzt).

Was bedeutet das?

Wenn personenbezogene Daten regelmäßig durch zehn oder mehr Mitarbeiter oder Mitglieder mithilfe von Computern oder der IT verarbeitet werden, muss zwingend ein Datenschutzbeauftragter bestellt werden. Eine Verarbeitung von personenbezogenen Daten findet typischerweise in den Bereichen Mitgliederverwaltung, Buchhaltung, Gruppenleiter statt. Auch in vielen anderen Bereichen sind Datenverarbeitungen denkbar. So gilt etwa das bloße Abrufen von personenbezogenen Daten ebenfalls als Verarbeitung (z. B. die Benutzung der Mitgliederdatenbank).

Auf welche Art und Weise die Personen bei der Datenverarbeitung an den Verein gebunden sind (etwa als Angestellte, Ehrenamtliche oder Praktikanten), spielt dagegen keine Rolle. Entscheidend ist vielmehr, ob die Personenzahl über einen längeren Zeitraum über zehn gehalten wird.

**Achtung**

**Anzahl der Mitarbeiter ist entscheidend**

Es kommt somit nicht auf die Anzahl der Vereinsmitglieder an, sondern auf die Anzahl der Personen mit Zugriff auf die personenbezogenen Daten und somit indirekt auf die Größe der Vereinsorganisation.

* Wenn die Kerntätigkeit des Vereins darin besteht, die betroffenen Personen **regelmäßig und systematisch zu überwachen**, ist unabhängig von der Vereinsgröße ein Datenschutzbeauftragter zu ernennen (Art. 37 Abs. 1 Buchst. b DSGVO). Dieses Kriterium ist beispielsweise bei Wirtschaftsvereinen erfüllt, die Bonitätsprüfungen durchführen.
* Wenn die Kerntätigkeit des Vereins in der umfangreichen Verarbeitung von **"besonderen Kategorien personenbezogener Daten"** besteht, ist ebenfalls immer ein Datenschutzbeauftragter zu bestellen. Das Gesetz definiert die besonderen Kategorien in Art. 9 DSGVO als Angaben über die

◦ rassische und ethnische Herkunft,

◦ politischen Meinungen,

◦ religiösen oder weltanschaulichen Überzeugungen,

◦ Gewerkschaftszugehörigkeit,

◦ genetischen Daten,

◦ biometrischen Daten, soweit sie zur eindeutigen Identifizierung einer Person verwendet werden,

◦ Gesundheitsdaten,

◦ Daten zum Sexualleben oder der sexuellen Orientierung.

Wenn die Verarbeitung solcher Daten zur Kerntätigkeit des Vereins gehört (z. B. bei Selbsthilfegruppen oder Sportvereinen, die Verletzungen speichern), dann muss ebenfalls zwingend ein Datenschutzbeauftragter bestellt werden (Art. 37 Abs. 1 Buchst. c DSGVO).

* Darüber hinaus muss ein Datenschutzbeauftragter auch bestellt werden, wenn der Verein eine Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO durchführen muss, weil die Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen aufweist (§ 38 Abs. 1 Satz 2 BDSG-neu).

Wenn keiner dieser Fälle zutrifft, sind dennoch alle anderen Vorschriften der Datenschutzgesetze zu beachten und einzuhalten. Deshalb kann es unter Umständen trotzdem Sinn ergeben, freiwillig einen Datenschutzbeauftragten zu bestellen, um den Vorstand zu entlasten. Auch ist der Aufbau einer eigenen Datenschutzkompetenz innerhalb des Vereins sinnvoll, um die Pflichten besser einschätzen und sich rechtstreu verhalten zu können.

**2.2 Welche Aufgaben hat ein Datenschutzbeauftragter?** (HI11406687)

Der Datenschutzbeauftragte hat die Aufgabe, die Einhaltung des Datenschutzes zu "überwachen" (Art. 39 DSGVO). Aber: Er darf selber keine Arbeitsanweisungen geben – dies bleibt dem Vorstand oder den Vorgesetzten vorbehalten. Der Datenschutzbeauftragte hat vielmehr zu kontrollieren, ob es Anweisungen zur Einhaltung des Datenschutzes gibt und ob diese beachtet werden. Darunter fällt auch die Kontrolle, ob Zuständigkeiten zugewiesen wurden.

Darüber hinaus besitzt der Datenschutzbeauftragte folgende gesetzliche Aufgaben:

* Unterrichtung und Beratung des Vorstands und der Mitarbeiter über die Datenschutzvorschriften und -pflichten
* Sensibilisierung und Schulung der Mitarbeiter (wobei der Datenschutzbeauftragte dies nur sicherstellen, aber nicht zwangsläufig selber schulen muss)
* Im Fall einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO): eine datenschutzrechtliche Beurteilung des Sachverhalts abgeben
* Anlaufstelle für die Datenschutz-Aufsichtsbehörde (z. B. bei Fragen und Nachforschungen der Behörde)
* Zusammenarbeit mit der Datenschutz-Aufsichtsbehörde.

**2.3 Welche Voraussetzungen muss ein Datenschutzbeauftragter mitbringen?** (HI11406688)

Zum Datenschutzbeauftragten darf nur eine Person bestellt werden, welche die "berufliche Qualifikation" und "insbesondere das Fachwissen" besitzt. Zudem muss sie in jeder Hinsicht die Fähigkeit besitzen, um die ihr zugewiesenen Aufgaben erfüllen zu können (Art. 37 Abs. 5 DSGVO).

Damit meint das Gesetz: Die Person muss Kenntnisse besitzen im Datenschutzrecht und in der Datenschutzpraxis. Diese richten sich nach den Umständen: Je sensiblere Daten der Verein verarbeitet, desto tiefer gehende Fachkenntnisse muss der Beauftragte besitzen. Außerdem benötigt er die soziale Kompetenz, um ins Gespräch kommen zu können.

Aus dem Gesetz ergibt sich allerdings auch: Mitarbeiter in Leitungsfunktionen dürfen nicht als Datenschutzbeauftragte ernannt werden. Denn das würde zu einem Interessenskonflikt führen, wenn sie sich selbst kontrollieren müssten.

**Achtung**

**Datenschutzbeauftragter darf kein leitender Mitarbeiter sein**

Nicht als Datenschutzbeauftragte bestellt werden dürfen daher insbesondere Vorstände, besondere Vertreter und Beiratsmitglieder, Geschäftsführer, Revisoren, Kassenwart und -prüfer.

Übrigens darf zum Beauftragten für den Datenschutz auch ein externer Dienstleister bestellt werden (Art. 37 Abs. 6 DSGVO); es muss sich nicht zwangsläufig um ein Vereinsmitglied handeln.

**2.4 Welche Stellung hat ein Datenschutzbeauftragter?** (HI11406689)

Der Datenschutzbeauftragte handelt weisungsfrei. Der Vorstand oder andere Personen dürfen ihm nicht vorschreiben, wie und wann er zu handeln hat (Art. 38 Abs. 3 DSGVO). Wegen der Erfüllung seiner Aufgaben darf er nicht benachteiligt werden.

Der Vorstand und andere Verantwortliche sind verpflichtet, den Datenschutzbeauftragten frühzeitig in alle Fragen einzubinden, die mit dem Schutz von personenbezogenen Daten zusammenhängen.

Seine Erkenntnisse und Hinweise muss der Datenschutzbeauftragte unmittelbar der höchsten Managementebene, also dem Vorstand, berichten.

**3 In welchen Fällen muss man an Datenschutz denken?** (HI11406690)

Wann greifen denn eigentlich alle diese datenschutzrechtlichen Vorgaben? Das ist dann der Fall, wenn mit personenbezogenen Daten umgegangen wird. Im rechtlichen Sinn liegt eine Datenverarbeitung vor, wenn personenbezogene Daten erhoben, erfasst, gespeichert, verwendet, geordnet, angepasst, verändert, ausgelesen, abgefragt, offengelegt, verbreitet, bereitgestellt, abgeglichen, verknüpft, eingeschränkt, gelöscht, vernichtet werden oder wenn mit ihnen auf eine andere Weise umgegangen wird – und das ist quasi immer der Fall, wenn man irgendetwas mit personenbezogenen Daten macht. Eine Unterscheidung zwischen elektronischer Datenverarbeitung und Datenverarbeitung auf Papier gibt es nicht.

**Praxis-Beispiel**

**Datenverarbeitungen sind zum Beispiel:**

* Speichern der Stammdaten eines Mitglieds;
* Veröffentlichungen auf der Internetseite des Vereins, z. B. von Fotos;
* Veröffentlichungen in der Vereinszeitung, z. B. Jubiläen (Geburtstag oder Mitgliedschaft);
* Weitergabe von personenbezogenen Daten an übergeordnete Organisationen, z. B. Meldungen und Mitteilungen an den Landessportbund zur Vergabe von Sportabzeichen und Ehrungen;
* Weitergabe von Mitgliederdaten an Dritte;
* Sonstige Veröffentlichungen von personenbezogenen Daten, zum Beispiel Meldungen und Mitteilungen an Sport-Fachverbände zur Vergabe von Startpässen, Herausgabe von Pressemitteilungen über Sportergebnisse und Ehrungen oder Aushänge am Schwarzen Brett.

**4 Welche Kernaussagen enthält das Datenschutzrecht?** (HI11406691)

Eine kompakte Übersicht über die wichtigsten datenschutzrechtlichen Eckpunkte listet Art. 5 DSGVO auf. Daraus lassen sich die Kernaussagen des Datenschutzrechts ableiten. Sie helfen, die Zusammenhänge besser zu verstehen:

* Personenbezogene Daten dürfen nur auf **rechtmäßige Weise** verarbeitet werden – nämlich so, wie es die Datenschutzgesetze vorsehen. Insbesondere muss jede Datenverarbeitung durch eine gesetzliche Erlaubnis gestattet sein (vgl. Kapitel 5). Zudem muss die Datenverarbeitung nach Treu und Glauben, also fair, und in einer für die Betroffenen nachvollziehbaren Weise erfolgen. Die Betroffenen müssen deshalb über die Datenverarbeitung unterrichtet werden und besitzen beispielsweise einen Auskunftsanspruch.
* Personenbezogene Daten dürfen nur verarbeitet werden, wenn dies einem bestimmen Zweck dient (**"Zweckbindung"** der Daten). Dieser Zweck muss definiert und dokumentiert sein (im "Verzeichnis der Verarbeitungstätigkeiten, vgl. Kapitel 7.4").
* Es dürfen nur so wenige Daten erhoben und verarbeitet werden, wie zum Erreichen der festgelegten Zwecke notwendig sind (Grundsatz der **"Datenminimierung"**).
* Alle personenbezogenen Daten müssen sachlich **richtig** und auf dem aktuellen Stand sein. Falsche personenbezogenen Daten sind zu korrigieren.
* Werden personenbezogene Daten nicht mehr benötigt, müssen sie gelöscht oder zumindest anonymisiert werden (Grundsatz der **"Speicherbegrenzung"**).
* Personenbezogene Daten müssen durch geeignete **technische und organisatorische Maßnahmen** geschützt werden. Das heißt, die Systeme und Dienste, auf denen sie verarbeitet werden, müssen sicher sein und die Beschäftigten müssen wissen, was sie tun dürfen und was nicht.

**5 Wann dürfen personenbezogene Daten verarbeitet werden?** (HI11406692)

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn das Gesetz es im Einzelfall zulässt. Juristisch gesprochen handelt es sich um ein "Verbot mit Erlaubnisvorbehalt". Somit muss das Gesetz immer dann, wenn im Verein personenbezogene Daten "angefasst" werden, eine gesetzliche Erlaubnis vorsehen.

Das hört sich komplizierter an, als es ist. Denn in den typischerweise auftretenden Fällen liegt eine solche Erlaubnis (Rechtsgrundlage) vor. Andere Fälle muss man vorher überprüfen (lassen), z. B. durch den Datenschutzbeauftragten.

In folgenden Fällen ist eine Datenverarbeitung zulässig, weil Art. 6 DSGVO dafür eine Rechtsgrundlage enthält:

* **Einwilligung:**

Wenn die betroffene Person freiwillig und ohne Zwang konkret zustimmt, dürfen Daten über sie verarbeitet werden. Der Verein muss die Einwilligung jedoch belegen können. Die Einwilligung ist jederzeit widerrufbar; falls ein Widerruf eingelegt wird, darf ab diesem Zeitpunkt keine weitere Datenverarbeitung mehr stattfinden. Das kann im Einzelfall zu Schwierigkeiten führen, weil dann die Rechtsgrundlage entfällt. Um dies zu verhindern, sollte – wenn möglich – auf eine der anderen Rechtsgrundlagen zurückgegriffen werden.

* **Vertragserfüllung:**

Wenn die Datenverarbeitung notwendig ist, um einen Vertrag mit der betroffenen Person erfüllen zu können, stellt das ebenfalls eine geeignete Rechtsgrundlage dar.

**Beispiel für Vertragserfüllung im Verein**

Die Mitgliedschaft im Verein stellt einen Vertrag dar. Damit der Verein den Vertrag erfüllen kann, darf er den Namen und die Anschrift des Mitglieds speichern und nutzen, um es identifizieren und kontaktieren zu können. Wenn ein Lastschrifteinzug des Mitgliedsbeitrags vereinbart wird, darf auch die Bankverbindung gespeichert werden.

Nicht zulässig wäre dagegen, wenn beispielsweise ein Museumsverein die Haarfarbe verarbeiten will oder ein Sportverein die Lieblingsfarbe – denn das wäre vom eigentlichen Zweck nicht mehr gedeckt.

* **Rechtliche Verpflichtung:**

Wenn der Verein rechtlich verpflichtet ist, mit den Daten umzugehen, etwa aufgrund von Gesetzen, ist die Datenverarbeitung ebenfalls gestattet.

**Beispiel für rechtliche Verpflichtungen im Verein**

Belege über die Zahlung von Mitgliedsbeiträgen muss der Verein aufgrund von Buchhaltungsvorschriften zehn Jahre lang aufbewahren (§ 257 HGB und § 147 AO).

* **Schutz lebenswichtiger Interessen:**

Daten dürfen auch dann verarbeitet werden, wenn dies dem Schutz des Lebens oder der körperlichen Unversehrtheit eines Menschen dient (beispielsweise bei einem Verein zur Unfallhilfe oder einem Rettungsdienst).

* **Berechtigte Interessen des Vereins:**

Wenn die Datenverarbeitung im "berechtigten Interesse" des Vereins liegt und keine Interessen des Betroffenen entgegenstehen, dürfen ebenfalls personenbezogene Daten verarbeitet werden. Es muss hier eine Abwägung der Interessen von Verein und Betroffenem vorgenommen werden. Es handelt sich zugegebenermaßen um eine etwas schwammige Rechtsgrundlage, bei der man zu unterschiedlichen Ergebnissen kommen kann. Bei der Einschätzung und Beurteilung kann ein Datenschutzbeauftragter unterstützen. Jedenfalls müssen die berechtigten Interessen des Vereins benannt und dokumentiert werden – und sie müssen dem Betroffenen mitgeteilt werden (siehe Kapitel 7.2).

**6 Wann dürfen Daten vom Verein veröffentlicht oder weitergegeben werden?** (HI11406693)

Die Weitergabe von personenbezogenen Daten stellt ebenso eine Datenverarbeitung dar wie deren Veröffentlichung. Deshalb sind auch sie nur zulässig, wenn für sie eine der oben genannten Rechtsgrundlagen (Kapitel 5) vorliegt.

Typische Beispiele für den Verein können sein:

**Datenübermittlung an andere Vereine (z. B. an den Dachverband für Ehrungsanträge, an Sport-Fachverbände für Spielerpässe oder -pläne)**

Dies ist zulässig, solange die Datenübermittlung erforderlich ist, um einem Mitglied die ihm zugesicherten Leistungen bieten zu können (im Sinne der Vertragserfüllung, Art. 6 Abs. 1 Buchst. b DSGVO).

Eine alternative Rechtsgrundlage kann zum Tragen kommen, wenn der Verein eigene berechtigte Interessen an der Datenübermittlung besitzt (Art. 6 Abs. 1 Buchst. f DSGVO). Welche Interessen als berechtigt gelten, kann sich auch aus der Vereinssatzung ergeben. Zudem muss eine Abwägung vorgenommen werden zwischen der Erfüllung des Vereinszwecks einerseits und den Interessen des Betroffenen andererseits. Demnach ist die Übermittlung nicht zulässig, wenn der einzelne Betroffene ein entgegenstehendes, höherwertiges Interesse am Schutz seiner Privatsphäre besitzt. Dies kann im Einzelfall jedoch schwer zu bestimmen sein.

Als dritte Möglichkeit kommt die Einwilligung des Betroffenen in Betracht (Art. 6 Abs. 1 Buchst. a und Art. 7 DSGVO). Holen Sie diese vorab und nachweisbar beim Betroffenen ein, um auf der sicheren Seite zu sein.

**Datenübermittlung an die Presse (z. B. Sportverein informiert über Spielergebnisse und sportliche Einzelleistungen)**

Eine Rechtsgrundlage hierfür könnte Art. 6 Abs. 1 Buchst. f DSGVO darstellen, wenn eine Interessenabwägung ergibt, dass der Verein ein berechtigtes Interesse an der Veröffentlichung hat und das Mitglied kein entgegenstehendes, höherwertiges Interesse an einer Nichtübermittlung besitzt. Da die Abwägung in jedem Einzelfall anders ausgelegt werden und zu einem anderen Ergebnis kommen kann, ist auch hier auf der sicheren Seite, wer auf eine Einwilligung zurückgreift. Die Einwilligung kann für den Einzelfall eingeholt oder pauschal für alle Fälle dieser Art abgegeben werden. Das Mitglied muss jedoch jederzeit seinen Widerspruch einlegen können, dieser ist dann auch zu beachten.

**Veröffentlichung von Mitgliederdaten auf der Vereinshomepage, in sozialen Netzwerken oder in der Mitgliederzeitung**

Wenn die Veröffentlichung nicht unmittelbar dem Vereinszweck dient, sollte ebenfalls eine vorherige Einwilligung des Betroffenen eingeholt werden. Denn eine der anderen Rechtsgrundlagen wird vermutlich nicht zutreffen.

Der Text der Einwilligung muss in einer klaren und einfachen Sprache erfolgen und von anderen Sachverhalten klar zu unterscheiden sein (Art. 7 DSGVO) – ein "Verstecken" im Kleingedruckten wäre nicht zulässig.

**Veröffentlichung einer Mitglieder- oder Spendenliste (beispielsweise im Internet oder in der Vereinszeitung)**

Es handelt sich hier um denselben Sachverhalt wie oben – personenbezogene Daten werden anderen zur Kenntnis gegeben. Daher ist er auch so wie oben zu beurteilen: Es sollte die schriftliche Einwilligung jedes einzelnen Betroffenen vor der Veröffentlichung eingeholt werden. Dies gilt insbesondere für Vereine, die sensible Daten verarbeiten (z. B. Gesundheitsdaten, politische Überzeugungen, religiöse oder weltanschauliche Überzeugungen).

**Datenweitergabe zu Werbezwecken (z. B. Verkauf von Mitgliederadressen an ein Versandhaus)**

Eine Datenweitergabe an Externe wird in der Regel nicht zulässig sein, weil die Interessen des Mitglieds am Schutz seiner Privatsphäre höher anzusiedeln sind als die Interessen des Vereins an einer Einnahmequelle. Das ergibt die Interessenabwägung, wenn man auf die Rechtsgrundlage des Art. 6 Abs. 1 Buchst. f DSGVO zurückgreift. Eine Datenweitergabe zu Werbezwecken wäre allenfalls zulässig, wenn jeder Betroffene seine Einwilligung dazu erteilen würde.

**Datenweitergabe aufgrund von Outsourcing (z. B. Versand der Mitgliederzeitung durch Druckerei, Auslagerung der Mitgliederverwaltung, Beitragseinzug durch Steuerberater)**

Wenn der Verein eine externe Stelle damit beauftragt, personenbezogene Daten in seinem Namen zu verarbeiten, gelten oftmals spezielle Regeln. Es könnte eine Auftragsverarbeitung vorliegen. In diesem Fall gelten die Vorgaben des Art. 28 DSGVO. Es ist dann in einer Vereinbarung festzuhalten, wie mit den Daten umgegangen wird und welche Schutzmaßnahmen getroffen werden (dazu mehr in Kapitel 7.3).

**7 Welche formalen Datenschutzvorgaben müssen beachtet werden?** (HI11406694)

Neben den Vorgaben zu Datenverarbeitungen enthält die Datenschutz-Grundverordnung auch einige eher formale Pflichten. Es handelt sich vor allem um die Folgenden:

**7.1 Rechenschaftspflicht** (HI11406695)

Wie bereits mehrfach erwähnt, muss sich jede Stelle (auch Vereine), die personenbezogene Daten verarbeitet, an die Datenschutzgesetze halten. Aber sie muss sich nicht nur daran halten, sondern dies auch "nachweisen können". Das wird als Rechenschaftspflicht bezeichnet und ergibt sich aus Art. 5 Abs. 2 DSGVO. Der Nachweis muss der Datenschutz-Aufsichtsbehörde auf Verlangen vorgelegt werden. Ist dies nicht möglich, drohen Bußgelder.

Was bedeutet das nun für die Praxis? Alle datenverarbeitenden Stellen (auch Vereine) sollten eine Datenschutz-Organisation aufbauen:

* Der Verein muss sich dazu mit den Vorgaben der Datenschutzgesetze vertraut machen.
* Der Verein sollte seine Erkenntnisse in konkrete Anweisungen für die Beteiligten (Mitarbeiter) herunterbrechen und dabei die spezifischen Besonderheiten und Anforderungen berücksichtigen.
* Diese Anweisungen sollten schriftlich vorliegen und verbindlich in Kraft gesetzt werden, so dass sie von allen Beteiligten beachtet werden müssen. Dass und wie dies genau passiert, muss nachgewiesen werden können.
* Die Vorgaben müssen regelmäßig kontrolliert und ggf. verbessert werden. Es muss sich insofern um einen fortlaufenden Prozess zur Verbesserung handeln. Eine einmalige Aktion ist nicht ausreichend.

**Wichtig**

**Empfohlene Dokumentationen**

Achten Sie darauf, unter anderem Dokumente aus folgenden Bereichen vorzuhalten:

* Sensibilisierung und Schulung der Mitarbeiter im Datenschutz (wann, wie, wer)
* Festlegung der Verantwortlichkeiten beim Umgang mit personenbezogenen Daten
* Verzeichnis der Verarbeitungstätigkeiten (gem. Art. 35 DSGVO)
* Übersicht über die Auftragsverarbeiter (Art. 28 DSGVO)
* Getroffene Maßnahmen zur technischen und organisatorischen Datensicherheit (Art. 32 DSGVO)
* Umgang mit Datenpannen (Art. 33 und Art. 34 DSGVO)
* Datenschutz-Folgenabschätzung, soweit im Einzelfall zutreffend (Art. 35 DSGVO)
* Bestellungsurkunde des Datenschutzbeauftragten, soweit einer bestellt ist (Art. 37 DSGVO).

Je umfassender die Dokumente verfasst und je besser sie ineinander verzahnt sind, umso besser kann damit der Rechenschaftspflicht nachgekommen werden.

**7.2 Informationspflicht bei Datenerhebung** (HI11406696)

Zu dem Zeitpunkt, zu dem personenbezogene Daten abgefragt oder anderweitig erhoben werden, müssen die Betroffenen über eine Reihe von detaillierten Angaben unterrichtet werden. Das Gesetz sieht bis zu 13 Pflichtangaben vor (Art. 12 bis 14 DSGVO), unter anderem Name und Kontaktdaten des Vereins, gegebenenfalls des Datenschutzbeauftragten, die Zwecke der Datenerhebung, ggf. die Empfänger der Daten, die Speicherdauer oder das Bestehen eines Auskunfts- und Beschwerderechts.[1]

Diese Informationen müssen immer dann erteilt werden, wenn personenbezogene Daten "erhoben", also erstmals erfasst und gespeichert werden und dem Betroffenen diese Informationen noch nicht vorliegen.

In der Praxis kann der Verein der Informationspflicht nachkommen, indem er Beiblätter erstellt und ausgibt (zum Beispiel zum Antrag auf Mitgliedschaft). Bei einem Online-Antrag sollten auch die Informationen online gegeben werden.

**Wichtig**

**Informationspflicht auch bei Daten, die nicht beim Betroffenen selbst abgefragt wurden**

Die Informationspflicht greift auch dann, wenn der Verein personenbezogene Daten aus einer anderen Quelle erhält (Beispiel: Prüfung der Bonität bei der Schufa oder Creditreform). In diesem Fall muss der Betroffene, also derjenige, um dessen Daten es geht, ebenfalls informiert werden. Die Pflichtangaben bestimmen sich in diesem Fall aus dem Katalog des Art. 14 DSGVO.

**7.3 Auftragsverarbeitung** (HI11406697)

Wenn der Verein Dienstleister einschaltet, die personenbezogene Daten im Auftrag verarbeiten, kann eine so genannte Auftragsverarbeitung vorliegen (Art. 28 DSGVO). Das ist dann der Fall, wenn der Verein die Entscheidungshoheit über die Zwecke und Mittel der Datenverarbeitung besitzt und der Dienstleister sich danach zu richten hat (oder wenn diese Entscheidung dem Dienstleister übertragen wird) – wenn der Dienstleister quasi nur als "verlängerter Arm" des Vereins tätig wird.

**Praxis-Beispiel**

**Typische Fälle von Auftragsverarbeitungen sind:**

* Externes Rechenzentrum,
* Nutzung von Cloud-Diensten (z. B. Office 365, Google Mail, Dropbox),
* Fernwartung von Geräten oder Software,
* Adressübermittlung an Druckerei für Postversand,
* Lettershop für Werbeaktionen,
* Schreibbüro,
* Callcenter,
* Akten- und Datenträgerentsorgung durch eine externe Firma.

**Keine Auftragsverarbeitung liegt dagegen vor bei:**

Rechtsanwalt oder Wirtschaftsprüfer, weil diese die Daten eigenständig verarbeiten und der Auftraggeber hier nicht die Mittel für die Datenverarbeitung vorgibt.

**An eine Auftragsverarbeitung knüpfen sich eine Reihe von Pflichten:**

**Auf was ist zu achten, wenn eine Auftragsverarbeitung vorliegt?**

|  |  |
| --- | --- |
| **1.** | **Sorgfältige Auswahl**  Der Dienstleister muss in datenschutzrechtlicher Hinsicht sorgfältig ausgewählt werden. Das heißt, er muss alle datenschutzrechtlichen Anforderungen erfüllen können. |
| **2.** | **Datenschutzkonforme Vereinbarung**  Es müssen die datenschutzrechtlichen Rechte und Pflichten zwischen Verein und Dienstleister vereinbart werden. Das Gesetz sieht in Art. 28 Abs. 3 DSGVO eine Reihe von Pflichtangaben vor[1], unter anderem über   * Art und Zweck der Datenverarbeitung; * die Arten der personenbezogenen Daten, die verarbeitet werden, sowie die Kategorien der davon betroffenen Personen; * technische und organisatorische Maßnahmen, die zum Schutz der Daten getroffen werden; * Weisungen, die zu dokumentieren sind; * Zustimmung oder zumindest Information, bevor der Dienstleister eventuelle Subunternehmer einschaltet; * Rückgabe oder Löschung der Daten nach Vertragsbeendigung. |

**Hinweis**

**Ältere Verträge müssen ggf. angepasst werden**

Vor dem Inkrafttreten der DSGVO am 25. Mai 2018 wird dieser Sachverhalt als Auftrags*daten*verarbeitung bezeichnet (§ 11 BDSG alter Fassung). Auch hier mussten datenschutzrechtliche Vereinbarungen geschlossen werden. Die Pflichtangaben verschieben sich jedoch unter der DSGVO zum Teil. Insofern müssen ältere Verträge, die noch auf § 11 BDSG alter Fassung beruhen, nachgebessert werden – oder es wird sicherheitshalber gleich eine neue Vereinbarung auf Basis einer DSGVO-Vorlage abgeschlossen.

**7.4 Verzeichnis der Verarbeitungstätigkeiten** (HI11406698)

Wer personenbezogene Daten verarbeitet, muss dies dokumentieren. Auf Nachfrage ist diese Dokumentation an die Datenschutz-Aufsichtsbehörde herauszugeben, damit sie sich ein schnelles Bild verschaffen kann. Das Verzeichnis dient lediglich der Behörde und eventuell eigenen Zwecken – an Dritte muss es jedoch nicht herausgegeben werden.

Die Inhalte, die das Verzeichnis der Verarbeitungstätigkeiten enthalten muss, listet Art. 30 DSGVO im Detail auf[1]:

* Namen und Kontaktdaten des Vereins, des Vorstands (als dessen Vertreter) sowie eines etwaigen Datenschutzbeauftragten
* eine Auflistung der Zwecke, zu denen personenbezogene Daten verarbeitet werden
* eine Beschreibung der Kategorien der betroffenen Personen und der Kategorien personenbezogener Daten
* die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden
* falls personenbezogene Daten an einen Empfänger in ein Drittland übermittelt werden (d. h. außerhalb der EU): Nennung von Empfänger, Drittland und Rechtsgrundlage für die Übermittlung
* die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien, wenn möglich
* eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung (gemäß Artikel 32 DSGVO), wenn möglich.

Diese Angaben müssen schriftlich festgehalten und aktualisiert werden. Ein elektronisches Format ist zulässig.

Es gibt zwar Ausnahmen von der Pflicht, ein Verarbeitungsverzeichnis zu führen (Art. 30 Abs. 5 DSGVO) – jedoch kommen diese in der Praxis quasi nie zum Tragen. Beispielsweise müsste die Verarbeitung "nicht nur gelegentlich" erfolgen. Jedoch erfolgt in Vereinen alleine die Mitgliederverwaltung immer systematisch und daher öfter als nur gelegentlich.

**Praxis-Tipp**

**Verzeichnis der Verarbeitungstätigkeiten nicht unterschätzen**

Auch wenn es etwas nach bürokratischer Arbeit aussieht – das aktuelle Verzeichnis der Verarbeitungstätigkeiten sollte in jedem Verein vorgehalten werden (oder zumindest innerhalb kürzester Zeit erstellt werden können). Wenn sich die Aufsichtsbehörde für den Verein interessiert, wird sie sich dieses Dokument als erstes vorzeigen lassen. Kann es nicht vorgelegt werden, drohen Bußgelder.

Aber auch für den Datenschutzbeauftragten ist das Verzeichnis nützlich. Es kann eine wichtige, kompakte Informationsquelle und Übersicht darstellen.

**7.5 Datenpannen** (HI11406699)

Wenn es zu einer Datenpanne kommt, greifen weitreichende Melde- und Informationspflichten gegenüber Behörden und Betroffenen. Weil dabei eine Frist von 72 Stunden gilt, sollten für den Fall der Fälle Vorbereitungen getroffen werden – dies ist auch Teil einer Datenschutz-Organisation.

Der Begriff der Datenpanne ist weit gefasst und erfasst jede Verletzung des Schutzes von personenbezogenen Daten. Darunter fallen Hackerangriffe auf die Mitgliederdatenbank ebenso wie versehentlicher Falschversand per E-Mail oder Fax – also insbesondere alle unbefugten Offenlegungen von personenbezogenen Daten.

Wenn durch solch einen Vorfall voraussichtlich ein Risiko für den Betroffenen entsteht (und das ist fast immer der Fall, außer, die Daten waren verschlüsselt), muss Folgendes beachtet werden:

Der Vorfall muss innerhalb von 72 Stunden nach Bekanntwerden **an die Datenschutz-Aufsichtsbehörde gemeldet** werden (verspätete Meldungen müssen eine Begründung für die Verzögerung enthalten, Art. 33 DSGVO). Die Meldung muss mindestens folgende Informationen enthalten:

* Beschreibung des Vorfalls, soweit möglich mit Angabe der Betroffenen (Kategorien und ungefähre Anzahl) und der betroffenen Daten (Kategorien und ungefähre Anzahl der Datensätze)
* Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
* Beschreibung der wahrscheinlichen Folgen des Vorfalls
* Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und gegebenenfalls Maßnahmen zur Abmilderung der möglichen nachteiligen Auswirkungen.

In einigen Fällen müssen auch die **betroffenen Personen** über die Datenpanne benachrichtigt werden, nämlich wenn sie voraussichtlich einem "hohen Risiko" ausgesetzt sind (Art. 34 DSGVO). In diesem Fall sind die Betroffenen so schnell wie möglich zu informieren (was auch länger dauern darf als 72 Stunden), und zwar in "klarer und einfacher Sprache". Das Gesetz nennt einige Ausnahmen, in denen von der Benachrichtigung abgesehen werden kann. Dazu zählt unter anderem ein besonderes Geheimhaltungsinteresse des Vereins, das jedoch zu begründen wäre (§ 29 Abs. 1 Satz 3 BDSG n. F.).

**8 Gibt es Vorgaben für die technische Datensicherheit?** (HI11406700)

Personenbezogene Daten können nur dann effektiv geschützt werden, wenn auch die IT-Systeme und Dienste geschützt sind, auf denen diese Daten verarbeitet werden. Deshalb besagt Art. 32 DSGVO, dass ein Schutzniveau hergestellt werden muss, das den Risiken beim Datenverarbeiter angemessen ist. Verarbeitet er besonders sensible Daten (z. B. Gesundheitsdaten), muss er deutlich bessere Schutzmaßnahmen umsetzen als wenn er beispielsweise nur einfache Daten wie Namen und Adressen speichert. Es kommt also ein risikobasierter Ansatz zum Tragen, der auch einen gewissen Interpretationsspielraum öffnet.

Auf jeden Fall dürfen die Maßnahmen nicht hinter den jeweils aktuellen "Stand der Technik" zurückfallen.

Das Gesetz sagt, es sollen Maßnahmen aus den folgenden Bereichen geprüft werden, um personenbezogene Daten (noch besser) zu schützen:

* **Pseudonymisierung** der personenbezogenen Daten (z. B. Ersetzung des Namens durch eine ID), soweit dies möglich ist
* **Verschlüsselung** (Einsatz von Kryptografie, z. B. für die Mitgliederdatenbank oder von Festplatten mobiler Notebooks)
* Sicherstellung der **Vertraulichkeit** der Systeme und Dienste (z. B. durch die Vergabe von Benutzerrechten, Anmeldung nur mit Passwort, Zugang über verschlüsselte Datenleitung)
* Sicherstellung der **Integrität** der Systeme und Dienste (Schutz vor Manipulation der Daten, z. B. durch Zugriffsberechtigungen, Antivirenprogramme oder Spamfilter)
* Sicherstellung der **Verfügbarkeit** der Systeme und Dienste (etwa durch Sicherheitskopien und Notstromversorgung)
* Sicherstellung der **Belastbarkeit** der Systeme und Dienste (z. B. Virenscanner, Firewall, Notfallkonzept)
* rasche **Wiederherstellung** der Daten nach einem physischen oder technischen Zwischenfall (z. B. redundante Speicherung in mehreren Rechenzentren oder in einem NAS, Wiederherstellung über Sicherungskopien).

Der letzte Punkt, den das Gesetz nennt (Art. 32 Abs. 1 Buchst. d DSGVO), hat es in sich: Es soll ein **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit all dieser technischen und organisatorischen Maßnahmen zum Einsatz kommen. Im optimalen Fall kann der Verein dies über ein Zertifikat nach ISO 27001 o. Ä. belegen. Ebenso hilfreich wäre es, wenn ein internes Kontroll- oder Qualitäts-Management-System (IKS/QMS) samt regelmäßiger Kontrolle bestehen würde. Ist beides nicht der Fall, bietet sich die Einführung eines PDCA-Prozesses an ("Plan" = Planen, "Do" = Umsetzen, "Check" = Prüfen, "Act" = Optimierung). Dadurch soll ein fortlaufender Prozess in Gang gesetzt werden, um regelmäßig zu überprüfen, ob die technischen und organisatorischen Maßnahmen ausreichend sind und um ggf. Verbesserungen anstoßen zu können.

Gerade in kleinen Vereinen wird dieser letzte Punkt nicht immer ganz einfach umzusetzen sein. Eventuell kann man auch zum Schluss kommen, dass kleine Vereine mit wenig risikobehafteten Datenverarbeitungen ein solches Verfahren nicht unbedingt umsetzen müssen. Welche Minimalanforderungen die Datenschutz-Aufsichtsbehörden hier als notwendig erachten, wird sich im Lauf der Zeit herausstellen.

**9 Welche Rechte besitzen die Betroffenen?** (HI11406701)

Damit Datenschutz kein zahnloser Tiger bleibt, besitzen diejenigen, deren Daten verarbeitet werden, eine Reihe von Rechten. Die Wichtigsten sind:

**Recht auf Auskunft**

Jeder kann sich an den Verein wenden und fragen, ob – und wenn ja, welche – Daten dort über ihn gespeichert sind (Art. 15 DSGVO). Der Verein muss die Auskunft dann in der Regel innerhalb eines Monats erteilen. Dem Antragsteller muss dazu eine Kopie seines Datensatzes zur Verfügung gestellt werden.

Darüber hinaus hat der Anfragende Anspruch auf folgende Informationen:

* die Zwecke, weshalb der Verein Daten über ihn verarbeitet
* die Kategorien der über ihn gespeicherten Daten
* eventuelle Empfänger, falls die Daten weitergeleitet werden (mit Namen oder zumindest als Sammelbezeichnung der Empfänger)
* die Speicherdauer der Daten oder zumindest Kriterien für die Bestimmung der Speicherdauer
* einen Hinweis, dass es die Rechte auf Berichtigung, Löschung, Einschränkung und Widerspruch gibt
* einen Hinweis auf das Beschwerderecht bei der Datenschutz-Aufsichtsbehörde
* falls die Daten nicht vom Betroffenen selbst kommen: woher die Daten stammen
* falls die Daten für eine automatisierte Entscheidungsfindung (einschließlich Profiling) herangezogen werden: eine aussagekräftige Angabe über deren Wirkungsweise.

Die Auskunft muss kostenfrei erteilt werden.

**Recht auf Berichtigung**

Wenn die gespeicherten personenbezogenen Daten sachlich falsch sind (z. B. Tippfehler im Namen oder Namensänderung nach Heirat), darf der Betroffene eine Berichtigung verlangen (Art. 16 DSGVO). Der Verein muss diesem Begehren dann nachkommen.

**Recht auf Löschung ("Recht auf Vergessenwerden")**

In einigen Fällen hat der Betroffene das Recht, die Löschung seiner Daten zu verlangen (Art. 17 DSGVO). Eine Löschung muss insbesondere dann durchgeführt werden, wenn

* die personenbezogenen Daten nicht mehr benötigt werden, weil der Zweck mittlerweile entfallen ist,
* die personenbezogenen Daten unrechtmäßig verarbeitet wurden (weil es z. B. keine Rechtsgrundlage gibt),
* der Betroffene ursprünglich eingewilligt hatte und seine Einwilligung dann widerrufen hat oder
* der Betroffene Widerspruch gegen die Datenverarbeitung einlegt und eine Prüfung ergibt, dass dem Widerspruch stattgegeben wird.

Einem Wunsch nach Löschung muss daher nicht in allen Fällen nachgekommen werden. Im Einzelfall kann und sollte auch der Datenschutzbeauftragte befragt und auf seine Fachkompetenz zurückgegriffen werden.

Einen teilweise anderen Fokus besitzt das **"Recht auf Vergessenwerden".** Wenn der Verein personenbezogene Daten öffentlich gemacht hatte (z. B. im Internet) und der Betroffene dann die Löschung seiner Daten erfolgreich beantragt, greifen weiterreichende Pflichten. Dann muss der Verein auch diejenigen informieren, die sich diese Daten gezogen und sie weiterverarbeitet haben. Es besteht also eine Informationspflicht über die Löschung. Um diese umsetzen zu können, müssen angemessene Maßnahmen getroffen werden (unter Berücksichtigung der verfügbaren Technologien und der Implementierungskosten). Hintergrund ist, dass es bei Veröffentlichungen im Internet häufig zu einem Kontrollverlust über die Daten kommt. Das Recht auf Vergessenwerden soll dem entgegenwirken und die Rechtsdurchsetzung etwas effektiver machen.

Wie das alles in der Praxis möglichst gut umgesetzt werden kann (im Sinn von Best practices), wird die Zukunft zeigen müssen.

**Recht auf Einschränkung der Verarbeitung**

Wenn die Verarbeitung von personenbezogenen Daten eingeschränkt ist, heißt dies, dass sie nur noch in wenigen Fällen verarbeitet werden dürfen (Art. 18 DSGVO). Eine Einschränkung der Verarbeitung kann etwa zur Anwendung kommen, wenn der Betroffene behauptet, dass die Daten über ihn nicht richtig sind. Die Einschränkung besteht dann für die Dauer, während der Verein dies überprüft.

Die Daten dürfen erst dann weiterverarbeitet werden, wenn z. B. der Betroffene selbst zustimmt.

**Recht auf Datenübertragbarkeit**

Der Betroffene besitzt das Recht, seine Daten als Computerdatei herauszuverlangen (Art. 20 DSGVO). Dieses Recht war ursprünglich gegen Facebook, Google und ähnliche Anbieter gerichtet, damit Nutzer ihre Profildaten zu anderen Anbietern umziehen können, wurde dann aber deutlich weiter gefasst und kann nun gegen alle Datenverarbeiter gerichtet werden.

Voraussetzungen sind, dass

|  |  |
| --- | --- |
| . | der Betroffene die Daten selbst bereitgestellt hat, |
| . | die Daten aufgrund einer Einwilligung oder Vertragserfüllung verarbeitet werden und |
| . | die Verarbeitung IT-mäßig erfolgt. |

Nur wenn alle drei Voraussetzungen zutreffen, hat der Betroffene das Recht, seine Daten in einem "strukturierten, gängigen und maschinenlesbaren Format" zu erhalten (beispielsweise als XML- oder CSV-Datei).

Alternativ kann der Betroffene verlangen, dass seine Daten nicht an ihn, sondern direkt an eine andere Stelle übermittelt werden. In einem Sportverein wäre es denkbar, dass ein Mitglied seine Mitgliedschaft kündigt und vom Verein verlangt, dass seine Stammdaten (Name, Anschrift, Kommunikationsdaten) direkt an einen anderen Sportverein digital übermittelt werden.

**Widerspruchsrecht**

Falls der Verein Direktwerbung betreiben sollte, muss er die Werbeempfänger auf ihr Recht zum jederzeitigen Widerspruch hinweisen. Nimmt ein Werbeempfänger dieses Widerspruchsrecht wahr, dürfen seine Daten nicht mehr für Werbung verwendet werden – und zwar ausnahmslos (Art. 21 Abs. 2 DSGVO).

Daneben gibt es noch ein Widerspruchsrecht gegen Datenverarbeitungen, die auf der Rechtsgrundlage der berechtigten Interessen des Vereins beruhen (Art. 6 Abs. 1 Buchst. f DSGVO). Hier muss dann eine weitere Abwägung vorgenommen werden.

**10 Wer überwacht die Einhaltung des Datenschutzes im Verein?** (HI11406702)

Von staatlicher Seite kontrolliert die Datenschutz-Aufsichtsbehörde, die es in jedem EU-Mitgliedsland und in allen deutschen Bundesländern gibt. Behördenmitarbeiter dürfen Informationen anfordern, Datenschutzüberprüfungen durchführen und den Zugang zu Informationen einfordern.

Daneben überwachen viele weitere Stellen die Einhaltung des Datenschutzes auf eine direkte oder indirekte Weise: Etwa Mitglieder (durch die Wahrnehmung ihrer Rechte), der Vorstand (durch klare Anweisungen) und natürlich der Datenschutzbeauftragte, sofern einer bestellt ist.

**11 Gibt es praktische Hilfe bei der Umsetzung?** (HI11406703)

Die Anforderungen an das Datenschutzrecht steigen insbesondere mit dem Inkrafttreten der DSGVO an. Um den Ansprüchen gut und gesetzeskonform nachkommen zu können, sollte es eine interne oder externe Stelle geben, die sich im Datenschutzrecht auskennt und die den Verein berät – optimalerweise als Datenschutzbeauftragter, zumindest aber als Berater.

Der Verein kann sich überlegen, ob er jemanden aus den eigenen Reihen qualifizieren möchte, etwa ein Mitglied. Dieses müsste vermutlich erst geschult werden. Es könnte Unterstützung beziehen durch

* Seminare
* Fachliteratur und Online-Dienste
* Datenschutz-Aufsichtsbehörden, die auch beraten und unterstützen müssen
* Datenschutz-Organisationen wie GDD e. V. oder BvD e. V. mit ihren Serviceangeboten
* Datenschutz-Dienstleister als Berater.

Alternativ kann auch eine externe Stelle beauftragt werden (externe Datenschutzbeauftragte, Datenschutz-Berater und -Dienstleister, Rechtsanwälte). Diese besitzen von Anfang an bessere Fachkenntnisse und praktische Erfahrungen, werden aber auch höhere Kosten verursachen.

**12 Was droht dem Verein bei Verstößen?** (HI11406704)

Anders als früher ist unter der DSGVO so gut wie jeder Verstoß mit einem Bußgeld bedroht. Die Bußgeldhöhe wurde dramatisch erhöht und kann existenzbedrohend sein. **Pro Verstoß drohen bis zu 20 Mio. Euro**, je nach Art und Schwere des Verstoßes, der getroffenen Maßnahmen, früheren Verstößen, Kooperationsbereitschaft und anderen Umständen des Einzelfalls.

Neben Bußgeldern können bei Verstößen aber auch weitere Konsequenzen drohen, etwa

* Schadensersatz, wenn durch die Nichteinhaltung des Datenschutzes ein materieller oder immaterieller Schaden entstanden ist;
* Untersagung der Datenverarbeitung durch die Datenschutz-Aufsichtsbehörde: Verstößt eine Datenverarbeitung gegen das Gesetz, kann die Behörde die weitere Verarbeitung untersagen;
* Image- und Vertrauensschaden: Wenn ein Datenmissbrauch oder fehlerhafter Umgang publik wird, können Ruf und Reputation des Vereins leiden. Im schlimmsten Fall gewinnt der Verein weniger neue Mitglieder oder verliert bestehende Mitglieder.

Besser ist es daher in jedem Fall, von vornherein auf die Einhaltung der Datenschutzregeln zu achten – damit es gar nicht erst zu Problemen kommen kann.