Selbstverpflichtungserklärung
(Erklärung zur einseitigen Verpflichtung)

durch

Psido Software GmbH, Auf der Heide 16, A-4225 Luftenberg

als Auftragsverarbeiter (in der Folge „Auftragnehmer") einerseits

gegenüber der

_____

_____

als Verantwortlicher (in der Folge „Auftraggeber") andererseits

Präambel

Gemäß den Bestimmungen des Art. 28 DSGVO haben Auftragsverarbeiter und Verantwortlicher durch einen Vertrag (oder ein anderes Rechtsinstrument gem. Art. 28 Abs. 3 DSGVO) die datenschutzkonforme Verarbeitung personenbezogener Daten sicherzustellen.

Der Auftragsverarbeiter gibt durch diese Selbstverpflichtungserklärung gegenüber seinem Vertragspartner, dem Auftraggeber, die einseitig verpflichtende Erklärung ab, im Rahmen der Datenverarbeitung die nachstehenden Pflichten einzuhalten. Den Verantwortlichen treffen durch diese einseitige Erklärung keinerlei Pflichten.

I. Gegenstand der Verpflichtungserklärung

(1) Der Auftragnehmer erbringt auf Grundlage eines Hauptvertrags für den Auftraggeber Leistungen im Bereich der Zurverfügungstellung einer Software-as-a-Service-Solution „PSIDO" (in der Folge „Hauptvertrag"). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten, hinsichtlich derer er sich verpflichtet, diese ausschließlich im Auftrag und nach Weisung des Auftraggebers zu verarbeiten. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich, soweit vorstehend nicht näher ausgeführt, aus dem Hauptvertrag, die Prüfung der Zulässigkeit der Datenverarbeitung obliegt ausschließlich dem Auftraggeber.

(2) Die Pflichten aus dieser Verpflichtungserklärung betreffen alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei in deren Zuge der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte

mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

II. Kategorien der verarbeiteten Daten und der betroffenen Personen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die nachstehend angeführten Kategorien personenbezogener Daten:

Stammdaten, Gesundheitsdaten, buchhaltungsrelevante Informationen

(2) Die Kategorien der von der Datenverarbeitung betroffenen Personen sind:

PatientInnen, Vertragspartner

III. Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer verpflichtet sich, Daten ausschließlich im Rahmen des Hauptvertrags und gemäß den ausdrücklichen Weisungen des Auftraggebers zu erheben, zu verarbeiten oder zu nutzen; dies betrifft auch die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Sofern der Auftragnehmer durch das Recht der Europäischen Union oder eines Mitgliedstaates, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet ist, verpflichtet er sich, dies dem Auftraggeber vor der Verarbeitung mitzuteilen.

(2) Der Auftragnehmer verpflichtet sich, vom Auftraggeber in schriftlicher Form zulässig erteilte Weisungen zu erfüllen, wobei dies auch Weisungen zu Berichtigung, Löschung und Sperrung von Daten umfasst. Erteilte Weisungen sind vom Auftragnehmer schriftlich zu dokumentieren.

(3) Sofern der Auftragnehmer zur Ansicht gelangt, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen und wird in diesem Fall die Durchführung dieser Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer wird die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

IV. Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer erklärt, dem Auftraggeber jederzeit das Recht einzuräumen, vor Aufnahme der Datenverarbeitung und in weiterer Folge regelmäßig die technischen und organisatorischen Maßnahmen des Auftragnehmers auf Kosten des Auftraggebers zu prüfen. In diesem Rahmen kann der Auftraggeber die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftragnehmer verpflichtet sich, Fehler oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt und über die er den Auftragnehmer informiert, in angemessener Frist zu beseitigen.

V. Datenschutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder diese dem Zugriff Dritter auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer verpflichtet sich, in seinem Verantwortungsbereich die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 EU-DSGVO, zumindest jedoch die in Anlage **./1** aufgeführten Maßnahmen der Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle und Verfügbarkeitskontrolle.

Der Auftragnehmer behält sich vor, die ergriffenen Maßnahmen zu ändern, sofern er sicherstellt, dass er das dem Auftraggeber zugesicherte Schutzniveau nicht unterschritten wird. Bei wesentlichen Änderungen verpflichtet sich der Auftragnehmer, den Auftraggeber zu informieren.

(3) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer verpflichtet sich daher, allen Personen, die von ihm mit der Bearbeitung und der Erfüllung des Hauptvertrags betraut werden (im folgenden Mitarbeiter genannt), entsprechend gem. Art. 28 Abs. 3 lit. b EU-DSGVO zur Vertraulichkeit zu verpflichten und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

Der Auftragnehmer verpflichtet sich sicherzustellen, dass diese Verpflichtungen auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Der Auftragnehmer verpflichtet sich, dem Auftraggeber die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

VI. Informationspflichten des Auftragnehmers

(1) Bei Prüfung des Auftragnehmers durch die Datenschutzbehörde, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte verpflichtet sich der Auftragnehmer den Auftraggeber umgehend schriftlich zu informieren und zumindest folgendes mitzuteilen:

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

b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer verpflichtet sich, unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen zu ergreifen sowie den Auftraggeber darüber zu informieren und um dessen weitere Weisungen zu ersuchen.

(3) Der Auftragnehmer verpflichtet sich zudem, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Anfrage nach VIII (1) betroffen sind.

(4) Sollten die Daten des Auftraggebers beim Auftragnehmer durch wie auch immer geartete Ereignisse oder Maßnahmen Dritter gefährdet werden, so verpflichtet sich der Auftragnehmer, den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der EU-DSGVO liegen.

(5) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 EU-DSGVO enthält. Das Verzeichnis wird dem Auftraggeber auf Anforderung zur Verfügung gestellt.

(6) Der Auftragnehmer verpflichtet sich, an der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber in angemessenem Umfang mitzuwirken und dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise auf dessen Kosten mitzuteilen.

VII. Einsatz von Subunternehmern

(1) Der Auftragnehmer verpflichtet sich, vertraglich vereinbarte Leistungen ganz oder teilweise nur unter Einbindung von solchen Subunternehmern durchzuführen, die er

sorgfältig nach deren Eignung und Zuverlässigkeit ausgewählt und diese entsprechend den Regelungen dieser Vereinbarung verpflichtet hat. Der Auftragnehmer verpflichtet sich darüber hinaus sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann und wird den Auftraggeber unverzüglich vor einer solchen Beauftragung in Kenntnis setzen und den beabsichtigten Subunternehmer nennen, um dem Auftraggeber die Möglichkeit zu geben, dem Einsatz eines Subunternehmers zu widersprechen. Die Liste der Subunternehmer ist auf https://www.psido.at/subs ersichtlich.

(2) Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, verpflichtet sich der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist, und dies dem Auftraggeber bei erster Aufforderung nachzuweisen.

(3) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen Subunternehmerverhältnisse im Sinne dieser Bestimmungen dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

VIII. Anfragen und Rechte Betroffener

(1) Der Auftragnehmer verpflichtet sich den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 EU-DSGVO zu unterstützen.

(2) Sofern ein Betroffener Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, etwa das Recht auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

IX. Beendigung des Hauptvertrags

(1) Diese Selbstverpflichtungserklärung gilt bis auf (jederzeit möglichen) Widerruf als solange abgegeben, als ein aufrechter Hauptvertrag zwischen den Parteien besteht. Mit Beendigung des Hauptvertrags gilt diese Selbstverpflichtungserklärung als widerrufen, sofern nicht nachstehend anderes erklärt wird.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger ausfolgen oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder nationalem Recht eine Verpflichtung zur

Speicherung der personenbezogenen Daten besteht – zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer verpflichtet sich, den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(3) Dem Auftraggeber wird auf Anfrage jederzeit das Recht eingeräumt, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(4) Der Auftragnehmer verpflichtet sich, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Selbstverpflichtungserklärung bleibt über das Ende des Hauptvertrags hinaus solange aufrecht, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

X. Sonstiges

(1) Zuständige Aufsichtsbehörde ist die Österreichische Datenschutzbehörde, Barichgasse 40-42, 1030 Wien. Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(2) Dieser Erklärung liegt folgende Anlage bei, die einen integrierenden Bestandteil der Erklärung bildet:

- • **Anlage ./1** – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 1
Technisch-organisatorische Maßnahmen
Präventive Sicherheitsmaßnahmen – Maßnahmen zur Verhinderung eines erfolgreichen Angriffs

Technische Maßnahmen:
(1) Encryption at Rest: Alle personenbezogenen Daten werden verschlüsselt in der Datenbank abgelegt. Jede KundIn erhält einen eigenen Schlüssel.

(2) Authentifizierung: Jeglicher Zugriff auf personenbezogene Daten erfolgt ausschließlich nach einer erfolgreichen Zwei-Faktor-Authentifizierung.

(3) Passwortsicherheit: Soweit Passwörter zur Authentifizierung eingesetzt werden, müssen diese mindestens 8 Zeichen lang sein.

(4) Verschlüsselung auf dem Übertragungsweg: Personenbezogene Daten werden auf dem Übertragungsweg über das Internet verschlüsselt und ebenso verschlüsselt abgespeichert.

(5) Netzwerksicherheit: Es wird eine Firewall eingesetzt, welche das interne Netzwerk

vom Internet trennt und – soweit möglich – eingehenden Netzwerkverkehr blockiert.

(6) Maßnahmen gegen Schadsoftware: Es wird nach Möglichkeit auf allen Systemen Anti-Viren Software eingesetzt.

(7) Management von Sicherheitslücken: Soweit möglich, wird auf allen Geräten die automatische Installation von Sicherheitsupdates aktiviert.

(8) Backup-Konzept: Regelmäßige Erstellung von Backups (Sicherungskopien), die räumlich getrennt vom Live-System aufbewahrt werden.

(9) Wiederherstellbarkeit: Regelmäßige Tests der Wiederherstellung von Daten aus Backups (Restore-Tests).

(10) Mandantentrennung: Strikte logische Trennung der Daten verschiedener Auftraggeber, sodass kein Kunde Zugriff auf die Daten eines anderen Kunden hat.

(11) Getrennte Umgebungen: Strikte Trennung von Entwicklungs-, Test- und Produktionsumgebungen.

Organisatorische Maßnahmen
(1) Klare Zuständigkeiten: Interne Zuständigkeiten für Fragen der Datensicherheit werden definiert.

(2) Verschwiegenheitspflicht der Dienstnehmer: Die Dienstnehmer werden über die Dauer ihres Dienstverhältnisses hinaus zur Verschwiegenheit verpflichtet. Insbesondere werden sie dazu verpflichtet, personenbezogene Daten nur auf ausdrückliche Anweisung eines Vorgesetzten an Dritte zu übermitteln.

(3) Schulungen und Informationsmaßnahmen: Die Dienstnehmer werden zu Fragen der Datensicherheit (intern oder extern) geschult und angemessen über Fragen der Datensicherheit informiert (z,B. Passwortsicherheit).

(4) Geordnete Beendigung des Dienstverhältnisses: Bei Beendigung des Dienstverhältnisses erfolgt eine unverzügliche Sperrung aller Konten des ausscheidenden Dienstnehmers sowie eine Abnahme aller Schlüssel des ausscheidenden Dienstnehmers.

(5) Keine unnötige Verwendung administrativer Accounts: Benutzer-Accounts mit administrativen Rechten werden nur in Ausnahmefällen verwendet. Die reguläre Nutzung von IT-Systemen erfolgt ohne administrative Rechte.