

# **Handlungsleitfaden / Maßnahmenkatalog** **zur Umsetzung der neuen EU-Datenschutz-Grundverordnung (DSGVO)**

## **1. Allgemeines / Vorwort**

Im Zuge des Inkrafttretens der EU-DSGVO zum 25. Mai 2018 sind die bisherigen Prozesse in Zusammenhang mit der Verarbeitung von personenbezogenen Daten innerhalb des Vereins einer Prüfung zu unterziehen und diesbezügliche Abläufe entsprechend zu dokumentieren.

Der Datenschutz betrifft personenbezogene Daten: Das sind alle Einzelangaben über die persönlichen oder sachlichen Verhältnisse! In Vereinen betrifft das beispielsweise vor allem Mitglieder, daneben aber auch Spender, Klienten oder Kunden sowie Mitarbeiter beziehungsweise Arbeitnehmer. Typischerweise erhoben werden beispielsweise Name und Anschrift, Kommunikationsdaten, Geburtsdatum, Eintrittsdatum, Bankverbindung, Wettkampfdaten, Lizenzen, Ehrungen. All das sind personenbezogene Daten: Die Art der Erfassung (digital oder auf Papier) spielt dabei keine Rolle!

Weitere Informationen können Sie beispielsweise auch unter [www.vibss.de](http://www.vibss.de) oder [www.lsb-nrw.de](http://www.lsb-nrw.de) finden; u.a. einige Mustervorlagen, die aber auch in der als Anlage beigefügten Übersichtsdatei „Datenschutz-im-Sportverein“ enthalten sind.

Für alle Informationen kann der Westdeutsche Tischtennis-Verband e.V. (WTTV) keinerlei Gewähr übernehmen, sie sind nach bestem Wissen und Gewissen zusammengestellt. Auf Grund der unterschiedlichen Struktur der einzelnen Vereine kann es keinen wirklich einheitlichen Maßnahmenplan zur Einhaltung der Bestimmungen aus der EU-DSGVO geben. Hier muss jeder Verein (nicht eine Abteilung), der die Verantwortung für die Maßnahmen hat, seinen individuellen Weg finden.

## **2. Ist für alle personenbezogenen Daten die Zulässigkeit der Verarbeitung geprüft worden?**

Eine Einwilligung in die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nicht erforderlich, soweit der Verein personenbezogene Daten für folgende Zwecke erhebt, verarbeitet und nutzt:

- **Verfolgung der Vereinsziele** (siehe Satzung, in der Regel also u.a. die Daten zur Organisation und Durchführung des Spielbetriebs)
- **Betreuung und Verwaltung der Vereinsmitglieder** (wie etwa Name, Anschrift, in der Regel auch das Geburtsdatum, ferner Bankverbindung, Bankleitzahl und Kontonummer, erhaltene Ehrungen, Lizenzen, Ergebnisse von Wettbewerben)
- **berechtigtes Interesse des Vereins** (beispielsweise statistische Informationen zu den Mitgliedern, um den Verein weiterzuentwickeln und zu organisieren [beispielsweise: Auswertung über Teilnahmen an Trainingsveranstaltungen, Vereinschronik, Organisation von vereinsinternen Arbeitseinsätzen, Daten für Spendenaufrufe zur Erreichung der eigenen Ziele des Vereins, Datenübermittlung an Dachverbände – soweit diese dort benötigt werden, um die Vereinsziele des übermittelnden Vereins oder um die Ziele des Dachverbandes zu verwirklichen]), sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person entgegenstehen.

Es empfiehlt sich nicht, Einwilligungen für Datenverarbeitungsmaßnahmen einzuholen, die bereits aufgrund einer gesetzlichen Erlaubnis möglich sind – beispielsweise, wenn Daten im Rahmen einer vertraglichen Beziehung erhoben werden. Bei Vereinen ist diese vertragliche Beziehung die Mitgliedschaft. Die für die Mitgliederverwaltung erforderlichen Daten (siehe oben) sowie für die Organisation des Spielbetriebs (beispielsweise Wettkampfdaten, Klasseneinteilung, Lizenzen) dürfen verarbeitet werden, da diese zur Erfüllung der Vertragsbeziehung, d.h. der Vereinsmitgliedschaft, erforderlich sind.

Aktion(en) des Vereins:

- Überprüfung der Zulässigkeit der Verarbeitung
- (gegebenenfalls) Einholen der Einwilligung von Betroffenen (=> siehe Ziffer 3.)

### **3. Gibt es im Aufnahmeantrag Hinweise auf den Umgang mit personenbezogenen Daten im Verein?**

Es empfiehlt sich, schon beim Vereinsbeitritt in Form einer Erklärung zum Datenschutz darauf hinzuweisen, zu welchem Zweck und auf welcher Grundlage welche personenbezogenen Daten von Seiten des Vereins erhoben und verarbeitet werden. In diesem Zuge ist es ratsam, bereits bei der Aufnahme von Mitgliedern, sich zur Verarbeitung von personenbezogenen Daten im Verein eine entsprechende schriftliche Einwilligung von den Betroffenen einzuholen, die den gesetzlichen Vorgaben zu Inhalt und Gestaltung von Einwilligungen, insbesondere den Betroffenenrechten, entspricht. Altmitgliedern kann man über die Vereinsmitteilungen eine allgemeine Information mit einer derartigen Einwilligungserklärung und dem Hinweis auf das jederzeitige Widerrufsrecht zukommen lassen. In Anlehnung an Ziffer 2. ist für Altmitglieder eine Einwilligung nur erforderlich, wenn der Verein in weitergehendem Maße personenbezogene Daten als unter Ziffer 2. beschrieben erhebt, verarbeitet und nutzt. Grundsätzlich gilt aber das Schriftformerfordernis einer Einwilligung.

Aktion(en) Verein:

- Erstellung einer Datenschutzerklärung
- Aufnahme der Datenschutzerklärung in den Aufnahmeantrag
- Erstellung einer Einwilligungserklärung für die Betroffenen
- (schriftliche) Einwilligung der Betroffenen
- Information(en) an Altmitglieder

### **4. Gibt es eine in der Vereinssatzung verankerte Datenschutzrichtlinie?**

Eventuell gibt es bereits Regelungen in der Satzung zum Umgang mit personenbezogenen Daten (Grundlage/Ermächtigung) beziehungsweise zum Datenschutz allgemein. Mit einer Datenschutzklausel in der Satzung kann der Verein den Informationspflichten gemäß Artikel 13 EU-DSGVO (zumindest teilweise) entsprechen. In einer Datenschutzrichtlinie kann festgeschrieben werden, welche Daten im Verein durch welche Funktionen erhoben und verarbeitet werden, wer Zugriff auf welche Kategorien von Daten hat und welche technischen Maßnahmen zum Schutz der Daten ergriffen werden. Die Regelungen in der Datenschutzrichtlinie können sich eng an das Verzeichnis der Verarbeitungstätigkeiten (siehe Ziffer 7.) anlehnen.

Aktion(en) Verein:

- Überprüfung der Satzung
- (gegebenenfalls) Update der Satzung
- Nachweis über die ordnungsgemäße Erfüllung der Informationspflicht(en) gegenüber Betroffenen
- Sicherstellung der zeitnahen und korrekten Reaktion auf Auskunftsverlangen von Betroffenen

### **5. Sind die Daten im Verein ausreichend geschützt?**

Der Verein muss dafür Sorge tragen und überprüfen, ob die eigenen technischen und organisatorischen Maßnahmen (sogenannte TOMs) der Datenverarbeitung geeignet sind, Datensicherheit zu gewährleisten. Bei allen Datenverarbeitungsvorgängen muss demnach überprüft werden, ob ausreichende Sicherheitsvorkehrungen getroffen worden sind. Dies reicht beispielsweise von Regelungen der Zugangskontrolle zu den Daten (=> Wer hat tatsächlich Zugriff auf die Daten?), des Passwortschutzes (passwortgeschützte Nutzer-Accounts für Personen, die die Daten verarbeiten), zu Anweisungen bezüglich der Eingabe und Löschung bis hin zur Sicherstellung der Verfügbarkeit von Daten (beispielsweise ein Firewall-System oder auch die Verschlüsselung der Daten).

Aktion Verein:

- Überprüfung (und Dokumentation) der TOMs zur Gewährleistung der Datensicherheit

## **6. Ist ein Datenschutzbeauftragter im Verein erforderlich?**

Wenn mindestens zehn Personen im Verein ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind, muss ein Datenschutzbeauftragter im Verein bestellt werden. Nach Bestellung eines Datenschutzbeauftragten muss dieser der zuständigen Aufsichtsbehörde namentlich gemeldet werden.

Aus der Praxis:

Wenn im Verein lediglich der Vorsitzende, der Schatzmeister, der Sportwart und zwei Übungsleiter Zugang zu personenbezogenen Daten haben, muss kein Datenschutzbeauftragter benannt werden. Dennoch hat der Verein die datenschutzrechtlichen Regelungen zu beachten: Dann liegt die Verantwortung beim Vorstand nach § 26 BGB!

Aktion(en) Verein:

- (möglicherweise) Benennung eines Datenschutzbeauftragten
- Meldung an die zuständige Aufsichtsbehörde

## **7. Gibt es ein Verzeichnis der Verarbeitungstätigkeiten im Verein?**

Es ist davon auszugehen, dass auch Vereine ein Verzeichnis aller Verarbeitungstätigkeiten erstellen und regelmäßig aktualisieren müssen, da bereits die Mitgliederverwaltung im Verein in der Regel systematisch und nicht nur gelegentlich erfolgt. Ein solches Verfahrensverzeichnis kann beispielsweise in Form einer tabellarischen Auflistung erfolgen, in der man neben den wichtigsten Eckdaten zum Verein und den Verantwortlichen beispielsweise auch Informationen darüber aufführt, von welchen Personen welche personenbezogenen Daten zu welchen Zwecken auf welcher Grundlage von wem im Verein verarbeitet werden.

Aktion Verein:

- Erstellung eines Verfahrensverzeichnisses

## **8. Sind alle Personen, die im Verein personenbezogene Daten bearbeiten, auf das Datengeheimnis verpflichtet worden?**

Jeder, der im Auftrag des Vereins mit personenbezogenen Daten in Berührung kommt, muss auf das Datengeheimnis schriftlich verpflichtet werden. Dazu sollte ein entsprechendes Formblatt vorbereitet werden, um dies per Unterschrift inhaltlich bestätigen zu lassen. Die Verpflichtungserklärung sensibilisiert die Mitarbeiter/innen im Umgang mit den personenbezogenen Daten.

Aktion(en) Verein:

- Erstellung eines Formblattes
- (schriftliche) Verpflichtung der Betroffenen auf das Datengeheimnis

## 9. Gibt es einen Ablaufprozess bei Datenpannen und Zuständigkeiten hierzu?

Es besteht nun auch für Vereine die Pflicht, eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde zu melden. Dies bedeutet, dass im Verein im Vorfeld ein Prozessablauf, ein Muster für die Meldung und die zuständige Person im Verein bestimmt werden sollten.

Aus der Praxis:

Es ist für den Verein festzulegen, wie im Fall, dass beispielsweise der Vereins-PC oder der Karteikasten mit den Mitgliederdaten aus dem Vereinsheim entwendet wurde, vorgegangen werden soll: Wer ist umgehend zu informieren, sobald der Verlust der Daten festgestellt wurde? Vorsitzender oder Datenschutzbeauftragter? Wer füllt das vorher festgelegte Muster für die Meldung aus und übersendet es an die Datenschutzaufsichtsbehörde? Wer informiert die betroffenen Personen, um deren Daten es geht?

In Abhängigkeit davon, ob beispielsweise besonders schützenswerte personenbezogene Daten (beispielsweise Gesundheitsdaten) im Verein verarbeitet oder risikobehaftete Datenverarbeitungsprozesse (beispielsweise sehr große Datenmengen) durchgeführt werden, ist ergänzend eine schriftliche Dokumentation darüber erforderlich, dass innerhalb des Vereins vorab eine Datenschutz-Folgeabschätzung durchgeführt wurde. Eine Datenschutz-Folgeabschätzung dürfte aber bei Vereinen nur in den seltensten Fällen notwendig sein.

Aktion(en) Verein:

- Festlegung eines Prozessablaufes, eines Musters für die Meldung und der personellen Zuständigkeit bei Datenschutzverletzungen
- (gegebenenfalls) Meldung an die zuständige Aufsichtsbehörde
- (gegebenenfalls) Information an die betroffene Person
- (gegebenenfalls) Erstellung einer Dokumentation über vorherige Datenschutz-Folgeabschätzung

## 10. Gibt es im Verein Vereinbarungen mit Dritten zur Auftragsdatenverarbeitung?

Wenn der Verein sich bei der Verarbeitung personenbezogener Daten externer Dienstleister bedient, ist hierzu eine Vereinbarung zur Auftragsdatenverarbeitung auf der Grundlage der gesetzlichen Bestimmungen zwingend erforderlich.

Aktion(en) Verein:

- Prüfung des Erfordernisses zu Vereinbarungen zur Auftragsdatenverarbeitung
- (gegebenenfalls) Vertragsabschluss zur Auftragsdatenverarbeitung

**WESTDEUTSCHER TISCHTENNIS-VERBAND E.V.**

**gez. Helmut Joosten**  
Präsident

**gez. Michael Keil**  
Geschäftsführer