Erläuterungen zu den technischen und organisatorischen Maßnahmen (nach Art. 32 DSGVO)

Zutrittskontrolle Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern.	MensaMax ist eine webbasierte Anwendung – darauf kann jedermann mit jedem webfähigen Clientgerät zugreifen, sofern er berechtigt ist. Die Server selbst sind Root-Server und stehen in einem Rechenzentrum. Derzeit nutzen wir als Subunternehmer: ☐ Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, www.hetzner.de Das Rechenzentrum gewährleistet die Durchführung der räumlichen Zutrittskontrolle: ☐ Per Video überwachter Hochsicherheitszaun um den gesamten Datacenterpark ☐ Zufahrt nur über Zutrittskontrollterminals mit Transponder bzw. Zutrittskarten ☐ Hochmoderne Überwachungskameras zur 24/7-Überwachung von Zufahrten, Eingängen, Sicherheitsschleusen und Serverräumen
Zugangskontrolle Eine unbefugte Systemnutzung ist zu verhindern.	Um sich in MensaMax einloggen zu können, sind 3 Faktoren notwendig: Projektname, Benutzername und Kennwort. Insbesondere der Benutzername und das Kennwort kann nicht aus einem Regelwerk hergeleitet werden. Das Kennwort unterliegt dabei besonderen Anforderungen durch Verwendung von Groß- und Kleinbuchstaben, Zahlen bzw. Sonderzeichen und einer Kennwortlänge von mind. 8 Zeichen. Die Kennwörter sind in der Anwendung hashverschlüsselt.
Zugriffskontrolle Benutzerkontrolle Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich sein.	MensaMax hat eine frei einstellbare Rechteverwaltung. Die Vergabe der jeweiligen Rechte obliegt allein dem Auftraggeber oder einer von Ihr autorisierten Person. Durch die Vergabe entsprechender Nutzerrechte wird ein Nutzer befugt, Daten zu lesen, zu schreiben oder zu löschen. Die Rechte können sowohl sachlich (was darf jemand tun) als auch räumlich (also mandantenübergreifend) eingeschränkt bzw. erweitert werden. Alle Anmeldeversuche in MensaMax werden geloggt. Die Protokolle werden zwölf Monate aufbewahrt. Die Server, auf denen MensaMax läuft und auf denen die Daten gespeichert sind, werden nur durch autorisierte Personen über Remotezugang administriert. Die hierfür notwendigen Benutzerkennungen und Kennwörter sind personengebunden und dürfen nicht weitergegeben werden. Das unbefugte Eindringen aus dem öffentlichen Netz wird durch Firewall inkl. AV, IPSec, DoS Konfiguration etc. verhindert.
Trennungskontrolle Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.	Auf den verwendeten Servern werden ausschließlich Daten zum gleichen Zweck (MensaMax) gespeichert. Es kommt zu keinerlei Verbunddatenspeicherung dieser personenbezogenen Daten und es kommt zu keinerlei anderweitiger Verarbeitung dieser Daten.

ParentPay Deutschland GmbH | Stuttgarter Straße 41 | 75179 Pforzheim
Geschäftsführer: Marco Schulten, Andrew Neubauer | Handelsregister: Amtsgericht Pinneberg HRB 11833 PI USt-IdNr. DE 299832368

Übertragungskontrolle Transportkontrolle Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.	Der Zugriff auf MensaMax erfolgt SSL-verschlüsselt. Daten, die aus MensaMax abgerufen werden, werden daher zum Zielrechner verschlüsselt übermittelt. Ab dann endet naturgemäß die Kontrollmöglichkeit der Software. Es werden aktuelle Versionen aller involvierten Systeme verwendet, um die Effektivität der verwendeten Verschlüsselungen zu gewährleisten. Alle unsere Mitarbeiter sind zur Geheimhaltung verpflichtet und somit nicht berechtigt, Daten jeder Art des Unternehmens, des Kunden oder involvierter Personen weiterzugeben.
Eingabekontrolle Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.	MensaMax hält fest, wer und wann einen Datensatz angelegt hat, und wer und wann diesen Datensatz zuletzt geändert hat. Die Durchführung derartiger Aktionen ist ausschließlich mit gültiger Benutzerkennung möglich.
Speicherkontrolle Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.	MensaMax ist durch Benutzername und Kennwort gesichert. Somit hat nur derjenige Zugang, der einen Benutzernamen und das zugehörige Passwort kennt. Das Kennwort ist hashverschlüsselt. Durch die Vergabe entsprechender Nutzerrechte wird ein Nutzer befugt, Daten zu lesen, zu schreiben oder zu löschen. Die Rechte können sowohl sachlich (was darf jemand tun) als auch räumlich (also mandantenübergreifend) eingeschränkt bzw. erweitert werden.
Datenträgerkontrolle Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.	Sollte seitens des Auftragnehmers ein Root-Server aus dem Serververbund bei dem hostenden Rechenzentrum gekündigt werden, wird zugesichert, dass die darin verwendeten Festplatten dergestalt vollständig gelöscht werden, dass unbefugte Dritte nicht an die Daten herankommen können. Sollte eine Festplatte defekt sein, wird diese geschreddert.
Auftragskontrolle Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	Nur ein beschränkter Personenkreis hat Zugriff auf die Daten. Dies sind die Personen, die Support leisten oder die die Serverwartung betreiben. Diese sind entsprechend unterwiesen und werden laufend geschult, so dass ein Verlust der Daten, die unbefugte Kenntnisnahme durch Dritte oder die unsachgemäße Verarbeitung vermieden werden soll. Personenbezogene Daten werden von unserem Unternehmen, mit Ausnahme des Serverstandortes, nicht an Fremdfirmen zur Datenverarbeitung im Auftrag weitergegeben. Für den Fall, dass derartige Aufträge in Zukunft notwendig werden, wird auf ein höchstes Maß an Sicherheit und Transparenz Wert gelegt, die betroffenen Auftraggeber zuvor in Kenntnis gesetzt sowie deren Zustimmung eingeholt.
Verfügbarkeitskontrolle Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.	Alle personenbezogenen Daten und Dokumente werden in einer zentralen Datenbank gespeichert, die wiederum in einem RAID-Verbund gespeichert sind. Auf den verwendeten Servern laufen Überwachungsprogramme, die im Falle einer Störung des Serverbetriebs umgehend aktiv Meldungen an verantwortliche Personen des Auftragnehmers versenden.

	Das Rechenzentrum seinerseits stellt weitgehende Ausfallsicherheit durch entsprechende Schutzprogramme, aktiven DDoS-Schutz sowie eine unterbrechungsfreie Stromversorgung sicher. Es erfolgt eine tägliche Datensicherung mit Rückverfolgung auf die letzten 7 Tagessicherungen, die letzten 4 Wochensicherungen, die letzten 12 Monatssicherungen, die letzten 2 Jahressicherungen.
Wiederherstellbarkeit Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.	Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen. Im Falle des Verlustes oder der Beschädigung von personenbezogenen Daten können diese von einem früheren Sicherungszeitpunkt der Datensicherungen wiederhergestellt werden.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM zur Gewährleistung der Sicherheit der Verarbeitung

Der Auftragnehmer unternimmt nachfolgend beschriebene Maßnahmen, um die Wirksamkeit der TOM zu gewährleisten:

☐ Die MensaMax-Software wird regelmäßig weiterentwickelt. Für die Entwicklung werden automatisierte Tests hinsichtlich der Datenqualität und –konsistenz verwendet. Eine Freigabe der neuen Versionen erfolgt außerdem durch eine eingerichtete Abteilung der Qualitätssicherung. Das Verfahren und die Testergebnisse sind protokolliert.

☐ Die Protokolle auf den MensaMax-Servern werden regelmäßig und automatisiert überwacht. Das betrifft insbesondere die Firewall-Protokolle und Login-Protokolle.

☐ Die Aktualität des Betriebssystems und der weiteren auf den Servern installierten Software wird regelmäßig überprüft sowie Updates und Patches eingespielt. Die Tätigkeiten werden dokumentiert.

☐ Die verwendeten Verschlüsselungsverfahren werden regelmäßig überprüft. Die Tätigkeit wird dokumentiert.

☐ Die durchgeführten Backups werden stichprobenartig überprüft. Die Tätigkeit wird dokumentiert.

☐ Alle Weisungen des Auftraggebers werden i.d.R. schriftlich eingefordert. Wo dies den Umständen nach nicht möglich oder sinnvoll ist, werden diese vom Auftragnehmer schriftlich protokolliert (z.B. Ticketsystem, E-Mail) und dem Auftraggeber zugesandt. Das Verfahren wird regelmäßig auf Einhaltung überprüft.

☐ Es bestehen klare Anweisungen an Mitarbeiter zur Einhaltung des Datenschutzes. Die Unterweisung wird regelmäßig wiederholt und protokolliert.