Vereinbarung zur Auftragsverarbeitung (AVV)

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

Dem im Angebot / Hauptvertrag bezeichneten Kunden / Verein

– nachfolgend **„Auftraggeber“** genannt –

und

Alexander Schütte (handball365.de)

Marktstraße 5, 48485 Neuenkirchen

E-Mail: info@handball365.de

– nachfolgend **„Auftragnehmer“** genannt –

– gemeinsam nachfolgend die **„Parteien“** genannt –

§ 1 Gegenstand und Dauer der Vereinbarung

1. Gegenstand dieses Vertrages ist die Durchführung von Verarbeitungen personenbezogener Daten durch den Auftragnehmer im Rahmen der Erbringung von SaaS-Dienstleistungen (Bereitstellung und Betrieb der Vereins-App, Administrations- und Sponsorenportal, Schnittstellenanbindung, Push-Dienste, Hosting) gemäß dem zugrundeliegenden Hauptvertrag / Angebot.
2. Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages. Er endet automatisch mit dem Ende des Hauptvertrages, es sei denn, aus den Bestimmungen dieses Vertrages ergibt sich darüber hinausgehend eine Verpflichtung.

§ 2 Konkretisierung des Auftragsinhalts (Gegenstand, Art und Zweck)

1. **Art und Zweck der Verarbeitung:** Bereitstellung, Betrieb, Wartung und Monitoring einer mobilen Vereins-Applikation sowie des dazugehörigen Administrationsportals; Übermittlung von Inhalten, Push-Benachrichtigungen und Spielbetriebsdaten an Endnutzer.
2. **Art der personenbezogenen Daten:**
    - **Technische Nutzungsdaten / Logdaten:** IP-Adressen, Datum und Uhrzeit des Abrufs, übertragene Datenmenge, Gerätetyp, Betriebssystemversion.
    - **Gerätekennungen:** Device-Tokens / Push-Tokens (zur Zustellung von Push-Mitteilungen).
    - **Nutzer- und Bestandsdaten des Portals:** Vor- und Nachname, E-Mail-Adresse, Rolle/Rechte, Login-Zeitstempel von Vereinsadministratoren.

- **Ggf. vom Verein eingepflegte Daten:** Namen von Ansprechpartnern, Trainer- oder Spielerlisten (sofern im Portal durch den Verein hinterlegt).

3. **Kategorien betroffener Personen:**
   - Endnutzer der Vereins-App (Vereinsmitglieder, Fans, Interessierte).
   - Administratoren, Redakteure und berechtigte Mitarbeiter/Funktionäre des Auftraggebers.

§ 3 Pflichten und Weisungsgebundenheit des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet. Der Hauptvertrag und diese Vereinbarung stellen die grundlegende Weisung dar.
2. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt.
3. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 4 Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DSGVO

1. Der Auftragnehmer trifft alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (siehe **Anlage 1** zu diesem Vertrag).
2. Die Sicherheitsmaßnahmen können im Zuge des technischen Fortschritts fortentwickelt werden. Wesentliche Änderungen, die das vereinbarte Schutzniveau verringern könnten, sind unzulässig.

§ 5 Einsatz von Unterauftragsverarbeitern (Subunternehmern)

1. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter (Subunternehmer) hinzuzuziehen. Die genehmigten Unterauftragnehmer sind in **Anlage 2** aufgeführt.
2. Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern in Textform (z. B. per E-Mail). Dem Auftraggeber steht das Recht zu, gegen solche Änderungen binnen 14 Tagen aus wichtigem datenschutzrechtlichem Grund Einspruch zu erheben.

3. Der Auftragnehmer stellt vertraglich sicher, dass den Subunternehmern dieselben Pflichten auferlegt werden, die in diesem Vertrag zwischen Auftraggeber und Auftragnehmer festgelegt sind.

§ 6 Rechte der betroffenen Personen

1. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit) nachzukommen.
2. Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter.

§ 7 Unterstützungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen:

1. bei der Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 DSGVO;
2. bei der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DSGVO) und der Benachrichtigung der betroffenen Person (Art. 34 DSGVO);
3. bei einer etwaigen Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und vorherigen Konsultation (Art. 36 DSGVO).

§ 8 Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat das Recht, die Einhaltung der Bestimmungen dieses Vertrages vor Ort oder durch von ihm beauftragte sachverständige Prüfer zu kontrollieren.
2. Der Nachweis kann primär durch Vorlage aktueller Zertifikate, Prüfberichte von anerkannten Dritten oder Selbstauskünften (z. B. der beteiligten Rechenzentren) erbracht werden. Eine Vor-Ort-Kontrolle ist mit angemessener Frist anzukündigen und soll den Betriebsablauf des Auftragnehmers nicht unverhältnismäßig stören.

§ 9 Löschung und Rückgabe von Daten

Nach Beendigung der Erbringung der Verarbeitungsleistungen ist der Auftragnehmer verpflichtet, alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Pflicht zur Aufbewahrung der Daten besteht.

§ 10 Schlussbestimmungen

1. Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, berührt dies die Gültigkeit der übrigen Bestimmungen nicht.

2. Es gilt deutsches Recht. Ausschließlicher Gerichtsstand ist der Geschäftssitz des Auftragnehmers, soweit gesetzlich zulässig.

Anlage 1: Technische und organisatorische Maßnahmen (TOM)

1. **Zutrittskontrolle:** Betrieb der Server in ISO 27001-zertifizierten deutschen Rechenzentren mit gesichertem Sicherheitsbereich, Videoüberwachung und biometrischer bzw. elektronischer Zugangskontrolle.
2. **Zugangskontrolle:** Zugriff auf Server und Datenbanken nur über geschützte SSH-Keys bzw. Multi-Faktor-Authentifizierung (2FA); restriktives Kennwort-Management.
3. **Zugriffskontrolle:** Differenzierte Rechteverwaltung im Administrationsportal (Rollen- und Rechtesystem); Zugriff auf Systemebene nach dem Minimal-Rechte-Prinzip (Need-to-know).
4. **Weitergabekontrolle / Übertragungssicherheit:** Verschlüsselte Übertragung aller Daten zwischen App, Portal und Server mittels aktueller Transportverschlüsselung (HTTPS / TLS 1.3).
5. **Eingabekontrolle:** Protokollierung von administrativen Anmeldevorgängen und sicherheitsrelevanten Änderungen im System.
6. **Verfügbarkeitskontrolle:** Tägliche automatische Datensicherungen (Backups); redundante Server-Infrastruktur; USV- und Notstromversorgung im Rechenzentrum.
7. **Trennungskontrolle:** Logische Mandantentrennung auf Datenbankebene; Entwicklungs- und Produktivumgebungen sind strikt getrennt.

Anlage 2: Genehmigte Unterauftragsverarbeiter (Subunternehmer)

Name / Unternehmen	**Sitz / Land**	**Gegenstand / Leistung**
Hetzner Online GmbH (bzw. IONOS / Netcup)	Deutschland / EU	Server-Hosting, Cloud-Infrastruktur & Datenbanken
Apple Inc. (Apple Push Notification service - APNs)	USA / Irland (EU-Standardvertragsklauseln / DPF)	Technischer Versand von Push-Nachrichten an iOS-Geräte

Name / Unternehmen	**Sitz / Land**	**Gegenstand / Leistung**
Google LLC (Firebase Cloud Messaging - FCM)	USA / Irland (EU-Standardvertragsklauseln / DPF)	Technischer Versand von Push-Nachrichten an Android-Geräte