Vereinbarung über eine Auftragsverarbeitung gemäß Art. 28 DSGVO

Der Verantwortliche:	Der Auftragsverarbeiter:
	Waldhart Software GmbH Unterdorf 1 6405 Pfaffenhofen
(im Folgenden Auftraggeber)	(im Folgenden Auftragnehmer)

1. Gegenstand der Vereinbarung

(1) Gegenstand

Der Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- WS SPORTS: ERP-Software inkl. Registrierkasse, Kundenverwaltung, Personalplanung, Zeiterfassung
- Online-Buchungssystem für Kunden
- WS SPORTS Mobil: Web-APP für Skilehrer zur Datenpflege
- Check-in: Web-APP für Kunden zur Adresseingabe

(2) Art und Zweck der Verarbeitung von Daten

Nähere Beschreibung des Auftrages in Hinblick auf Art und Zweck der vorgesehenen Verarbeitung durch den Auftragnehmer:

- Daten von Kunden, die Leistungen des Auftraggebers in Anspruch nehmen
- Daten von Mitarbeitern, die Leistungen zusammen mit dem Auftraggeber erbringen
- Daten von an der Geschäftsabwicklung mitwirkende wie Hotels, Reisebüros, Dienstleister
- Zugangsdaten zum IT-System des Auftraggebers

(2) Art der Daten

Folgende Datenkategorien werden verarbeitet:

- Daten zur Person: Name, Adressen, Geburtsdatum, Fahrkönnen, Sprache
- Buchhalterische Daten: Angebote, Rechnungen, Zahlungen
- Daten zur Leistung: Leistungsart, Preis, Leistungszeitraum

- Organisatorische Daten: Zuteilung von Kunden und Mitarbeitern
- Dokumentation der Arbeitsleistung von Mitarbeitern: Arbeitszeit, Art der Tätigkeit
- Zugang zu Servern und Clients: IP-Adresse, Fernwartungstool inkl. Benutzernamen und Kennwörtern

(3) Kategorien betroffener Personen

Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

- Kunden
- Mitarbeiter
- Unterkünfte, Reisebüros, Dienstleister, Lieferanten

2. Dauer der Vereinbarung

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von einem Monat zum 30. August gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(3) Wahrung der Vertraulichkeit und Verschwiegenheit: Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(4) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32ff DSGVO ergriffen hat. Konkret handelt es sich hierbei um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der

Systeme. Einzelheiten hierzu finden sich im Anhang (Technisch-organisatorische Maßnahmen).

(5) Mitwirkungspflicht bei Betroffenenrechten: Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Betroffenenrechte nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen.
Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(6) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer durchzuführen (sicherzustellen).

(7) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten. Dazu gehören Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation.

(8) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu erstellen hat.

(9) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(10) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, sämtliche in seinem Besitz gelangten Unterlagen, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber zu übergeben oder auf dessen Auftrag zu löschen. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.
Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

(11) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. Technisch-organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen (TOMs) unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

Einzelheiten sind dem Anhang zu entnehmen.

5. Ort der Durchführung der Datenverarbeitung

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

6. Sub-Auftragsverarbeiter

Der Auftragnehmer ist befugt folgende Unternehmen als Sub-Auftragsverarbeiter zur unmittelbaren Erbringung der Hauptdienstleistung hinzuziehen:

- Provider für Cloud und Internetdienste
    - Cibex Gmbh, Eduard Wallnöfer Platz 3/3, 6410 Telfs
    - myNet GmbH, Burgfeldstraße 5, 6500 Landeck
    - adino.at Internetservice GmbH, Achstrasse 18, 6971 Hard
    - Hetzner Online GmbH, Industriestr. 25, D-91710 Gunzenhausen
    - DigitalOcean, 101 Avenue of the Americas, 10th Floor, New York, NY 10013
- Payment Provider
    - Viveum Zahlungssysteme GmbH, Riemergasse 14/30, 1010 Wien
    - Ingenico Payment Services GmbH, Daniel-Goldbach-Str. 17-19, D-40880 Ratingen
    - TrekkSoft AG, Hauptstrasse 15, CH-3800 Matten bei Interlaken
    - SIX Payment Services GmbH, Marxergasse 1B, 1030 Wien
    - hobex AG, Josef-Brandstätter-Straße 2b, 5020 Salzburg

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer dies dem Auftraggeber eine angemessene Zeit vorab schriftlich anzeigt und
- der Auftraggeber nicht gegenüber dem Auftragnehmer schriftlich Einspruch gegen die geplante Auslagerung erhebt und
- die erforderlichen Vereinbarungen zwischen dem Auftragnehmer und dem Sub-Auftragsverarbeiter gemäß des Art. 28 Abs. 4 DSGVO abgeschlossen werden.
  Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

…….., am
Für den Auftraggeber:

.....

Pfaffenhofen, am 20.02.2019
Für den Auftragnehmer:

.....
Hannes Waldhart

Anhang – Technisch-organisatorische Maßnahmen (TOMs)

Vertraulichkeit

- Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch versperrbare Tür
- Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch Kennwörter
- Protokoll der Tätigkeiten
- Klassifikationsschema der Daten vertraulich, intern, öffentlich

Integrität

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung per HTTS und SSL-Zertifikaten, Virtual Private Networks (VPN)
- Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch Protokollierung

Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch stündliche Backups auf der Festplatte des Datenbankservers
  Für zusätzliche Backups trägt der Auftraggeber selber Sorge
- Rasche Wiederherstellbarkeit durch Restore eines Datenbankbackups
- Löschungsfristen legt der Auftraggeber fest

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Incident-Response-Management durch Erreichbarkeit per Telefon oder E-Mail
- Datenschutzfreundliche Voreinstellungen
- Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers
- 4-Augen-Prinzip: Auftraggeber kontrolliert die Richtigkeit der Daten, die vom Auftragnehmer im System eingegeben wurden