Auftragsverarbeitung: Was ist das und wann liegt sie vor?

Die meisten Sportvereine setzen externe Dienstleister ein, etwa für die Mitgliederverwaltung, das Hosting der Vereinswebsite oder die Lohnabrechnung. Werden dabei personenbezogene Daten **im Auftrag** des Vereins verarbeitet, spricht man von Auftragsverarbeitung (AVV) gem. Art. 28 DSGVO. Der Verein bleibt dabei „Verantwortlicher“, während der Dienstleister als „Auftragsverarbeiter“ wie ein **verlängerter Arm des Vereins rein weisungsgebunden** tätig wird.

Beispiel

Ein Verein beauftragt einen IT-Dienstleister mit dem Hosting einer Mitgliederverwaltungssoftware. Der Dienstleister darf die Daten nur nach Weisung des Vereins verarbeiten. Dazu schließen der Verein und der IT-Dienstleister einen Vertrag, der alle Einzelheiten zum Umgang der Daten und der Weisungsabhängigkeit regelt.



Anforderungen an die Auftragsverarbeitung

Vor Beginn der Zusammenarbeit muss ein **schriftlicher Vertrag** abgeschlossen werden, der die Rechte und Pflichten beider Seiten regelt. Dieser Vertrag wird in der Regel von den Dienstleistern als Teil der Allgemeinen Geschäftsbedingungen (AGB) oder als Zusatz zu eurem Vertrag bei der Beauftragung abgeschlossen. Sollte dies ausnahmsweise nicht der Fall sein, z.B. wenn Ihr eine nicht standardisierte Leistung beauftragt, könnt ihr einen Muster-Vertrag der für euch zuständigen Aufsichtsbehörde herunterladen, auf euren Anwendungsfall anpassen und mit dem Dienstleister vereinbaren.

In diesem Ausnahmefall könnte es sich auch lohnen, die Beratungsleistung eines Spezialisten im Datenschutz in Anspruch zu nehmen.

Beispiel

Der Verein beauftragt eine individuelle App für Smartphones, die keine Standardmodule verwendet, sondern Nutzerdaten für neu programmierte Funktionen verarbeitet. Er verpflichtet den Dienstleister per Vertrag zur rechtmäßigen und weisungsgebundenen Verarbeitung. Auch der Verbleib der Daten nach Beendigung des Vertrages wird darin geregelt.



IT-Sicherheit in der Verarbeitung

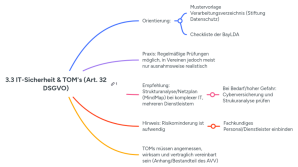
Auch in der Zusammenarbeit mit Auftragsverarbeitern ist der Verein verpflichtet, angemessene geeignete technische und organisatorische Maßnahmen (**TOMs**) nach Art. 32 Abs. 1 DSGVO zu treffen. Diese müssen also als Bestandteil oder Anhang zum Vertrag mit euch vereinbart werden. Das Thema ist sehr umfangreich und erfordert oft besonderes Fachwissen. Gleichwohl ist die IT-Sicherheit in der Praxis immer bedeutsamer, da Angriffe **immer gezielter und professioneller durchgeführt** werden. Dabei werden sowohl technische als auch klassische "menschliche" Schwächen gnadenlos ausgenutzt, meist mit dem Ziel der Datenerpressung zur Zahlung von Geld an die Täter.

Wenn ihr eine konkrete Vorstellung von TOMs erhalten möchtet, lohnt sich ein Blick in Richtung der staatlichen Organisationen. Die Stiftung Datenschutz der Bundesregierung hat bspw. eine Vorlage mit Hinweisen erstellt, die ihr als "Mustervorlage Verarbeitungsverzeichnis" hier abrufen könnt. Wenn ihr eine umfassende Checkliste sucht, um eine noch konkretere Vorstellung von solchen Maßnahmen zu erhalten, bietet sich die Checkliste der Datenschutzaufsichtsbehörde Bayern an.

Die Einhaltung dieser Maßnahmen durch den Dienstleister kann zwar regelmäßig überprüft und dokumentiert werden, wird in der Praxis jedoch aus Kapazitätsgründen nur sehr selten und nur von größeren Gesellschaften mit eigener Datenschutzabteilung und kritischen Verarbeitungen durchgeführt. Für klassische Vereine dürfte die **Kontrolle der Dienstleister nur in Ausnahmefällen** und nach vorheriger professioneller Beratung in Betracht kommen.

Ergänzend kann es bei Interesse an einer Cyberversicherung, einer umfassenden Vereins-IT oder mehreren Dienstleistern sinnvoll sein, eine **Strukturanalyse** durchzuführen und hierfür einen Netzplan in Form einer MindMap zu erstellen. Für den Abschluss einer Cyberversicherung ist das teilweise auch Voraussetzung. Die anschließende Risikomitigation ist jedoch sehr zeitaufwendig und erfordert viele Fachkenntnisse. Sie sollten daher nur von fachkundigem Personal durchgeführt werden.

In der Regel muss der Verein also einen Dienstleister beauftragen, wenn er das Thema IT-Sicherheit auf ein neues Level heben möchte und/oder eine Cyberversicherung in Anspruch nehmen will.



Datenübermittlung in Drittländer

Werden personenbezogene Daten an Dienstleister außerhalb der EU/des EWR (sog. Drittländer) übermittelt, gelten besondere Anforderungen nach Kapitel V DSGVO (Art. 44 ff. DSGVO). Ziel ist es, das **europäische Datenschutzniveau auch im Drittland zu gewährleisten**.

Mögliche Rechtsgrundlagen für den Drittlandstransfer sind insb. folgende:

- **Angemessenheitsbeschluss** der EU-Kommission, einsehbar hier Angemessenheit des Datenschutzes für Nicht-EU-Länder (z.B. für die Schweiz, Japan),
- Abschluss von **Standarddatenschutzklauseln** (SCC) mit dem Dienstleister (Implementing decision - 2021/914 - EN - EUR-Lex),
- Binding Corporate Rules (BCR) bei internationalen Konzernen,

- wenige Ausnahmen sind möglich, z.B. wenn die Übermittlung zur Vertragserfüllung erforderlich ist (z.B. Buchung eines Sporthotels im Ausland).

Beispiel

Der Verein will einen US-amerikanischen Cloud-Dienst nutzen. Da für die USA ein **Angemessenheitsbeschluss** vorliegt, prüft der Verein zusätzlich die Zertifizierung des Cloud Dienstleisters im **Data Privacy Framework**, anderenfalls unterlässt er die Nutzung oder holt sich professionelle Unterstützung bei der Verhandlung von bspw. **Standardvertragsklauseln** mit dem Anbieter.



Praktische Hinweise für Vereine

- Sofern Daten im Auftrag des Vereins verarbeitet werden, **muss** ein AVV abgeschlossen werden. In der Regel wird dies bereits durch die Dienstleister mit angeboten und abgeschlossen, anderenfalls muss der Verein sich darum kümmern.

- Informationen in den Datenschutzhinweisen bzw. der Datenschutzordnung über eingesetzte Dienstleister und etwaige Drittlandtransfers sind aus Transparenzgründen sinnvoll.

- Bei Drittlandtransfer: Angemessenheit des Datenschutzes für Nicht-EU-Länder prüfen sowie bei US-Transfer zusätzlich, ob die Unternehmen hier gelistet sind: Data Privacy Framework

BEACHTE: Ein Drittlandstransfer sollte nur in Staaten erfolgen, für die ein **Angemessenheitsbeschluss** vorliegt. Alles andere erfordert viel Fachwissen und eine Verhandlung mit dem Dienstleister, in der Regel auf einer anderen Sprache. Das überfordert die meisten Vereine, nimmt viel Zeit und Aufwand in Anspruch und bringt nur selten angemessenen Ertrag.



Details

Autor:
Sandro Geil

zuletzt aktualisiert:
Februar 2026

Quelle:

Art. 28 DSGVO

Art. 32 Abs. 1 DSGVO