Anmerkungen zum „Verzeichnis von Verarbeitungstätigkeiten mit personenbezogenen Daten“

[1] Wann muss der Verein ein „Verzeichnis von Verarbeitungstätigkeiten mit personenbezogenen Daten“ erstellen?

Immer dann, wenn er personenbezogene Daten verarbeitet.

„Personenbezogene Daten“ sind alle Daten, anhand derer man eine natürliche Person identifizieren kann; Beispiele: Name, Wohnort, Steuernummer, Religionszugehörigkeit, E-Mail-Adresse, Gesundheitsdaten, aber auch Fotoaufnahmen etc.

Was immer auch Sie mit personenbezogenen Daten machen, es handelt sich stets um eine „Verarbeitung“ im Sinne der DS-GVO! Die DS-GVO gilt sowohl für digitale als auch für analoge Datensammlungen (z. B. Mitgliederverzeichnis auf Dateikarten).
(„Verarbeitung“ ist „jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.)

[2] Verantwortlicher

Datenschutz ist Chefsache! Dem Vorstand des Vereins – vor allem dem Vorsitzenden –, aber auch dem nach § 30 BGB zum „besonderen Vertreter“ bestellten Geschäftsführer obliegt die Verantwortung für die Wahrung des Datenschutzes. (So gehört es zu seinen Aufgaben, für jede „Verarbeitungstätigkeit mit personenbezogenen Daten“ ein gesondertes Verzeichnis zu erstellen.)
Dies gilt auch dann, wenn der Verein einen „Datenschutzbeauftragten“ bestellt hat (zu den Aufgaben des Datenschutzbeauftragten siehe unten, Anm. 3 Punkt 2).

[3] Datenschutzbeauftragter

1. Unter bestimmten Umständen sind Sie verpflichtet, einen Datenschutzbeauftragten zu bestellen!

Dies ist dann der Fall, wenn

- der Verein in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt
  (siehe § 38 Abs. 1 Satz 1 BDSG-neu).
  Betrifft sowohl Haupt- als auch Ehrenamtliche.
  Entgegen einer in der Literatur vertretenen Meinung werden nur die Personen gezählt, zu deren Kern- bzw. Haupttätigkeit die Verarbeitung personenbezogener Daten gehört; also z. B. bei der Aufnahme und Verwaltung von Mitgliederdaten oder bei der Regelung der Finanzen des Vereins (Auskunft des Landesdatenschutzbeauftragten). Der Übungsleiter oder Trainer, dessen Kernaufgabe die Gestaltung des Trainings ist, fällt nicht in diese Kategorie, selbst dann, wenn er „nebenbei“ eine Liste mit den von ihm zu betreuenden Sportlern nutzt.

  oder wenn

- der Verein besonders sensible Daten wie Gesundheitsdaten verarbeitet, aber nur, wenn die Verarbeitung dieser Daten eine „Kerntätigkeit“ des Vereins darstellt (vgl. Art. 37 Abs. 1 c) DS-GVO).
  Die Erhebung von gesundheitlichen Daten durch Rehasportvereine zur Durchführung von Rehabilitationskursen stellt in der Regel nicht die Kerntätigkeit des Vereins dar. Haupttätigkeit ist vielmehr die Durchführung des Kurses (z. B. Berücksichtigung der

Belastbarkeit des Kursteilnehmers); die Datenverarbeitung ist in diesem Fall lediglich eine Nebentätigkeit.

oder wenn

- der Verein Daten verarbeitet, die einer „Datenschutz-Folgenabschätzung“ unterliegen (siehe § 38 Abs. 1 Satz 2 BDSG-neu, Art. 35 Abs. 1, 3 DS-GVO).
  Dies ist in der Regel bei der Verarbeitung von Gesundheitsdaten im Leistungssportbereich der Fall!
  (Zur „Datenschutz-Folgenabschätzung siehe auch unten zu Anmerkung 21.)

Bei kleineren Vereinen dürfte die Bestellung eines Datenschutzbeauftragten in der Regel also nicht erforderlich sein. Auch in solchen Fällen bleibt der Verein aber zur Einhaltung der Regeln des Datenschutzes verpflichtet und sollte daher Angebote (z. B. des LSB) zur Weiterbildung/Schulung wahrnehmen!

2. Welche Aufgaben hat der Datenschutzbeauftragte?

- Er kontrolliert die Einhaltung der datenschutzrechtlichen Bestimmungen.
- Er unterstützt und berät den Vorstand sowie die Beschäftigten im Umgang mit personenbezogenen Daten.
- Er ist Ansprechpartner für Betroffene sowie den Landesdatenschutzbeauftragten (Aufsichtsbehörde) und arbeitet mit diesem zusammen.

3. Welche Voraussetzungen muss der Datenschutzbeauftragte erfüllen?

Der Verein kann einen externen Dienstleister beauftragen oder aber eine interne Variante wählen (Mitarbeiter oder Vereinsmitglied; um Interessenkonflikte zu vermeiden, darf er jedoch nicht dem Vorstand angehören oder verantwortlich für die Datenverarbeitung sein!). Der Datenschutzbeauftragte muss qualifiziert sein und über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügen. Daher sollte der Verein den Datenschutzbeauftragten regelmäßig fortbilden und dies auch nachweisen können.

4. Veröffentlichung

Der Verein hat die Kontaktdaten seines Datenschutzbeauftragten zu veröffentlichen (sinnvollerweise auf der Internetseite). Dabei genügt eine E-Mail-Funktionsadresse (z. B.: datenschutzbeauftragter@x-verein.de), wenn sichergestellt ist, dass nur er oder sein Vertreter die Eingänge lesen können. Die Daten sind auch dem Landesdatenschutzbeauftragten mitzuteilen:
https://www.datenschutz-mv.de/kontakt/Mitteilung-von-Datenschutzbeauftragten/

[4] Datum der Anlegung

Der Verein hat nach der „Erstanlegung“ in regelmäßigen Abständen (z. B. einmal im Jahr) zu prüfen, ob die jeweilige Verarbeitungstätigkeit verändert oder erweitert wurde, und das Verzeichnis entsprechend anzupassen. Nach Möglichkeit sollten die Änderungen nicht einfach „überschrieben“ werden, sondern es sollte jedes Mal ein kompletter Neuausdruck erfolgen.

[5] Verfahrensverantwortlicher

Verfahrensverantwortlicher ist, wer hierzu vom Vorstand bzw. von der Vereinsleitung beauftragt wurde.

Insbesondere dann, wenn es keinen Datenschutzbeauftragten im Verein gibt, ist der Vorstand als „Verantwortlicher“ (siehe oben zu Anmerkung 2) verpflichtet, seinen Unterweisungspflichten gegenüber den Verfahrensverantwortlichen (Haupt- oder Ehrenamtliche) nachzukommen, sie für den Datenschutz zu sensibilisieren und zu schulen.

[6] **Beispiele für Verarbeitungstätigkeiten im Verein:**

Mitgliederverwaltung
Beitragsverwaltung
Trainings- und Wettkampfplanung
Verwaltung der Übungsleiter-Lizenzen
Adressverzeichnis
Geburtstagsliste
Führen der Personalakte/Personaldatenverwaltung
Lohnabrechnung (über externen Dienstleister)
Betrieb der Webseite des Vereins (über Hosting-Dienstleister)
Veröffentlichung von Fotos der Mitglieder/Mannschaftsfotos im Netz
Veröffentlichung von Bestenlisten oder Ergebnislisten im Netz

Für jede Verarbeitungstätigkeit ist ein gesondertes Verzeichnis auszufüllen!

[7] **Zweck der Datenverarbeitung**

Die Daten dürfen nur für den angegebenen Zweck verwendet werden.

Nicht mit dem Zweck „Verwaltung der Vereinstätigkeiten“ vereinbar und daher unzulässig wäre z. B. eine Weitergabe der Mitgliederdaten an einen Sponsor zwecks Werbung für dessen Produkte.

[8] **Kategorien personenbezogener Daten**

Hier haben Sie festzulegen, welche Daten konkret erhoben werden („Kategorien personenbezogener Daten“). Es dürfen nur die Daten erhoben werden, die für den angegebenen Zweck erforderlich sind („Datenminimierung“).

So sind zur Erreichung des Zweckes „Verwaltung der Vereinstätigkeiten“ die in dem Musterbeispiel genannten Angaben wie Name, Adresse, Eintrittsdatum etc. erforderlich – Angaben wie Herkunftsland oder -ort oder Religionszugehörigkeit hingegen nicht. Erheben Sie mehr Daten, als Sie wirklich brauchen, sollten Sie das ändern!

Als „besondere Kategorien“ personenbezogener Daten (Art. 9 DS-GVO) kommen insbesondere Gesundheitsdaten in Frage (v. a. Rehasportvereine).

Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO) werden im Sportverein verarbeitet, wenn Führungszeugnisse (beispielsweise von Übungsleitern) verlangt werden.

[9] **Empfänger personenbezogener Daten**

Hier ist anzugeben, ob und wem gegenüber die personenbezogenen Daten offengelegt werden.
Intern = anderes Mitglied des Vorstandes oder Mitarbeiter
Extern = Dritter außerhalb des Vereins; z. B. bei Auftragsdatenverarbeitung wie Lohnabrechnung über externen Dienstleister (Auftragsdatenverarbeitung darf nur auf Grundlage eines Vertrages mit dem „Auftragsverarbeiter“ erfolgen, vgl. Art. 28 Abs. 3 DS-GVO).
Bei Weitergabe an Dritte sind die Informationspflichten gem. Art. 13 DS-GVO zu beachten (siehe unten zu Anmerkung 12).

[10] Löschfristen

Grundsätzlich gilt:

Die personenbezogenen Daten sind unverzüglich zu löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (vgl. Art. 17 DS-GVO).

Aber:

Die Daten dürfen zu einem späteren Zeitpunkt gelöscht werden, wenn

- sie ggf. noch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden oder wenn
- anderweitige Aufbewahrungsfristen zu beachten sind.

Beispiele:

- Mitgliederverwaltung: grundsätzlich 3 Jahre nach Beendigung der Vereinsmitgliedschaft (Jahresende; Ablauf der dreijährigen Verjährungsfrist laut BGB); aber: Daten wie Name, Geschlecht, Geburtsdatum sind für steuerliche Zwecke 10 Jahre aufzubewahren (vgl. Art. 18 DS-GVO, Einschränkung der Verarbeitung).
- Jahresabschlussunterlagen (z. B. Lohnbuchhaltung, Kontoauszüge): 10 Jahre
- Unterlagen Arbeitszeit, Mutterschutz: 2 Jahre
- Wettkampfergebnisse (Ergebnis-, Bestenlisten): nach „angemessener Zeit“; unangemessen wäre beispielsweise eine Veröffentlichung im Internet über mehrere Jahre unter Angabe einzelner personenbezogener Daten (siehe auch unten zu Anmerkung 11 Punkt 4)

Bitte beachten Sie:

Wenn der Betroffene eine ausdrücklich erteilte Einwilligung widerruft, sind die Daten grundsätzlich unverzüglich zu löschen (*Recht auf Löschung bzw. „Vergessenwerden“*, Art. 17 DS-GVO).

Beispiel: Veröffentlichung einer Porträtaufnahme auf der Internetseite des Vereins (wenn die erforderliche Einwilligung nicht eingeholt wurde, muss der Verein dem Löschungsbegehren des Vereinsmitglieds natürlich ebenfalls umgehend nachkommen)

[11] Rechtsgrundlage (Rechtmäßigkeit der Datenverarbeitung gem. Art. 6 DS-GVO)

1. Einwilligung erforderlich

- Grundsätzlich ist für eine Verarbeitung personenbezogener Daten immer eine Einwilligung (= vorherige Zustimmung) erforderlich (zu Ausnahmen und Einschränkungen siehe nachfolgend Punkte 2 – 5).
- Achtung: Die Einwilligung ist nur dann wirksam, wenn sie
  - freiwillig und
  - für einen bestimmten, klar und verständlich beschriebenen Fall und
  - durch eine eindeutig bestätigende Handlung (z. B. schriftliche Erklärung, Ankreuzen einer Erklärung im Internet) abgegeben wurde;
  - die betroffene Person darüber informiert wurde, dass die Einwilligung jederzeit widerrufen werden kann, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung hierdurch berührt wird. *Achtung: Der Hinweis auf das Widerspruchsrecht muss von den anderen Informationen getrennt erfolgen, z. B. durch optische Hervorhebung mittels Rahmung oder Fettdrucks.*

- *Beispiel* Geburtstagsliste:

  Geburtstagsjubilaren darf nur „öffentlich“ gratuliert werden, wenn eine ausdrückliche Einwilligung vorliegt (z. B. im Aufnahmeantrag). Aus der Einwilligung muss hervorgehen, auf welche Weise konkret die Veröffentlichung erfolgen darf (z. B. nur in der internen Vereinszeitung oder etwa an einem auch von Nichtvereinsmitgliedern einsehbaren „schwarzen Brett“).

- Minderjährige:

  Wenn der Verein einen Erwerb der Mitgliedschaft oder die Anmeldung zu einer Sportveranstaltung über das Internet ermöglicht, dürfen Minderjährige hiervon erst ab Vollendung des 16. Lebensjahres ohne die Einwilligung der Sorgeberechtigten Gebrauch machen (vgl. Art. 8, 6 Abs. 1 a) DS-GVO).

- *Sonderfall* Gesundheitsdaten:

  Bei Gesundheitsdaten (z. B. im Rehasportverein) handelt es sich um eine besondere Kategorie personenbezogener Daten i. S. d. § 9 DS-GVO, für deren Verarbeitung es – abgesehen von eng definierten Ausnahmen – stets einer Einwilligung des Betroffenen bedarf.

2. Verarbeitung zur Begründung bzw. Erfüllung eines Vertrages erforderlich

- Die Datenkategorien, die in dem Musterverzeichnis „Mitgliederverwaltung“ erhoben werden, sind – abgesehen von der E-Mail-Adresse und der Telefonnummer – zur Erfüllung eines Vertrages erforderlich (bei der Vereinsmitgliedschaft handelt es sich, rechtlich gesehen, um einen Vertrag!). Ohne diese Angaben wäre eine ordnungsgemäße Mitgliederverwaltung ausgeschlossen oder zumindest stark eingeschränkt. Deshalb darf der Verein diese personenbezogenen Daten auch ohne ausdrückliche Einwilligung des Betroffenen verarbeiten.

- Bei Minderjährigen gilt dies entsprechend (vorausgesetzt, die Sorgeberechtigten haben dem Eintritt ihres Kindes in den Verein ausdrücklich zugestimmt). Die Mitgliederdaten dürfen beispielsweise auch ohne ausdrückliche Einwilligung an Dachverbände weitergegeben werden, um Lizenzen oder Spielerpässe ausstellen zu lassen.
  Hinweis: Um auf Nummer sicher zu gehen, empfiehlt es sich auch in diesen Fällen, rein vorsorglich die Einwilligung der Sorgeberechtigten einzuholen.

- „Gesundheitsdaten“ (z. B. im Rehasportverein) können ebenfalls zur Begründung bzw. Erfüllung eines Vertrages erforderlich sein. Da es sich um eine besondere Kategorie personenbezogener Daten i. S. d. § 9 DS-GVO handelt, ist dennoch stets eine Einwilligung des Betroffenen erforderlich!

3. Erfüllung einer rechtlichen Verpflichtung

Bei Vorliegen einer rechtlichen Verpflichtung zur Verarbeitung von personenbezogenen Daten ist eine Einwilligung der betroffenen Person nicht erforderlich.

Beispiele:

- Ausstellung von Spendenbescheinigungen: Name und Anschrift des Zuwendenden sind anzugeben (vgl. § 50 Einkommensteuer-Durchführungsverordnung).
- Beschäftigung von Arbeitnehmer/-innen: Verpflichtende Erhebung bestimmter Daten bei der Führung des Lohnkontos (u. a. auch die allgemeinen Besteuerungsmerkmale wie Kirchensteuermerkmale, vgl. § 4 Lohnsteuer-Durchführungsverordnung)

4. Wahrung berechtigter Interessen des Verantwortlichen

Wenn berechtigte Interessen des Vereins gegenüber den schutzwürdigen Interessen der betroffenen Person überwiegen, ist die Datenverarbeitung auch ohne ausdrückliche Einwilligung rechtmäßig. Dies gilt unter bestimmten Umständen auch für Veröffentlichungen im Internet.

Beispiele:

- Personenbezogene Daten von Vorstandsmitgliedern oder anderen Organen:
  Ohne Einwilligung dürfen in der Regel Name, Vorname oder eine Vereins-E-Mail-Adresse veröffentlicht werden (einer Einwilligung bedarf es hingegen bei der Veröffentlichung der privaten Post- und E-Mail-Adresse!). Ohne weiteres zulässig ist auch die Veröffentlichung von Wahlergebnissen.
- Wettkampfergebnisse (Ergebnis-, Bestenlisten):
  Jeder Sportverein hat in der Regel ein berechtigtes Interesse daran, die Leistungen seiner Sportler zu veröffentlichen (zunehmend nicht nur per Aushang im Verein, sondern auch im Internet). Ohne Einwilligung des Betroffenen darf der Verein jedoch nur den Namen, das Geschlecht, das Geburtsjahr und das Wettkampfergebnis veröffentlichen, außerdem den Verein bzw. die Mannschaft – das Geburtsdatum, die Nationalität oder die Adresse jedoch nur mit Einwilligung des Betroffenen! Zu beachten sind aber stets die Löschfristen (siehe oben zu Anmerkung 10).
  Hinweis: Bei Minderjährigen gelten die gleichen Grundsätze; dennoch sollte in diesen Fällen rein vorsorglich die Einwilligung der Sorgeberechtigten eingeholt werden!

5. Beispiele zur Veröffentlichung von Fotos im Internet

Bei Veröffentlichungen von personenbezogenen Daten im Internet ist besondere Vorsicht geboten. Dies gilt vor allem auch für Fotos. Hier muss man aber differenzieren:

a. Fotos im Verein (Erwachsene)

Grundsätzlich gelten die allgemeinen gesetzlichen Regelungen (KunstUrhG). Im Einzelnen gilt Folgendes:

- Fotos von Spielszenen: grundsätzlich keine Einwilligung erforderlich, wenn der Bezug zum Spiel erkennbar ist; anders aber z. B. bei anstößigen Fotos oder wenn ein einzelner Spieler gezielt fotografiert worden ist
- Fotos von Zuschauern: Veröffentlichung des Fotos ist ohne Einwilligung zulässig (auch wenn die Gesichter einzelner Zuschauer zu erkennen sind); anders aber, wenn einzelne Personen aus der Zuschauermenge „herangezoomt“ werden!
- Fotos von „Personen der Zeitgeschichte“ zu Besuch im Verein:
  Wenn z. B. ein hochrangiger Politiker, ein Schauspieler o. ä. den Verein besucht, können Fotos hiervon auch ohne Einwilligung der prominenten Person oder der mit dieser abgebildeten sonstigen Personen veröffentlicht werden.
- Mannschaftsfotos: Zumindest bei Veröffentlichung im Internet wird die Einholung der Zustimmung empfohlen (aus Beweisgründen schriftliche Einwilligung günstig).
- Fotos Verstorbener (z. B. in Vereinschronik): Bis zum Ablauf von 10 Jahren nach dem Tod müssen die Angehörigen einwilligen; danach können die Fotos problemlos veröffentlicht werden.

b. Fotos von Minderjährigen

- Spielszenen, Mannschaftsfotos: schriftliche Einwilligung aller Sorgeberechtigten dringend empfohlen
- Abbildung mit Personen der Zeitgeschichte: wie bei Erwachsenen grundsätzlich ohne Einwilligung zulässig

[12] Informationspflicht

a) Worüber ist der Betroffene zu informieren?

Gem. Art. 13 Abs. 1 DS-GVO hat der Verein die betroffene Person zum Zeitpunkt der Erhebung der Daten umfassend zu informieren über:

- Namen und Kontaktdaten des Verantwortlichen / dessen Vertreters
- Kontaktdaten eines Datenschutzbeauftragten, sofern vorhanden
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, und die Rechtsgrundlagen dafür
- die berechtigten Interessen des Verantwortlichen, wenn er Daten auf der Basis einer Interessenabwägung verarbeiten möchte
- Empfänger der Daten, wenn der Verantwortliche sie weitergeben möchte

Gem. Art. 13 Abs. 2 DS-GVO sind – ebenfalls zum Zeitpunkt der Erhebung der Datenerhebung – folgende Informationen zur Verfügung zu stellen:

- Dauer der Speicherung oder Kriterien für die Löschung
- Hinweis auf Recht auf Auskunft (Art. 15 DS-GVO), Berichtigung (Art. 16 DS-GVO), Löschung (Art. 17 DS-GVO), Einschränkung der Verarbeitung (Art. 18 DS-GVO), Datenübertragbarkeit (Art. 20 DS-GVO), Widerspruch (Art. 21 DS-GVO)
- Hinweis, dass eine Einwilligung jederzeit grundlos widerrufen werden kann, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung hierdurch berührt wird (vgl. Art. 7 DS-GVO)
- Hinweis auf Beschwerderecht bei der Aufsichtsbehörde (Art. 77 DS-GVO)

b) Wie bzw. wo hat die Information zu erfolgen?

Der Verein kann die Informationen auf seiner *Internetseite* veröffentlichen (z. B. Datenschutzbeauftragter) oder aber über die *Satzung* (z. B. die Informationen gem. § 13 Abs. 2 DS-GVO) oder den *Aufnahmeantrag* informieren. Im Einzelfall kann auch eine *direkte Information* an betroffene Vereinsmitglieder angemessen sein.

c) Wann entfällt die Informationspflicht?

Wenn der Betroffene bereits über die Informationen gem. Art. 13 Abs. 1 und Abs. 2 DS-GVO verfügt.

Beispiel Wettkampfergebnisse:

Dem Betroffenen dürfte in der Regel klar sein, warum der Verein ein Interesse an der Veröffentlichung der Wettkampfergebnisse hat (Zweck der Datenverarbeitung). Hierüber muss der Verein ihn daher nicht gesondert informieren. (Dennoch besteht natürlich die Möglichkeit, dass der Verein z. B. in der Satzung darüber informiert, dass – und ggf. unter welchen Voraussetzungen – Ergebnislisten veröffentlicht werden.)

d) Was ist, wenn die Daten für einen anderen Zweck weiterverarbeitet werden?

In diesem Fall sind dem Betroffenen vorher Informationen über den anderen Zweck und die maßgeblichen Informationen gemäß Art. 13 Abs. 2 DS-GVO zur Verfügung zu stellen.

Beispiel: *Mitgliederdaten sollen nicht nur für Vereinsverwaltung genutzt werden, sondern an einen Sponsor zwecks Werbemaßnahmen weitergegeben werden.*

Hinweise:

- Die Informationspflicht ist in Art. 13 DS-GVO geregelt, wenn personenbezogene Daten bei der betroffenen Person erhoben werden. Werden personenbezogene Daten hingegen nicht bei der betroffenen Person erhoben, so ist Art. 14 DS-GVO anzuwenden.

- Kommt es zu Verletzungen des Schutzes personenbezogener Daten (z. B. Vernichtung, Verlust oder unbefugte Offenlegung), sind die Aufsichtsbehörde sowie die betroffenen Personen unverzüglich zu informieren (Meldepflicht gem. Art. 33 DS-GVO; Benachrichtigungspflicht gem. Art. 34 DS-GVO).

[13] Technische und Organisatorische Maßnahmen (TOM)

In das Verarbeitungsverzeichnis ist eine allgemeine Beschreibung der geeigneten technischen organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DS-GVO aufzunehmen (vgl. Art. 30 Abs. 1 g) DS-GVO).

Zu beschreiben sind die Maßnahmen, die im Einzelfall erforderlich sind, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Umfang, Umstände und Zweck der Vereinbarung einerseits; Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten andererseits). Nötig ist immer eine einzelfallbezogene Betrachtung.

Die TOM können direkt in dem Verzeichnis angegeben werden (siehe Musterbeispiel). Zulässig ist aber auch der Verweis auf ein IT-Sicherheitskonzept, in welchem die entscheidenden (Einzelfall-)Fragen dann aber bezogen auf alle Verarbeitungstätigkeiten zu behandeln sind.

[14] Vertraulichkeit

Ist gewährleistet, dass Informationen vor Unbefugten verborgen werden?

[15] Integrität

Ist gewährleistet, dass die Informationen unversehrt bleiben (Schutz vor Veränderungen oder Manipulation der Daten)?

[16] Verfügbarkeit und Belastbarkeit

Ist gewährleistet, dass die vorhandenen Daten bei Bedarf jederzeit genutzt werden können? Ist gewährleistet, dass es ausreichende Speicher-, Zugriffs- und Leitungskapazitäten gibt?

[17] Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Gibt es für diesen Fall entsprechende Sicherungssysteme (Backup-Konzepte oder mehrfache Datenspeicherung)?

[18] Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Gibt es regelmäßige Prüfungen – z. B. durch den Datenschutzbeauftragten? Ist in einem Sicherheitskonzept die regelmäßige Überprüfung festgelegt?

[19] Verschlüsselung

Eine Verschlüsselung ist bei mobilen Geräten sowie standortfesten Geräten vor allem dann geboten, wenn besonders sensible Daten wie Gesundheitsdaten betroffen sind.

Bei mobiler Kommunikation (E-Mails) ist in der Regel immer eine Verschlüsselung erforderlich, da die Daten ansonsten quasi offen einsehbar sind!

Zu Einzelheiten wird vor allem auf die Ausführungen des Bayerischen Landesamtes für Datenschutzaufsicht verwiesen (siehe *Literaturhinweis*).

[20] Pseudonymisierung

Darunter versteht man das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren (so eine Definition aus dem BDSG-alt; vgl. auch Art. 4 Ziffer 5 DS-GVO).

[21] Datenschutz-Folgenabschätzung (DS-FA)

- Der Verein hat *vor* der Datenverarbeitung eine „Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten“ durchzuführen, wenn die Datenverarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Pflichten natürlicher Personen zur Folge“ hat (vgl. Art. 35 DS-GVO).
- Dies ist gemäß Art. 35 Abs. 3 DS-GVO vor allem dann der Fall, wenn
  - (Gesundheits-)Daten im Leistungssportbereich verarbeitet werden (vgl. Art. 35 Abs. 3 a) DS-GVO: „systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen“;
  - besondere Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DS-GVO (z. B. Gesundheitsdaten) *„umfangreich“* verarbeitet werden; aber nur, wenn Risiken für die Rechte und Freiheiten natürlicher Personen bestehen;
    Dürfte bei Rehasportvereinen in der Regel nicht der Fall sein.
  - besondere Kategorien personenbezogener Daten gem. Art. 10 DS-GVO (z. B. Führungszeugnisse) *„umfangreich“* verarbeitet werden.
    Dürfte auch bei Vereinen, die Führungszeugnisse ihrer Mitarbeiter (z. B. Übungsleiter) verlangen, in der Regel nicht der Fall sein.

Die Durchführung von Datenschutz-Folgeabschätzungen dürfte in den meisten Vereinen in der Regel nicht erforderlich sein!

Hinweis:

Wenn eine Datenschutz-Folgenabschätzung nicht erforderlich ist, ist dies entsprechend zu dokumentieren!