Auftragsverarbeitungsvertrag CloudPal

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

zwischen

Auftraggeber

– nachfolgend **„Auftraggeber“** genannt –

und

“CloudPal”, Pico Ventures GmbH, Novalisstraße , 10119 Berlin

– nachfolgend **„Auftragnehmer“** genannt –

1. Vertragsgegenstand

Im Rahmen der Leistungserbringung nach dem Vertrag über die Nutzung der CloudPal-Plattform (nachfolgend **„Hauptvertrag“** genannt) ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend **„Auftraggeber-Daten“** genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

2. Umfang der Beauftragung

(1) Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.

(2) Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie in Anlage 1 zu diesem Vertrag spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

(3) Die Verarbeitung der personenbezogenen Daten des Auftraggebers durch den Auftragnehmer erfolgt ausschließlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR). Eine Verarbeitung in Staaten außerhalb des EWR ist grundsätzlich ausgeschlossen und derzeit nicht vorgesehen. Nur für den Fall, dass der Auftragnehmer zukünftig eine Verarbeitung in einem Drittland erwägt, gilt: Eine solche Verarbeitung darf ausschließlich erfolgen, wenn

der Auftraggeber vorab ausdrücklich informiert wird und der Auftraggeber der Drittlandverarbeitung vorab zugestimmt hat und die Voraussetzungen der Art. 44–48 DSGVO eingehalten werden oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

3. Weisungsbefugnisse des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens, in dem die Weisung zu dokumentieren und die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber zu regeln ist.

(3) Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeber-Daten beim Auftraggeber liegt.

4. Verantwortlichkeit des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen. Für weitere Auftragsverarbeiter gemäß Ziffer 7. haftet Pico Ventures gemäß Ziffer 13. wie für eigenes Verschulden.

(2) Dem Auftraggeber obliegt es, dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeber-Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

(3) Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

(4) Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

5. Anforderungen an Personal

Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

6. Sicherheit der Verarbeitung

(1) Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.

(2) Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrags zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen.

7. Inanspruchnahme weiterer Auftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus Anlage 2. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.

(2) Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht

innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 30 Tagen zu kündigen.

(3) Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrags obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

(4) Derzeit findet keine Verarbeitung personenbezogener Daten außerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR) statt. Für den Fall, dass künftig eine Verarbeitung in einem Drittstaat erforderlich wird, gelten ergänzend die folgenden Regelungen: Unter Einhaltung der Anforderungen der Ziffer 2. (3) dieses Vertrags gelten die Regelungen in dieser Ziffer 7 auch wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird. In diesem Fall vereinbart der Auftragnehmer mit dem weiteren Auftragsverarbeiter die EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern vom 04. Juni 2021, Modul 3. Der Auftraggeber erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Art. 49 DSGVO im erforderlichen Maße mitzuwirken.

8. Rechte der betroffenen Personen

(1) Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

(2) Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

(3) Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Auftraggeber-Daten, die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.

(4) Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

(5) Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Art. 20 DSGVO besitzt, wird der

Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen bei der Bereitstellung der Auftraggeber-Daten in einem gängigen und maschinenlesbaren Format unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

(6) Soweit dem Auftragnehmer durch die Unterstützung des Auftraggebers bei der Erfüllung seiner Verpflichtungen gegenüber betroffenen Personen gemäß dieses Abschnitts Kosten entstehen, die über einen üblichen und angemessenen Aufwand hinausgehen, ist der Auftraggeber verpflichtet, dem Auftragnehmer diese Mehrkosten zu erstatten.

9. Mitteilungs- und Unterstützungspflichten des Auftragnehmers

(1) Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber zeitnah, aber spätestens 24 Stunden nach Bekanntwerden, über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen unterstützen. Die Regelung in Ziffer 8.6 gilt entsprechend.

(2) Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich ggf. anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

10. Datenlöschung

(1) Der Auftragnehmer wird die Auftraggeber-Daten nach Beendigung dieses Vertrages löschen oder herausgeben, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

11. Nachweise und Überprüfungen

(1) Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

(2) Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

(3) Zur Durchführung von Inspektionen nach Ziffer 11.2 ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 18 Uhr) nach rechtzeitiger Vorankündigung gemäß Ziffer 11.5 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeber-Daten verarbeitet werden.

(4) Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

(5) Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.

(6) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 11 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

12. Vertragsdauer und Kündigung

Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Die Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

13. Haftung

(1) Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich

Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

(2) Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

14. Schlussbestimmungen

(1) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DSGVO genügt.

(2) Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

Anlagen:

Anlage 1:	Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen
Anlage 2:	Weitere Auftragsverarbeiter
Anlage 3:	Technische und organisatorische Maßnahmen

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Zweck der Datenverarbeitung: Vertragsgemäße Bereitstellung der CloudPal-Plattform, Nutzung von LLMs
Art und Umfang der Datenverarbeitung: Art der Daten: - Vor-/Nachname, E-Mail-Adresse von Mitarbeitern und sonstigen Nutzern des Auftraggebers - Kommunikationsinhalte mit LLMs (z.B. vom Nutzer eingegebene Chat-Nachrichten) - Informationen in Dokumenten, die der Auftraggeber auf der Plattform speichert (zusammen “Auftraggeber-Daten”)
Betroffene Personen (Kategorien): - Mitarbeiter und sonstige Nutzer des Auftraggebers (zusammen “Nutzer”) - Personen, auf die sich Kommunikationsinhalte mit LLMs beziehen - Personen, auf die sich Dokumente beziehen, die der Auftraggeber auf der Plattform speichert (zusammen “Betroffene Personen des Auftraggebers”)

Anlage 2: Weitere Auftragsverarbeiter

Firma, Anschrift	Zweck der Datenverarbeitung	Betroffene Personen (Kategorien)	Personenbezogene Daten (Kategorien)	Drittlandtransfer sowie geeignete Garantie
Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855, Luxembourg	Leistungserbringung gemäß Hauptvertrag	Betroffene Personen des Auftraggebers	Auftraggeber-Daten	EU-Region (Frankfurt), in seltenen Ausnahmefällen US-Zugriff (SCCs/DPF)
Microsoft Ireland Operations Limited, The Atrium / Building, Block B, Carmanhall Road, Sandyford Business Estate, Dublin 18, Ireland	Leistungserbringung gemäß Hauptvertrag	Betroffene Personen des Auftraggebers	Auftraggeber-Daten	EU-Region, in seltenen Ausnahmefällen US-Zugriff (SCCs)
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland	Leistungserbringung gemäß Hauptvertrag	Betroffene Personen des Auftraggebers	Auftraggeber-Daten	EU-Region, in seltenen Ausnahmefällen US-Zugriff (SCCs/DPF)

Anlage 3: Technische und organisatorische Maßnahmen des Auftragsverarbeiters

CloudPal nutzt Amazon Web Services als Datenverarbeiter für ihr Kernprodukt und zugehörige Datenbanken. Amazon Web Services ist eine vertrauenswürdige und hochsichere Infrastruktur, die regelmäßig von internationalen Standards wie ISO/IEC 27001:2013, 27017:2015, 27018:2019 und ISO/IEC 9001:2015 sowie CSA STAR CCM v3.0.1 geprüft und zertifiziert wird.

Zudem trifft CloudPal geeignete technische und organisatorische Maßnahmen, um ein angemessenes Schutzniveau im Rahmen des Datenschutzes und der Datensicherheit des vorliegenden Auftragsverhältnisses zu gewährleisten. CloudPal sichert - insbesondere die Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der eingesetzten Systeme bzw. Anwendungen - zu und setzt hierzu u. a. die nachfolgenden Maßnahmen um. CloudPal erfüllt dies durch folgende Maßnahmen:

1. **Maßnahmen zur Sicherung der Vertraulichkeit gemäß Art. 32 Abs. 1 lit. b) DSGVO**

   a. **Zutrittskontrolle**

   Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie vertraulichen Akten und Datenträgern physisch verwehren:

CloudPal		**Maßnahmen bei Amazon Web Services**	
✓	Alarmanlage	✓	Physische Barrieren für unbefugte Besucher
✓	Klingelanlage mit Kamera	✓	elektronische Zugangskontrolle (z. B. Kartenlesegeräte usw.)
✓	Chipkarten/Transponder-Systeme	✓	Überprüfung durch Sicherheitspersonal (Empfang)
✓	Manuelles Schließsystem	✓	Foto-ID-Ausweise für Mitarbeiter und Auftragnehmer (Tragepflicht)
✓	Sicherheitsschlösser	✓	Anmeldung von Besuchern (Ausweiskontrolle)

✓	Türen mit Knauf Außenseite	✓	Tragepflicht von Besucherausweisen
✓	Kontrollierte Schlüsselvergabe	✓	Besucherbegleitung durch autorisiertes Personal
		✓	Gesicherter Zustand aller Zugangspunkte (außer Hauseingangstüren)
		✓	Videoüberwachung der Zugangspunkte
		✓	Elektronische Einbruchmeldesysteme (Überwachung Schwachstellen (z. B. Hauseingangstüren, Dachluken, Laderampentüren etc.)
		✓	Innenraum-Bewegungsmelder
		✓	Glasbruchmelder
		✓	Protokollierung der Besucher

b. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können:

CloudPal	Maßnahmen bei Amazon Web Services

✓	Authentifikation Benutzername/Passwort	✓	Zugangskontrollen und Richtlinien (Zugang zum AWS-Netzwerk von jeder Netzwerkverbindung und jedem Benutzer)
✓	Einsatz und Aktualisierung Anti-Viren-Software Server/Clients	✓	Verwendung von Firewalls oder funktional äquivalenter Technologie
✓	Einsatz Hardware-Firewall	✓	Authentifizierungskontrollen
✓	Automatische Desktopsperre	✓	Korrekturmaßnahmen und Vorfallsreaktions-pläne
✓	Anleitung “Manuelle Desktopsperre”	✓	Ausgewählte Zugangsprivilegien und Widerruf bei Wegfall des Geschäftsbedarfs
✓	Verwalten von Benutzerberechtigungen		
✓	Erstellen von Benutzerprofilen		
✓	Richtlinie “Sicheres Passwort”		
✓	Richtlinie “Löschen/Vernichten” bzw. Archivierungskonzept		

✓	Richtlinie “Clean-Desk”		
✓	Allg. Richtlinie Datenschutz und/oder Sicherheit		

c. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

CloudPal		**Maßnahmen bei Amazon Web Services**	
✓	Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten		
✓	Passwortrichtlinie (Passwortlänger und Passwortwechsel)		
✓	Minimale Anzahl an Administratoren		
✓	Verwaltung Benutzerrechte durch Administratoren		

d. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist:

CloudPal	**Maßnahmen bei Amazon Web Services**

✓	Logische Kunden-/Mandantentrennung	✓	Zugangskontrollen und Richtlinien (Zugang zum AWS-Netzwerk von jeder Netzwerkverbindung und jedem Benutzer)
✓	Datenschutzrichtlinie	✓	Verwendung von Firewalls oder funktional äquivalenter Technologie
✓	Festlegung von Datenbankrechten	✓	Authentifizierungskontrollen
		✓	Korrekturmaßnahmen und Vorfallsreaktionspläne

2. Maßnahmen zur Sicherung der Integrität gemäß Art. 32 Abs. 1 lit. b) DSGVO

a) Weitergabe- und Übertragungskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können sowie Maßnahmen mit denen überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist:

CloudPal		**Maßnahmen bei Amazon Web Services**	
✓	Protokollierung der Zugriffe und Abrufe (Aufzeichnungsverfahren)	✓	Zugangskontrollen und Richtlinien (Zugang zum AWS-Netzwerk von jeder Netzwerkverbindung und jedem Benutzer)
✓	Bereitstellung über verschlüsselte Verbindungen wie sftp, https	✓	Verwendung von Firewalls oder funktional äquivalenter Technologie

✓	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen	✓	Authentifizierungskontrollen
		✓	Korrekturmaßnahmen und Vorfallsreaktionspläne

b) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind:

CloudPal		**Maßnahmen bei Amazon Web Services**	
✓	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können	✓	Aufzeichnung aller Systemaktivitäten und Speicherung dieser Aufzeichnungen für mindestens drei Jahre
✓	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	✓	Systeme zur Auswertung der Aufzeichnungen
✓	Manuelle oder automatisierte Kontrolle der Protokolle		

3. Maßnahmen zur Sicherung der Verfügbarkeit gemäß Art. 32 Abs. 1 lit. b) DSGVO

a) Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

CloudPal		Maßnahmen bei Amazon Web Services	
✓	Feuer- und Rauchmeldeanlagen	✓	Informationssicherheitsprogramm
✓	Alarmsystem	✓	Unterstützung bei Sicherung von Kundendaten gegen zufälligen oder unrechtmäßigen Verlust, Zugriff oder Offenlegung
✓	Prozess und Kontrolle des Datensicherungsvorgangs	✓	Unterstützung bei Identifikation von vorhersehbaren und internen Sicherheitsrisiken sowie unbefugten Zugang zum AWS-Netzwerk
✓	Backup-Überwachung	✓	Unterstützung bei Minimierung von Sicherheitsrisiken durch Risikobewertung und regelmäßige Tests
✓	Hosting in zertifizierten Rechenzentren		

4. Maßnahmen zur Sicherung der Verfügbarkeit gemäß Art. 32 Abs. 1 lit. b) DSGVO

Maßnahmen, die die Überprüfung einer datenschutzkonformen und sicheren Verarbeitung kontinuierlich sicherstellen:

CloudPal	Maßnahmen bei Amazon Web Services

✓	Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeitende nach Bedarf/Berechtigung (z. B. Wiki, Intranet etc.)	✓	periodische Überprüfungen der Sicherheit des AWS-Netzwerks und Angemessenheit des Informationssicherheitsprogramms (Branchensicherheitsstandards)
✓	Anderweitiges dokumentiertes Sicherheits-Konzept	✓	Kontinuierliche Bewertung der Sicherheit des AWS-Netzwerks und der zugehörigen Dienste
✓	Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen (mind. jährlich)	✓	Unterstützung bei Sicherung von Kundendaten gegen zufälligen oder unrechtmäßigen Verlust, Zugriff oder Offenlegung
✓	Regelmäßige Schwachstellenanalysen	✓	Unterstützung bei Identifikation von vorhersehbaren und internen Sicherheitsrisiken sowie unbefugten Zugang zum AWS-Netzwerk
✓	Regelmäßiges Penetrations-Testing	✓	Unterstützung bei Minimierung von Sicherheitsrisiken durch Risikobewertung und regelmäßige Tests
✓	Benennung interne/r oder externe/r Datenschutzbeauftragte/r (DSB)		
✓	Interner/externer Informations-Sicherheits-Beauftragter		
✓	Regelmäßige Schulung der Mitarbeitenden (mind. jährlich) und auf Vertraulichkeit/Datengeheimnis verpflichtet		

✓	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener		
✓	Formalisierter Prozess im Falle von Datenschutz- oder Sicherheitsvorfällen		
✓	Durchführung Datenschutz-Folgeabschätzung (DSFA)		