Vertrag zur Auftragsverarbeitung gem. Art.28 Abs. 3 DSGVO

A. AUFTRAGGEBER

Adresse

B. AUFTRAGNEHMER

Firma	ParentPay Deutschland GmbH
Adresse	Stuttgarter Straße 41 75179 Pforzheim Deutschland

C. VEREINBARUNG

1. Gegenstand der Beauftragung

a. Hosting der dem Auftragnehmer vom Auftraggeber zur Verfügung gestellten Daten auf einem Web-Server.
b. Zurverfügungstellung der Software MensaMax auf einem Web- Server für die Bearbeitung der Daten.
c. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrags.

2. Dauer der Beauftragung

a. Die Beauftragungsdauer ist an den Bestand des gegenseitig geschlossenen Nutzungs- oder Dienstleistungsvertrages gebunden.
b. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt.

3. Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung der Daten, Ort der Verarbeitung

a. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten ergeben sich aus dem zwischen den Vertragsparteien bestehenden Vertrag.
b. Der Auftragnehmer ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden.
c. Dem Auftragnehmer ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemäßen Erhebung, Verarbeitung und / oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt. Dem Auftragnehmer ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.
d. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt. Eine Verlagerung in ein Drittland findet nicht statt.

4. Art der verarbeiteten personenbezogenen Daten

a. Es werden die für den Betriebsablauf erforderlichen Daten verarbeitet. Hierzu können unter anderem, aber nicht ausschließlich gehören: Daten über Personen und deren Essensbestellungen, Kioskkäufe, weitere Buchungen, Ein- und Auszahlungen, Ausleihdaten, Zeiterfassungsdaten, Bankdaten. Die genauen Daten werden in einer Anlage beschrieben.
b. Im Fall der Nutzung biometrischer Legitimationsverfahren werden aus den „besonderen Kategorien personenbezogener Daten“ biometrische Daten erhoben und verarbeitet.

5. Kreis der Betroffenen

a. Nutzer der Software MensaMax. Dies beinhaltet unter anderem, aber nicht ausschließlich, Essensteilnehmer, Kursteilnehmer, Verwaltungspersonal. Die genauen Daten werden in einer Anlage beschrieben.

6. Gegenstand der Vereinbarung

a. Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers ausschließlich in dessen Auftrag nach Weisung; eine Funktionsübertragung auf den Auftragnehmer wird ausdrücklich ausgeschlossen.

7. Pflichten des Auftraggebers

a. Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Personen ist allein der Auftraggeber verantwortlich.
b. Der Auftraggeber erteilt dem Auftragnehmer Weisungen über Art und Umfang der Datenverarbeitung.
c. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
d. Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
e. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt und umgekehrt.
f. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

8. Pflichten des Auftragnehmers

a. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nur auf dokumentierter Weisung des Auftraggebers, auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Er verwendet die zur Datenverarbeitung überlassenen Daten nur für Zwecke der Auftragsverarbeitung.
b. Der Auftragnehmer hat personenbezogene Daten zu berichtigen, zu löschen oder zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt und dies nicht durch den Auftraggeber selbst gemacht werden kann.
c. Wenn eine betroffene Person sich bezüglich Berichtigung, Löschung oder Sperrung unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
   Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12-22 DSGVO hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen.
d. Der Auftragnehmer verarbeitet die überlassenen Daten ausschließlich in der Weise, dass diese jederzeit von sonstigen Datenbeständen getrennt bereitgestellt werden können.
e. Der Auftragnehmer ermöglicht dem Auftraggeber die Kontrolle der Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen. Dies geschieht insbesondere durch die Erteilung von Auskünften und die Einsichtnahme in die gespeicherten Daten, die Datenverarbeitungsprogramme sowie die Verarbeitungsprotokolle oder durch Inspektionen (sog. Vor-Ort-Kontrollen).
   Der Auftragnehmer erteilt auf Anforderung die erforderlichen Auskünfte weist die Umsetzung der technischen und organisatorischen Maßnahmen nach.
f. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

g. Für die Durchführung der Auftragsverarbeitung nicht mehr benötigte Unterlagen und Datenbestände werden nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet. Test- und Ausschussmaterial ist unverzüglich datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
h. 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.
i. Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter oder Subunternehmer mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und zur Verschwiegenheit für die Zeit ihrer Tätigkeit wie auch nach Beendigung der Tätigkeit verpflichtet.
j. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.
k. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers zur Einhaltung der datenschutzrechtlichen Anforderungen nach der DSGVO. Dieses besteht auch nach Beendigung des Vertrages fort. Er verpflichtet sich, spezialgesetzliche Datenschutzbestimmungen, die für den Auftraggeber gelten, auch gegen sich gelten zu lassen, sofern ihm diese durch den Auftraggeber bekanntgemacht werden.
l. Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

9. Unterauftragsverhältnisse mit Subunternehmern

a. Der Auftragnehmer bedient sich für das Hosting der Daten eines Rechenzentrums. Zum Zeitpunkt des Vertragsabschlusses ist dies:
   - Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, www.hetzner.de

   Der Auftraggeber stimmt hiermit der Hinzuziehung und Inanspruchnahme des Subunternehmers zu.
b. Die Hinzuziehung weiterer oder die Ersetzung bestehender Subunternehmer zur Verarbeitung von personenbezogenen Daten des Auftraggebers sind gem. Art. 28 Abs. 2 S. 1 Alt. 2 DSGVO zulässig, soweit der Auftragnehmer eine solche Änderung dem Auftraggeber mit einer Vorlauffrist von 4 Wochen schriftlich oder in Textform anzeigt und der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten an den neuen Subunternehmer schriftlich oder in Textform gegenüber dem Auftragnehmer Einspruch aus wichtigem Grund gegen die geplante Änderung erhebt (Art. 28 Abs. 2 S. 2 DSGVO). Der Einspruch ist zu begründen. Unterbleibt der Einspruch, gelten die neuen Subunternehmer als genehmigt.
c. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber Subunternehmen gelten. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

10. Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

a. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitung derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.
b. Das im Anhang beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen, passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik, der eingesetzten IT-Systeme und der Verarbeitungsprozesse dar.
c. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

d. Der Auftragnehmer informiert den Auftraggeber unverzüglich über geplante Veränderungen in der Organisation der Datenverarbeitung und den angewandten Verfahren, soweit sie für die Auftragsverarbeitung sicherheitsrelevant sind.
e. Der Auftragnehmer verarbeitet die Daten regelmäßig nur in den eigenen Büroräumen. Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) erfolgt nur im Rahmen eines Notfalles im Rahmen der Notfall-Hotline (365/24). Der Auftragnehmer stellt sicher, dass die datenschutzrechtlichen Rahmenbedingungen auch bei Einsatz von Telearbeitsplätzen oder mobilem Zugriff seiner Mitarbeiter auf Datenverarbeitungssysteme oder Daten des Auftragnehmers beachtet werden.
f. Der Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:
   - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
   - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
   - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
   - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

11. Zusammenarbeit

a. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
b. Der Auftragnehmer informiert den Auftraggeber über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.
c. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer zu unterstützen. Für die Unterstützung kann der Auftragnehmer einen Vergütungsanspruch geltend machen.
d. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32-36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und zu vorherigen Konsultationen. Hierzu gehören u.a.:
   - die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
   - die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
   - die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
   - die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
   - die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
e. Für Unterstützungsleistungen, die nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

12. Verpflichtungen nach Beendigung des Vertrags

a. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
b. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

c. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der verarbeiteten Daten ausgeschlossen.
d. Sollten Sicherheit oder Verfügbarkeit der Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse möglicherweise gefährdet sein, so hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten und dem Auftraggeber aller erforderlichen Auskünfte zur Sicherung der Daten selbst sowie ihre Verfügbarkeit zu erteilen.

13. Haftung

a. Auf Art. 82 DSGVO wird verwiesen.

14. Datenschutzbeauftragte, Weisungsberechtigte und Weisungsempfänger

a. Ansprechpartner für die datenschutzrechtlichen Belange sind die bei Auftraggeber und Auftragnehmer jeweiligen Datenschutzbeauftragten, deren Kontaktdaten auf der Homepage des Auftraggebers und Auftragnehmers leicht zugänglich hinterlegt oder anderweitig der jeweiligen Gegenseite bekannt gemacht sind.
b. Ansprechpartner (Weisungsberechtigte) sind beim Auftraggeber die in einem extra Dokument (Anlage zum Hauptvertrag) benannten Ansprechpartner für MensaMax.
c. Ansprechpartner (Weisungsempfänger) für die auftragsspezifischen, aber nicht datenschutzrechtlichen Belange sind beim Auftragnehmer die Mitarbeiter der Support-Abteilung. Kontaktdaten hierzu sind auf der Homepage des Auftragnehmers ersichtlich.

15. Sonstiges

a. Die Vertragspartner stellen sicher, dass die Übergabeformate der zu verarbeitenden Daten in den Einzelvereinbarungen verlässlich geregelt werden.
b. Die Vertragspartner definieren klare Schnittstellen und Verantwortlichkeiten.
c. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
d. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
e. Soweit der Auftraggeber den Regelungen des Datenschutzgesetzes der Evangelischen Kirche in Deutschland (DSG-EKD) unterliegt, wird in Ergänzung zu den oben genannten Regelungen auf der Grundlage der DSGVO festgehalten, dass für die Vertragsparteien auch die Bestimmung des DSG-EKD gelten.
f. Dies erstreckt sich insbesondere auf die Paragraphen §30 (Verarbeitung personenbezogener Daten im Auftrag), §31 (Verzeichnis von Verarbeitungstätigkeiten) und §§43+44 (Befugnisse und Aufgaben der Datenschutzaufsicht).
g. Soweit der Auftraggeber den Regelungen des Datenschutzgesetzes des kirchlichen Datenschutzgesetzes (KDG) unterliegt, wird in Ergänzung zu den oben genannten Regelungen auf der Grundlage der DSGVO festgehalten, dass für die Vertragsparteien auch die Bestimmung des KDG gelten.
Dies erstreckt sich insbesondere auf die Paragraphen §29 (Verarbeitung personenbezogener Daten im Auftrag), §31 (Verzeichnis von Verarbeitungstätigkeiten) und §44 (Aufgaben der Datenschutzaufsicht).

D. UNTERSCHRIFTEN

Hiermit akzeptieren wir die vorstehende Vereinbarung.

Ort

Datum

Unterschrift Auftraggeber

Name Unterzeichner(in)

Ort

Datum

Unterschrift Auftraggeber

Name Unterzeichner(in)

Pforzheim
Ort

Datum

Unterschrift Auftragnehmer

Marco Schulten, Geschäftsführer
Name Unterzeichner

Anlage A

BITTE BEACHTEN SIE: DIESE ANLAGE IST DURCH DEN AUFTRAGGEBER AUSZUFÜLLEN!

A. AUFTRAGGEBER

Adresse

Art der verarbeiteten personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO)

Es werden die für den Betriebsablauf erforderlichen Daten verarbeitet. Gegenstand der Verarbeitung sind folgende Arten personenbezogener Daten:

Allgemeine Kategorien personenbezogener Daten:

☐ Personenstammdaten (z. B. Vorname, Nachname, Geburtsdatum)

☐ Kommunikationsdaten (z. B. Anschrift, Telefon, E-Mail)

☐ Vertragsstammdaten (z. B. Debitorennummer, Kundennummer)

☐ Vertragsabrechnungs- und Zahlungsdaten (z. B. Bankverbindung, Einzahlungen, Lastschriften)

☐ Kundenhistorie (z.B. Essensbestellungen, Kioskkäufe)

☐ Absprachen (z.B. Gesprächsnotizen, Merkmale)

☐ _____

☐ _____

☐ _____

☐ _____

☐ _____

Besondere Kategorien personenbezogener Daten:

☐ Genetische Daten und Gesundheitsdaten (Unverträglichkeiten, Allergien)

☐ Biometrische Daten (Fingerprint))

☐ _____

☐ _____

☐ _____

Kategorien betroffener Personen
(entsprechend der Definition von Art. 4 Nr. 1 DSGVO)

Die Kategorien der durch den Umgang mit den personenbezogenen Daten des Auftraggebers im Rahmen dieses Vertrags betroffenen Personen umfasst:

☐ Essensteilnehmer

☐ Am Kiosk/Bistro/Pausenverkauf teilnehmende Personen

☐ Personen, die an einem weiteren Angebot (z.B. Betreuung, AG, Kurs, Projekt) teilnehmen

☐ Personen, die Medien ausleihen

☐ Mitarbeiter des Caterers

☐ Mitarbeiter, die mit der MensaMax-Verwaltung bzw. Administration beauftragt sind

☐ _____

☐ _____

☐ _____

☐ _____

☐ _____

<