Vertrag über die Auftragsverarbeitung von persönlichen Daten: Controller-Prozessor Vereinbarung

Version: 1.0

zwischen

X-Fitness GmbH
Hauptstraße 60-64
82467 Garmisch-Partenkirchen
Deutschland

Im Folgenden benannt als **Controller**

und

SuperSaaS B.V.
Keizersgracht 639
1077 KR Amsterdam
Niederlande

Im Folgenden benannt als **Prozessor**

1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Controller und Prozessor (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag von dem Controller.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Prozessors oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Controllers verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2 2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Prozessor übernimmt folgende Verarbeitungen:

Stellt einen internetbasierten Service, um es den Endbenutzern des Controllers zu erlauben online Termine machen zu können.
Stellt einen internetbasierten Service, der dem Controller die Verwaltung dieser Termine und der gesammelten Daten der Endbenutzer erlaubt.

2.2 Dauer

Die Verarbeitung beginnt am 20.04.2016 und soll für eine unbestimmte Zeit weitergeführt werden, solange bis das SuperSaaS Konto vom Controller gelöscht wurde.

3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung

3.1 Art und Zweck der Verarbeitung

Datenverarbeitung besteht aus dem Folgenden: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten

Die Verarbeitung dient folgendem Zweck: Endbenutzern des Controller können damit Onlinetermine planen

3.2 Art der Daten

Es werden folgende Daten verarbeitet:

- Daten, die von den Endbenutzern eingegeben werden im Prozess der Servicenutzung

3.3 Kategorien der betroffenen Personen

Die folgenden Datensubjekte sind von der Datenverarbeitung betroffen:

- Endbenutzer der online Termin-Anwendung des Controller

4 Pflichten des Prozessors

(1) Der Prozessor verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Controller angewiesen, es sei denn, der Prozessor ist gesetzlich zu einer bestimmten Datenverarbeitung verpflichtet. Sofern solche Verpflichtungen für den Prozessor bestehen, teilt der Prozessor diese dem Controller vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Prozessor verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Prozessor bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Prozessor verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Der Prozessor sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Prozessor trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(6) Im Zusammenhang mit der beauftragten Verarbeitung hat der Prozessor den Controller bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Controller auf Anforderung unverzüglich zuzuleiten.

(7) Wird der Controller durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Prozessor den Controller im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung des Controllers im Auftrag betroffen ist.

(8) Auskünfte an Dritte oder den Betroffenen darf der Prozessor nur nach vorheriger Zustimmung durch den Controller erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Controller weiterleiten.

(9) Soweit gesetzlich verpflichtet, bestellt der Prozessor eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Controller direkt an den Datenschutzbeauftragten wenden. Der Prozessor teilt dem Controller unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet,

weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Prozessor dem Controller unverzüglich mit.

(10) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Controllers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

5 Technische und organisatorische Maßnahmen

(1) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden solange das geschuldete Minimum erfüllt ist. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Prozessor unverzüglich umzusetzen. Änderungen sind dem Controller unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(2) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Controllers nicht oder nicht mehr genügen, benachrichtigt der Prozessor den Controller unverzüglich.

(3) Kopien oder Duplikate werden ohne Wissen des Controllers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(4) Sollte die Verarbeitung in einer Privatwohnung erfolgen, ist vom Prozessor sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Controllers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können.

(5) Dedizierte Datenträger, die vom Controller stammen bzw. für den Controller genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags für den Controller verarbeitete Daten wird der Prozessor nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Controller's berichtigen, löschen oder sperren.

(2) Den entsprechenden Weisungen des Controller wird der Prozessor jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7 Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Controllers im Einzelfall zugelassen.

(2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Controller erhält auf Verlangen Einsicht in die relevanten Verträge zwischen

Prozessor und Subunternehmer.

(3) Die Rechte des Controllers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Prozessor berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

(4) Die Verantwortlichkeiten des Prozessors und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(5) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.

(6) Der Prozessor wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

(7) Jede Weiterleitung von im Auftrag des Controller verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Prozessor dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat.

(8) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag des Controller nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel 4 (10) und (11) dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Prozessor teilt dem Controller mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.

(9) Der Prozessor hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Controller unaufgefordert vorzulegen.

(10) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Prozessors, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8 Rechte und Pflichten des Controller

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Controller verantwortlich.

(2) Der Controller erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Controller unverzüglich dokumentiert bestätigen.

(3) Der Controller informiert den Prozessor unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Controller ist berechtigt eine dritte Partei als unabhängigen Prüfer zu ernennen, der über die benötigten professionellen Fähigkeiten verfügt und durch eine Schweigepflicht zur Vertraulichkeit gebunden ist, die Wahl des Prüfers muss dabei für den Prozessor akzeptabel sein, zur Überprüfung der Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Prozessor zu kontrollieren. Die Inanspruchnahme des Rechts zu dieser Prüfung wird mindestens 4 Wochen vorher beim Prozessor mit einer schriftlichen Mitteilung angekündigt. Der Controller trägt dabei alle entstehenden Kosten dieser Prüfung.

(5) Kontrollen beim Prozessor haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Controller zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Prozessors, sowie nicht häufiger als alle 12 Monate statt. Soweit der Prozessor den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9 Mitteilungspflichten

(1) Der Prozessor teilt dem Controller Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Prozessors vom relevanten Ereignis an eine vom Controller benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d. eine Beschreibung der vom Prozessor ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(3) Ebenfalls sind dem Controller unverzüglich erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Prozessors oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen mitzuteilen.

(4) Der Prozessor informiert den Controller unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(5) Der Prozessor sichert zu, den Controller bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10 Weisungen

(1) Der Controller behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

(2) Der Prozessor wird den Controller unverzüglich darauf aufmerksam machen, wenn eine vom Controller erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Prozessor ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Controller bestätigt oder geändert wird.

(3) Der Prozessor hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11 Beendigung des Auftrags

(1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Controllers hat der Prozessor die im Auftrag verarbeiteten Daten nach Wahl des Controllers entweder zu vernichten oder an den Controller zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

(2) Der Prozessor ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

(3) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Prozessor den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Der Prozessor kann die entsprechende Dokumentation zu seiner Entlastung dem Controller bei Vertragsende übergeben.

12 Vergütung

Die Vergütung des Prozessors ist abschließend in den Nutzungsbedingungen geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

13 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haftet der Controller als Gesamtschuldner.

(2) Der Controller trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der the Prozessor den Controller auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Controller erhoben werden.

(3) Der Prozessor haftet dem Controller für Schäden, die der Prozessor, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

(4) Die Haftung des Prozessors gegenüber dem Controller ist begrenzt auf die Höhe der Zahlungen des Controllers an den Prozessor der zwei vorhergehenden Jahre vor dem Ereignis, das die Haftung verursacht.

(5) Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Controller erteilten Weisung entstanden ist.

14 Sonderkündigungsrecht

(1) Der Controller kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Prozessors gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Prozessor eine rechtmäßige Weisung des Controllers nicht ausführen kann oder will oder der Prozessor Kontrollrechte des Controllers vertragswidrig verweigert.

(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Prozessor die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

(3) Bei unerheblichen Verstößen setzt der Controller dem Prozessor eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Controller zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

15 Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Sollte Eigentum des Controllers beim Prozessor durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Prozessor den Controller unverzüglich zu verständigen.

(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(4) Sollten einzelne Teile dieser Vereinbarung inhaltlich von der englischsprachigen Version abweichen, so gilt diese.