PsyCalc

Auftragsverarbeitungsvertrag

Auftragsverarbeiter:
PsyCalc UG (haftungsbeschränkt)
Platanenstr. 27, 40233 Düsseldorf

Im Rahmen der Leistungserbringung nach dem Hauptvertrag wird zum Schutz der von dem Auftragsverarbeiter verarbeiteten Daten des Auftraggebers nach Vorgabe der Datenschutzgrundverordnung folgendes vereinbart:

§ 1 Vertragsinhalt und Laufzeit

(1) Inhalt des Vertragsanhangs ist die Datenverarbeitung, die der Auftragsverarbeiter für den Auftraggeber im Rahmen des Hauptvertrages ausführt. Dies umfasst jede Verarbeitung von personenbezogenen Daten im Rahmen des Hauptvertrages gem. Art. 28 DSGVO.

(2) Zweck der Verarbeitung ist die Erfüllung des Hauptvertrages durch den Auftragsverarbeiter und die Erfüllung der Verpflichtungen beider Parteien aus der DSGVO.

(3) Die Laufzeit dieses Vertrages ergibt sich aus seinem Zweck. Er läuft für die Dauer des Hauptvertrages einschließlich der Erfüllung von Gewährleistungspflichten oder sonstigen nachvertraglichen Pflichten durch den Auftragsverarbeiter. Wird der Hauptvertrag gekündigt, bleibt dieser Vertrag für die Dauer der verbleibenden nachvertraglichen Pflichten bestehen und endet erst mit der Vollbeendigung des Hauptvertrages und der Löschung oder Rückgabe der Daten nach Maßgabe dieses Anhangs.

§ 2 Art der Daten, der Betroffenen und der Verarbeitung, Vertragsort

(1) Dieser Vertragsanhang gilt für alle Arten von Verarbeitungen gem. Art. 4 Nr. 2 DSGVO.

(2) Die Art der verarbeiteten Daten umfasst alle Daten, die der Auftragsverarbeiter für den Auftraggeber im Rahmen des Hauptvertrages verarbeitet. Die Daten sind in Anlage 1 zu diesem Vertrag näher aufgeführt.

(3) Die Kategorien der von diesem Vertrag betroffenen Personen ergeben sich aus der Datennutzung durch den Auftraggeber, sie sind in Anlage 1 zu diesem Vertragsanhang näher aufgeführt.

(4) Eine Verarbeitung außerhalb der europäischen Union ist nur in den gesetzlich erlaubten Fällen möglich.

§ 3 Verantwortung und Weisungen

(1) Dieser Vertragsanhang ändert nichts daran, dass der Auftraggeber für die Einhaltung der Datenschutzgesetze und eine rechtmäßige Weitergabe der Daten an den Auftragsverarbeiter gem. Art. 4 Abs. 7 DSGVO allein Verantwortlicher bleibt. Dies gilt auch für alle Verarbeitungen, die Gegenstand dieses Vertragsanhangs sind.

(2) Weisungen im Rahmen der Auftragsverarbeitung werden von dem Auftraggeber zum einen im Hauptauftrag festgelegt. Anschließend können sie mündlich oder in Textform erteilt werden. Der Auftragsverarbeiter hat einen Anspruch darauf, dass mündliche Weisungen unverzüglich auch in Textform bestätigt werden (z.B. E-Mail oder sonstige elektronische Form). Der Auftragsverarbeiter kann – außer bei Gefahr im Verzuge – die Ausführung der Weisung von einer vorherigen Weisung in Textform abhängig machen.

(3) Weisungen, die über den Inhalt des Hauptvertrages hinausgehen, sind für den Auftragsverarbeiter nur verbindlich, wenn sie nach dem Sinn des Hauptvertrages und auf Grund der Bestimmungen der DSGVO erforderlich sind (zB in einer Angriffssituation erforderliche Sicherungen). Sie sind gleichzeitig eine Zusatzleistung im Rahmen des Hauptvertrages und nach den dortigen Bestimmungen zusätzlich – ersatzweise anhand der ortsüblichen und angemessenen Vergütung – zu entrichten.

(4) Ist der Auftragsverarbeiter nicht zur Ausführung der Weisung verpflichtet, kann er die Ausführung verweigern, bis der Auftraggeber die Zusatzleistung bestätigt und kostenpflichtig beauftragt hat. Die Ausführung der Weisung ist kein Verzicht auf einen Anspruch auf zusätzliche Vergütung.

(5) Ist dem Auftragsverarbeiter die Ausführung einer Weisung nicht zuzumuten, etwa weil Ihre Befolgung technisch nicht möglich ist, kann der Auftragsverarbeiter den Hauptvertrag kündigen, sofern zwischen den Parteien keine andere Lösung gefunden wird. Ein Beispiel ist etwa eine Leistungserbringung durch den Auftragsverarbeiter auf einer technischen Plattform mit anderen Auftraggebern einer Aufttragsverarbeitung, bei der die Weisung nicht ohne Konsequenzen für andere Vertragspartner des Auftragsverarbeiters befolgt werden kann (z.B. Daten können nicht getrennt werden).
(6) Erteilt der Auftraggeber eine rechtswidrige Weisung, hat er die daraus entstehenden Kosten zu tragen, einschließlich der Rechtsberatungs- oder -vertretungskosten des Auftragsverarbeiters.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter ist verpflichtet, die Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers zu verarbeiten. Dies gilt nicht, soweit der Auftragsverarbeiter zu einer anderen Verarbeitung aufgrund eines in der europäischen Union für ihn gültigen Rechts verpflichtet ist. Der Auftragsverarbeiter kann eine Weisung, die gegen geltendes Recht verstößt, das auch für ihn bindend ist, zurückweisen und ist zu Ihrer Ausführung nicht verpflichtet. Der Auftragsverarbeiter wird in einem solchen Fall den Auftraggeber auffordern, eine rechtmäßige Weisung zu erteilen.
(2) Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Erfüllung von Auskunftspflichten Betroffener im Rahmen seiner Kapazitäten. Er benennt dem Auftraggeber einen Ansprechpartner im Rahmen des Datenschutzes.
(3) Der Auftragsverarbeiter wird in seinem Bereich für den Auftraggeber die Pflichten aus Art. 32 bis 36 DSGVO unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen einhalten und in angemessenen Abständen überprüfen.
(4) Der Auftragsverarbeiter organisiert seinen Betrieb derart, dass er den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft gem. Art. 32 DSGVO unter Berücksichtigung seiner zumutbaren Möglichkeiten und Einrichtungen technische und organisatorische Maßnahmen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Die derzeitigen technischen und organisatorischen Maßnahmen sind in Anlage 2 zu diesem Vertrag festgehalten.

(5) Der Auftragsverarbeiter gewährleistet, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere eingesetzte Dritte verpflichtet sind, die Daten nicht außerhalb der Weisungen des Auftraggebers zu verarbeiten und die Daten vertraulich zu behandeln sowie diese Verschwiegenheitspflicht auch nach der Beendigung des Hauptvertrages fort gilt.
(6) Der Auftragsverarbeiter unterrichtet den Auftraggeber, sofern er Kenntnis davon erlangt, das Daten des Auftraggebers verletzt wurden oder werden. Er trifft zur Gefahrenabwehr eigenständig die erforderlichen Maßnahmen zur Datensicherung und mindert soweit möglich die Folgen für die Betroffenen. Er spricht sich so schnell wie möglich mit dem Auftraggeber ab.
(7) Der Auftragsverarbeiter wird den Auftraggeber im Rahmen seiner Möglichkeiten bei der Abwehr von Ansprüchen gem. Art. 82 DSGVO unterstützen.
(8) Nach Abschluss der Verarbeitungstätigkeit löscht der Auftragsverarbeiter nach Wahl des Auftraggebers entweder alle personenbezogenen Daten oder gibt sie dem Auftraggeber zurück. Dies gilt nicht, soweit die Daten nach dem anwendbaren Recht weiter gespeichert bleiben müssen oder sich aus dem Vertrag ein anderes ergibt. Erteilt der Auftraggeber keine Weisung, gilt die Löschung als vereinbart.

§ 5 Vergütung

(1) Für alle Leistungen nach diesem Vertrag hat der Auftragsverarbeiter Anspruch auf eine zusätzliche Vergütung nach Maßgabe des Hauptvertrages, ersatzweise der ortsüblichen und angemessenen Vergütung. Dies gilt nicht, soweit der Hauptvertrag ausdrücklich ein anderes regelt oder solche Ansprüche aufgrund Gewährleistung oder Verschulden des Auftragsverarbeiters ausgeschlossen sind.
(2) Die Verpflichtung zur Vergütung gilt bis zur Vollbeendigung dieses Anhanges und endet nicht mit dem Hauptvertrag.

§ 6 Pflichten des Auftraggebers

(1) Der Auftraggeber darf keine Weisung erteilen, die gegen geltendes Recht verstößt. Der Auftraggeber ist weiter Verantwortlicher für die Daten, es ist daher seine Sache, sich über die geltenden Gesetze zu informieren und sich dazu beraten zu lassen und dem Auftragsverarbeiter nur solche Weisungen zu erteilen, die rechtmäßig sind.

(2) Der Auftraggeber ist verpflichtet, die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters zu erfragen und zu prüfen. Er trägt die Verantwortung dafür, dass die Maßnahmen des Auftragsverarbeiters für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau darstellen.
(3) Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich und vollständig, wenn ihm Tatsachen offenbar werden, dass bei der Datenverarbeitung Fehler oder Unregelmäßigkeiten vorkommen.
(4) Der Auftraggeber benennt auf Anforderung des Auftragsverarbeiters einen Ansprechpartner für alle Datenschutzfragen in seinem Hause.
(5) Der Auftraggeber ist verpflichtet, Forderungen von Betroffenen auf Berichtigung, Löschung oder Auskunft zu bearbeiten. Der Auftragsverarbeiter wird die betroffene Person an den Auftraggeber verweisen, sofern das aufgrund der Angaben der betroffenen Person möglich ist. Der Auftragsverarbeiter haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 7 Nachweise

(1) Der Auftragsverarbeiter informiert den Auftraggeber über alle Maßnahmen zur Einhaltung der Anforderungen des Art. 28 DSGVO und ermöglicht in zumutbarem Rahmen Überprüfungen. § 5 gilt entsprechend.
(2) Der Auftragsverarbeiter ist berechtigt, von dem Auftraggeber und/oder dessen Prüfer eine Verschwiegenheitserklärung zu verlangen. Der Auftraggeber kann einen unabhängigen externen Prüfer benennen, sofern er dem Auftragsverabreiter eine Kopie des Auditberichts zur Verfügung stellt. Wettbewerber des Auftragsverarbeiters oder Personen, die dem Auftragsverabreiter sonst nicht zumutbar sind, kann der Auftragsverarbeiter ablehnen.
(3) Für Prüfungen einer Behörde gelten diese Regeln entsprechend, einschließlich § 5.

§ 8 Weitere Auftragsverarbeiter/Subunternehmer

(1) Der Auftragsverarbeiter ist berechtigt, weitere Auftragsverarbeiter nach Art. 28 DSGVO einzusetzen, um den Vertrag zu erfüllen.
(2) Die weiteren Auftragsverarbeiter, die derzeit eingesetzt werden, sind in Anlage 3 zu diesem Vertrag aufgeführt. Der Auftraggeber willigt in ihren Einsatz ein.

(3) Der Auftragsverarbeiter wird den Auftraggber unterrichten, wenn er andere Subunternehmer einzusetzen wünscht. Der Auftraggeber kann diese ablehnen, wenn dafür ein wichtiger Grund besteht. Ist dem Auftragsverarbeiter aufgrund der Ablehnung eines neuen Subunternehmers die Erfüllung des Vertrages nicht mehr zumutbar, kann er den Hauptvertrag innerhalb einer angemessenen Frist kündigen.
(4) Der Auftragsverarbeiter ist verpflichtet, die Pflichten aus diesem Vertrag auf die Subunternehmer zu übertragen.
(5) Subunternehmer im Sinne dieser Regelung sind nur solche Unternehmen, die Dienstleistungen unmittelbar in Bezug auf die Hauptleistung des Vertrages beziehen. Davon sind insbesondere Nebenleistungen wie Telekommunikations-, Druck- und Transportleistungen ebenso ausgenommen wie Pflichten zu reiner Wartung, die Entsorgung von Datenträgern sowie Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der personenbezogenen Daten, Netze, Dienste, Datenverarbeitungsanlagen und sonstiger IT- Systeme. Unberührt bleibt die Verpflichtung des Auftragsverarbeiters, Datenschutz und Datensicherheit in Bezug auf die Daten des Auftraggebers sicher zu stellen.

§ 9 Haftung und Schadensersatz

(1) Macht ein Betroffener Schadensersatzansprüche gegen eine Vertragspartei geltend, unterstützen sich die Parteien und tragen gemeinsam und zur Aufklärung des Sachverhalts bei.
(2) Für die Haftung gilt ansonsten der Hauptvertrag.

§ 10 Schlussbestimmungen

(1) Für Streitschlichtung, Rechtswahl und Gerichtsstand gilt der Hauptvertrag.
(2) Dieser Vertrag ist in Textform geschlossen und bedarf zu seiner Änderung der Textform.

- Anlage 1 – betroffene Daten- und Personengruppen
- Anlage 2 – technische und organisatorische Maßnahmen
- Anlage 3 - Subunternehmer

Anlage 1 - Betroffene Daten- und Personengruppen

Art der Daten	Art und Zweck der Datenverarbeitung	Kategorien betroffener Personen
Kundendaten - Bestandsdaten (z.B. Namen, Adressen) - Kontaktdaten (z.B. E-Mail, Telefonnummern) - Vertragsdaten (z.B. Vertragsgegenstand, Laufzeit) - Zahlungsdaten (z.B. Bankverbindung, Zahlungshistorie)	Finanzbuchhaltung	Kunden
Mitarbeiterdaten - Name - E-Mail - Nutzungsdaten (z.B. Protokolldaten, Zugriffszeiten) - Meta-/ Kommunikations-daten (z.B. IP-Adressen, Standortdaten)	Autorisierungsprozess für die Zugangsberechtigung zu PsyCalc	Mitarbeiter der Kunden
Patientendaten - Geschlecht - Geburtsjahr	Normen für die Durch-führung bei einigen Tests	Patienten der Kunden

Anlage 2 - technische und organisatorische Maßnahmen zum Schutz der Daten

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Kontrollziele	Maßnahmen
Zugangskontrolle Maßnahmen, die verhindern, dass unbefugte Dritte Zugang zu Datenverarbeitungsanlagen haben	- Persönlicher und individueller Login bei Anmeldung am System/Netzwerk - Arbeitsgeräte sind alle passwort-geschützt - Anti-Viren Systeme werden eingesetzt - Einsatz einer Software-Firewall
Zugriffskontrolle Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	- Autorisierungsprozess für Berechtigungen - Verwaltung und Dokumentation von differenzierten Berechtigungen - Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten - Einhaltung von betriebsinternen Passwortrichtlinien
Trennungskontrolle Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	- Speicherung der Datensätze in physikalisch getrennten Datenbanken - Zugriffsberechtigungen nach funktioneller Zuständigkeit - Trennung von Produktiv- und Testsystem

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Kontrollziele	Maßnahmen
Weitergabekontrolle Maßnahmen, die gewährleisten, dass Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert, entfernt oder sonst verarbeitet werden können und überprüft werden kann, welche Personen oder Stellen Zugriff auf Daten erhalten haben.	- E-Mail-Verschlüsselung - Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
Eingabekontrolle Es ist zu gewährleisten, dass nachträglich überprüft und Festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt werden.	- Protokollierung der Eingabe, Änderung und Löschung der Daten - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen - Vergabe von Rechten zur Eingabe,

	Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Kontrollziele	Maßnahmen
Verfügbarkeitskontrolle / Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	- Bedarfsgerechtes Einspielen von Sicherheits-Updates - Backup-System - Virenschutz - Firewall

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Kontrollziele	Maßnahmen
Datenschutz-Management Maßnahmen, die gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist	- Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO) - Verpflichtung der Mitarbeiter auf die Vertraulichkeit - Hinreichende Schulungen der Mitarbeiter im Datenschutz
Auftragskontrolle Durch folgende Maßnahmen ist sichergestellt, dass Daten nur nach Weisungen des Auftraggebers verarbeitet werden	- Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten der Parteien

Anlage 3 – Subunternehmer im Rahmen der Auftragsverarbeitung

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistungen
RAIDBOXES GmbH Friedrich-Ebert-Straße 7 48153 Münster	Hosting der Standard-Software PsyCalc
Haufe-Lexware GmbH & Co. KG Munzinger Straße 9 79111 Freiburg	Finanzbuchhaltung