Data Processing Agreement (DPA)

Version: 2026.1

Gueltig ab: March 8, 2026

Auftragnehmer: Julian Meyer, IT-Solutions, Christian-Dierig-Straße 7, 86157 Augsburg, Deutschland

Kontakt: mail@shooterium.de, +49 155 63179142

1. Vertragsparteien und Gegenstand

Auftragnehmer / Processor:

Julian Meyer, IT-Solutions, Christian-Dierig-Straße 7, 86157 Augsburg, Deutschland

Auftraggeber / Controller:

Der jeweilige Verein, der die Plattform Shooterium nutzt und diesen Vertrag annimmt.

Dieser Data Processing Agreement (DPA) konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien für Verarbeitungen personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers im Zusammenhang mit der Bereitstellung und dem Betrieb von Shooterium durchführt.

Der DPA ergänzt den zugrunde liegenden Nutzungs- bzw. Hauptvertrag. Im Fall eines Widerspruchs zwischen diesem DPA und dem Hauptvertrag geht dieser DPA für die Verarbeitung personenbezogener Daten vor.

2. Dauer, Art und Zweck der Verarbeitung

Die Verarbeitung beginnt mit der Nutzung der Plattform durch den Auftraggeber und läuft für die Dauer des Hauptvertrags sowie darüber hinaus nur, soweit gesetzliche Aufbewahrungs- oder Nachweispflichten bestehen.

Die Verarbeitung dient insbesondere:

- der Bereitstellung eines SaaS-Portals für Vereins-, Mitglieder-, Rollen- und Berechtigungsverwaltung,
- der Organisation von Veranstaltungen, Wettkämpfen, Kursen und Anmeldungen,
- der Verwaltung von Beitritts-Anfragen, Teilnehmerdaten und Kommunikation,
- der Bereitstellung vereinsbezogener Funktionsbereiche wie Schießbuch- oder Gastverwaltungsfunktionen,
- der Sicherstellung von Betrieb, Sicherheit, Support, Fehleranalyse und Wiederherstellung.

3. Kategorien betroffener Personen und Daten

Betroffene Personen können insbesondere sein:

- Vereinsvorstände, Administratoren und sonstige Ansprechpartner,
- Mitglieder und Nutzerkonten des Vereins,
- Veranstaltungsorganisatoren, Trainer, Helfer und Teilnehmer,
- Gäste, Interessenten und Personen aus Beitritts- oder Kontaktprozessen.

Datenkategorien können insbesondere umfassen:

- Stamm- und Identifikationsdaten (Name, Geburtsdatum und Adresse),
- Kontakt- und Kommunikationsdaten (Email und Telefonnummer),
- Vereins-, Rollen- und Berechtigungsdaten,
- Veranstaltungs-, Buchungs- und Teilnahmedaten,
- Protokoll-, Sicherheits- und Nutzungsdaten,
- vom Auftraggeber eingestellte Freitext- oder Notizdaten.

Eine Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO ist nicht Vertragszweck. Soweit der Auftraggeber entsprechende Daten dennoch über die Plattform verarbeitet, bleibt er für die rechtliche Zulässigkeit, Information der Betroffenen und etwaige zusätzliche Schutzmaßnahmen verantwortlich.

4. Weisungsgebundenheit

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, soweit nicht gesetzliche Pflichten eine abweichende Verarbeitung verlangen.

Allgemeine Produktfunktionen, Konfigurationen innerhalb der Anwendung, Supportanfragen des Auftraggebers sowie die Auswahl aktiv genutzter Features gelten als dokumentierte Weisungen im Rahmen dieses DPA und des Hauptvertrags.

Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Der Auftragnehmer kann die Ausführung einer Weisung bis zur Bestätigung aussetzen, soweit dies sachlich erforderlich ist.

Hält der Auftragnehmer eine Weisung für datenschutzrechtlich unzulässig, informiert er den Auftraggeber unverzüglich. Bis zur Klärung darf der Auftragnehmer die betroffene Verarbeitung aussetzen.

5. Vertraulichkeit und Berechtigungskonzept

Der Auftragnehmer stellt sicher, dass nur solche Personen Zugriff auf personenbezogene Daten erhalten, die diese zur Erfüllung ihrer Aufgaben benötigen. Diese Personen sind auf Vertraulichkeit verpflichtet oder unterliegen einer gesetzlichen Verschwiegenheitspflicht.

Zugriffsrechte werden rollenbasiert und nach dem Need-to-know-Prinzip vergeben. Administrative Zugriffe auf Produktivsysteme werden auf einen engen, erforderlichen Personenkreis begrenzt.

6. Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen (TOMs) nach Art. 32 DSGVO. Er darf diese Maßnahmen weiterentwickeln und an den Stand der Technik anpassen, solange das vertraglich geschuldete Sicherheitsniveau nicht unterschritten wird.

Wesentliche Änderungen mit erheblicher Auswirkung auf das Schutzniveau werden dokumentiert und dem Auftraggeber auf Anfrage erläutert.

7. Unterstützung bei Betroffenenrechten

Der Auftragnehmer unterstützt den Auftraggeber nach Maßgabe des Art. 28 Abs. 3 lit. e DSGVO durch geeignete technische und organisatorische Maßnahmen dabei, Anträge betroffener Personen zu bearbeiten.

Soweit eine Unterstützung über die vertraglich vereinbarten Standardleistungen hinausgeht, kann der Auftragnehmer den hierdurch entstehenden angemessenen Aufwand gesondert nach vorheriger Ankündigung abrechnen, sofern die Unterstützung nicht gesetzlich unentgeltlich geschuldet ist.

8. Unterstützung bei Sicherheit, Vorfällen und Folgenabschätzungen

Der Auftragnehmer unterstützt den Auftraggeber nach Art. 28 Abs. 3 lit. f DSGVO in angemessenem Umfang bei:

- der Bewertung und Behandlung von Sicherheitsvorfällen,
- der Erfüllung von Melde- und Benachrichtigungspflichten,
- Datenschutz-Folgenabschätzungen und Konsultationen von Aufsichtsbehörden,

soweit dies unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer verfügbaren Informationen möglich ist.

Erkennt der Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten im Verantwortungsbereich des Auftragnehmers, informiert er den Auftraggeber unverzüglich nach Bekanntwerden.

9. Unterauftragsverarbeiter

Der Auftraggeber erteilt eine allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern. Die aktuell eingesetzten Unterauftragsverarbeiter werden öffentlich unter https://dev.shooterium.de/legal/subprocessors veröffentlicht.

Der Auftragnehmer darf Unterauftragsverarbeiter hinzufügen, ersetzen oder austauschen, sofern diese ein angemessenes Datenschutzniveau gewährleisten. Über wesentliche Änderungen der Liste informiert der Auftragnehmer durch Aktualisierung der veröffentlichten Liste in angemessener Vorlaufzeit.

Ein Widerspruch des Auftraggebers ist nur aus wichtigen, konkret darzulegenden datenschutzrechtlichen Gründen zulässig. Erfolgt keine Einigung, steht beiden Parteien hinsichtlich der betroffenen Leistung ein außerordentliches Kündigungsrecht zu.

Der Auftragnehmer legt den Unterauftragsverarbeitern die datenschutzrechtlich erforderlichen Pflichten inhaltlich entsprechend diesem DPA auf.

10. Drittlandtransfers

Eine Verarbeitung soll vorrangig innerhalb der EU bzw. des EWR erfolgen. Soweit für einzelne Infrastruktur- oder Sicherheitsleistungen Zugriffe oder Datenübermittlungen in Drittländer erforderlich sind, erfolgt dies nur auf Grundlage eines nach Kapitel V DSGVO zulässigen Transfermechanismus, insbesondere EU-Standardvertragsklauseln und, soweit einschlägig, ergänzender Schutzmaßnahmen oder eines Angemessenheitsbeschlusses.

Der Auftragnehmer schuldet keinen Ausschluss sämtlicher Drittlandbezüge, soweit solche für standardisierte Infrastruktur- oder Sicherheitsleistungen technisch oder organisatorisch nicht vollständig vermeidbar sind und ein zulässiger Transfermechanismus besteht.

11. Nachweise und Audits

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die Informationen zur Verfügung, die erforderlich sind, um die Einhaltung dieses DPA nachzuweisen.

Der Nachweis erfolgt vorrangig durch geeignete Unterlagen, Selbstauskünfte, Zertifizierungen, Auditberichte, technische Beschreibungen oder vergleichbare Nachweise. Nur soweit diese nicht ausreichen, kann der Auftraggeber eine weitergehende Prüfung verlangen.

Vor-Ort-Audits sind nur zulässig, wenn:

- ein konkreter Anlass besteht oder die Standardnachweise objektiv nicht ausreichen,
- sie mindestens 30 Kalendertage vorher angekündigt werden,
- sie während üblicher Geschäftszeiten erfolgen,
- Betriebs- und Geschäftsgeheimnisse sowie die Sicherheit anderer Kunden nicht beeinträchtigt werden,
- der Prüfende auf Vertraulichkeit verpflichtet ist.

Der Auftragnehmer kann Audits aus wichtigem Grund ablehnen oder von angemessenen Sicherheitsvorgaben abhängig machen. Soweit das Audit keinen durch den Auftragnehmer zu vertretenden erheblichen Datenschutzverstoß aufdeckt, trägt der Auftraggeber die angemessenen externen und internen Aufwände des Auftragnehmers.

12. Rückgabe und Löschung nach Vertragsende

Nach Beendigung der vertraglichen Leistungen löscht oder gibt der Auftragnehmer personenbezogene Daten des Auftraggebers nach dessen Wahl zurück, soweit keine gesetzlichen Aufbewahrungs- oder Nachweispflichten entgegenstehen.

Sicherungsmedien und Backups werden im Rahmen üblicher Lösch- und Überschreibzyklen entfernt. Bis zur endgültigen Löschung bleiben sie technisch geschützt und werden nicht für andere Zwecke verwendet.

13. Haftung und Verantwortungsabgrenzung

Die gesetzliche Verantwortungsverteilung nach DSGVO bleibt unberührt. Der Auftraggeber bleibt für die Rechtmäßigkeit der Datenverarbeitung, die Erfüllung eigener Informationspflichten, die Festlegung von Löschfristen, die Zulässigkeit der Inhalte und die Bewertung, ob besondere Datenkategorien verarbeitet werden, verantwortlich.

Soweit Unterstützungs-, Mitwirkungs- oder Prüfpflichten des Auftragnehmers gesetzlich auf das Erforderliche und Zumutbare begrenzt sind, gilt diese Begrenzung auch vertraglich. Eine über die gesetzlichen Vorgaben hinausgehende verschuldensunabhängige Haftung des Auftragnehmers wird nicht begründet.

14. Schlussbestimmungen

Diese Fassung des DPA trägt die Versionsnummer **2026.1** und gilt ab **March 8, 2026**.

Der Auftragnehmer darf diesen DPA für künftige Vertragsabschlüsse und Verlängerungen aktualisieren, sofern die Aktualisierung gesetzliche Anforderungen umsetzt, das Schutzniveau nicht unangemessen reduziert und dem Auftraggeber in geeigneter Weise zugänglich gemacht wird.

Die jeweils aktuelle Fassung ist unter https://dev.shooterium.de/legal/dpa.pdf als PDF abrufbar.

Anlage 1: Beschreibung der Verarbeitung

Punkt	Beschreibung
Gegenstand	Bereitstellung und Betrieb der Plattform Shooterium als webbasierter SaaS-Dienst
Zweck	Vereinsverwaltung, Nutzerverwaltung, Event- und Teilnehmerverwaltung, Kommunikation, Sicherheits- und Betriebsprozesse
Betroffene Personen	Vereinsmitglieder, Ansprechpartner, Nutzerkonten, Organisatoren, Teilnehmer, Gäste, Interessenten
Datenkategorien	Stamm-, Kontakt-, Rollen-, Organisations-, Event-, Kommunikations- und Protokolldaten
Verarbeitungshandlungen	Erheben, Erfassen, Strukturieren, Speichern, Auslesen, Übermitteln, Löschen, Sichern, Wiederherstellen
Häufigkeit	Laufend im Rahmen des Produktbetriebs

Anlage 2: Technische und organisatorische Maßnahmen (TOMs)

1. Zutrittskontrolle

- Hosting in professionellen Rechenzentren mit baulichen und organisatorischen Schutzmaßnahmen.
- Zugang zu Rechenzentrumsflächen nur für autorisierte Personen des jeweiligen Infrastrukturproviders.
- Einsatz von Videoüberwachung, Sicherheitszonen und physischer Zutrittskontrolle gemäß Providerstandard.

2. Zugangskontrolle

- Zugriff auf Produktivsysteme nur für berechtigte Administratoren.
- Einsatz starker Authentifizierungsmechanismen und, wo vorgesehen, Multi-Faktor-Authentifizierung.
- Trennung von persönlichen Accounts und administrativen Zugriffen.

3. Zugriffskontrolle

- Rollen- und berechtigungsbasierte Vergabe von Zugriffsrechten.
- Need-to-know-Prinzip für interne Zugriffe.
- Protokollierung sicherheitsrelevanter administrativer Vorgänge in angemessenem Umfang.

4. Weitergabe- und Übermittlungskontrolle

- Transportverschlüsselung bei Zugriffen auf die Plattform mittels TLS.
- Beschränkung externer Datenweitergaben auf vertraglich oder technisch erforderliche Empfänger.
- Drittlandtransfers nur auf Grundlage zulässiger Transfermechanismen.

5. Eingabekontrolle

- Nachvollziehbarkeit administrativer Änderungen und sicherheitsrelevanter Systemereignisse.
- Applikations- und Server-Logs zur Fehleranalyse, Missbrauchserkennung und Systemsicherheit.

6. Auftragskontrolle

- Vertragliche Bindung eingesetzter Unterauftragsverarbeiter.
- Auswahl von Dienstleistern mit dokumentierten Sicherheits- und Datenschutzmaßnahmen.
- Veröffentlichung der aktuellen Subprocessor-Liste auf der Website.

7. Verfügbarkeitskontrolle

- Regelmäßige Datensicherungen nach internem Sicherungskonzept.
- Schutz vor Datenverlust durch Backup-, Wiederherstellungs- und Monitoring-Prozesse.
- Maßnahmen zur Absicherung gegen typische Infrastruktur- und Netzwerkstörungen.

8. Belastbarkeit und Wiederherstellbarkeit

- Laufende Überwachung zentraler Dienste.
- Verfahren zur zeitnahen Wiederherstellung bei technischen Störungen.
- Nutzung redundanter oder skalierbarer Infrastrukturkomponenten, soweit für die jeweilige Betriebsumgebung vorgesehen.

9. Trennungsgebot

- Logische Trennung mandantenbezogener Daten innerhalb der Anwendung.
- Trennung von Entwicklungs-, Test- und Produktivumgebungen, soweit betrieblich vorgesehen.
- Zweckgebundene Verarbeitung und beschränkte interne Zugriffe.

10. Datenschutzmanagement und Incident Response

- Dokumentierte Prozesse zur Behandlung von Sicherheits- und Datenschutzvorfällen.
- Vertraulichkeitsverpflichtung der mit Daten befassten Personen.
- Regelmäßige Überprüfung und Weiterentwicklung von Sicherheitsmaßnahmen.

11. Privacy by Design / Default

- Grundsätzliche Ausrichtung auf Datensparsamkeit und rollenbasierte Zugriffssteuerung.
- Produktfunktionen werden so gestaltet, dass standardmäßig nur erforderliche Daten verarbeitet werden.
- Neue oder wesentlich geänderte Prozesse werden risikoorientiert bewertet.

Subunternehmerliste: https://dev.shooterium.de/legal/subprocessors