

AVV (Auftragsverarbeitungsvertrag)

Datenschutz ist uns wichtig.

Der Schutz personenbezogener Daten hat für Calmio einen hohen Stellenwert. Deshalb haben wir diesen Auftragsverarbeitungsvertrag bewusst klar, transparent und praxisnah gestaltet. Er regelt, wie wir personenbezogene Daten im Auftrag unserer Kunden verarbeiten und welche Rechte und Pflichten dabei für beide Seiten gelten.

Worum geht es in Kürze?

- Calmio verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Kunden.
- Der Kunde bleibt Verantwortlicher im Sinne der DSGVO und entscheidet über Zweck und Rechtmäßigkeit der Datenverarbeitung.
- Wir setzen angemessene technische und organisatorische Maßnahmen ein, um personenbezogene Daten zu schützen.
- Weitere Informationen zu unseren Sicherheitsmaßnahmen findest Du in den Technischen und Organisatorischen Maßnahmen (TOMs), die Bestandteil dieses Vertrags sind.

Solltest Du Fragen zu diesem Auftragsverarbeitungsvertrag oder zum Datenschutz bei Calmio haben, unterstützen wir Dich jederzeit gerne.

Auftragsverarbeitungsvertrag (AVV)

zwischen

Kunde (Praxis) – Verantwortlicher

und

Calmio GmbH – Auftragsverarbeiter (nachfolgend „Calmio“)

§1 Gegenstand

Gegenstand dieses Auftragsverarbeitungsvertrages ist die Verarbeitung personenbezogener Daten durch Calmio im Auftrag des Kunden im Rahmen der Nutzung der Calmio-Plattform und der hierzugehörigen Dienste.

Dieser Vertrag erfüllt die Anforderungen des Art. 28 DSGVO und konkretisiert die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten im Auftrag.

Die Verarbeitung erfolgt ausschließlich im Rahmen der vertraglich vereinbarten Leistungen sowie nach dokumentierten Weisungen des Kunden im Sinne des Art. 28 DSGVO.

§2 Zweck der Verarbeitung

Die Verarbeitung erfolgt ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen, insbesondere zur Unterstützung und Automatisierung administrativer, organisatorischer und kommunikationsbezogener Prozesse im Gesundheitswesen. Hierzu zählen insbesondere:

- Bearbeitung von Patientenfragen
- Kommunikation über Telefon, E-Mail, Messaging-Dienste und sonstige Kommunikationskanäle
- Terminmanagement
- Unterstützung der Praxisorganisation
- Dokumentation von Kommunikationsvorgängen
- Automatisierung administrativer Abläufe
- Bereitstellung statistischer und organisatorischer Auswertungen

§3 Datenarten

- Name
- Telefonnummer
- Terminwünsche
- Kommunikationsinhalte
- ggf. gesundheitsbezogene Informationen
- E-Mail-Adresse
- Anschrift (soweit übermittelt)
- Geburtsdatum (soweit übermittelt)
- Terminhistorie
- Kommunikationshistorie
- Gesprächsprotokolle
- technische Nutzungsdaten (z. B. IP-Adresse, Geräteinformationen, Logdaten)
- Patienten- oder Kundennummern
- Verordnungs- oder Rezeptinformationen (soweit verarbeitet)

Gesundheitsbezogene Daten werden mit besonderer Sorgfalt und unter Anwendung erhöhter Sicherheitsmaßnahmen verarbeitet.

§4 Kategorien betroffener Personen

- Patienten
- Interessenten

§5 Rechtsgrundlage

Die datenschutzrechtliche Verantwortlichkeit für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten, insbesondere das Vorliegen einer geeigneten Rechtsgrundlage gemäß Art. 6 und Art. 9 DSGVO, liegt ausschließlich beim Kunden als Verantwortlichem. Calmio verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach dokumentierten Weisungen des Kunden.

§6 Weisungsrecht

Der Kunde kann jederzeit Weisungen zur Datenverarbeitung erteilen. Weisungen des Kunden erfolgen grundsätzlich in Textform (z. B. E-Mail). Mündliche Weisungen sind vom Kunden unverzüglich in Textform zu bestätigen.

Hält Calmio eine Weisung des Kunden für datenschutzrechtlich oder gesetzlich unzulässig, wird Calmio den Kunden hierauf unverzüglich hinweisen. Bis zur Bestätigung oder Änderung der Weisung ist Calmio berechtigt, deren Ausführung auszusetzen.

§7 Technische und organisatorische Maßnahmen (TOMs)

Calmio trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau sicherzustellen.

Die Einzelheiten ergeben sich aus der diesem Vertrag als Anlage beigefügten Beschreibung der Technischen und Organisatorischen Maßnahmen (TOMs), die Bestandteil dieses Vertrages ist.

Calmio ist berechtigt, die TOMs an den Stand der Technik oder geänderte gesetzliche Anforderungen anzupassen, sofern hierdurch das Datenschutzniveau nicht abgesenkt wird. Calmio überprüft die Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig und passt diese bei Bedarf an den Stand der Technik an.

§8 Subunternehmer

Calmio ist berechtigt, Unterauftragsverarbeiter einzusetzen.

Sämtliche Unterauftragsverarbeiter werden vertraglich verpflichtet, mindestens die datenschutzrechtlichen Verpflichtungen dieses Vertrages einzuhalten.

Die jeweils aktuelle Liste der eingesetzten Unterauftragsverarbeiter wird dem Kunden in elektronischer Form zur Verfügung gestellt bzw. ist unter einer von Calmio bekanntgegebenen Internetadresse abrufbar. Änderungen werden dem Kunden gemäß § 8 dieses Vertrages mitgeteilt.

Über die beabsichtigte Hinzunahme oder den Austausch eines Unterauftragsverarbeiters wird der Kunde rechtzeitig informiert. Der Kunde kann aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Tagen nach Information Einwände gegen den Einsatz eines neuen Unterauftragsverarbeiters erheben. Können die Parteien keine einvernehmliche Lösung erzielen, steht beiden Parteien das Recht zur außerordentlichen Kündigung des Hauptvertrages hinsichtlich der betroffenen Leistungen zu.

Calmio bleibt gegenüber dem Kunden auch bei dem Einsatz von Unterauftragsverarbeitern für die Erfüllung der datenschutzrechtlichen Verpflichtungen aus diesem Vertrag verantwortlich.

§9 Datenschutzvorfälle

Calmio informiert den Kunden unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten, soweit diese die im Auftrag verarbeiteten personenbezogenen Daten betrifft.

Calmio stellt dem Kunden die zur Erfüllung gesetzlicher Melde- und Informationspflichten erforderlichen Informationen im angemessenen Umfang zur Verfügung. Die Mitteilung enthält, soweit verfügbar, Art und Umfang des Vorfalls, die betroffenen Datenkategorien, die voraussichtlichen Folgen sowie die bereits ergriffenen oder geplanten Abhilfemaßnahmen.

§10 Auditrechte

Der Kunde ist berechtigt, die Einhaltung der datenschutzrechtlichen Verpflichtungen dieses Vertrages nach angemessener Vorankündigung und während der üblichen Geschäftszeiten zu überprüfen oder durch einen zur Verschwiegenheit verpflichteten Dritten überprüfen zu lassen. Der Kunde wird bei der Durchführung des Audits auf die berechtigten Geschäfts- und Betriebsgeheimnisse von Calmio sowie auf die Vertraulichkeit gegenüber anderen Kunden angemessen Rücksicht nehmen.

Audits dürfen grundsätzlich höchstens einmal pro Kalenderjahr erfolgen, sofern kein konkreter Anlass für eine weitergehende Prüfung besteht.

Die Durchführung eines Audits darf den Geschäftsbetrieb von Calmio nicht unangemessen beeinträchtigen.

Soweit vorhanden, können geeignete Zertifizierungen, Testate oder Auditberichte als Nachweis der Einhaltung datenschutzrechtlicher Anforderungen herangezogen werden.

Der Kunde trägt die ihm durch das Audit entstehenden Kosten selbst. Soweit durch außergewöhnliche oder unverhältnismäßige Auditmaßnahmen erhebliche Aufwände bei Calmio entstehen, ist Calmio berechtigt, diese nach vorheriger Ankündigung angemessen in Rechnung zu stellen.

§11 Drittlandtransfer

Datenübertragungen außerhalb der EU erfolgen nur unter Einhaltung der DSGVO (z. B. Standardvertragsklauseln). Soweit personenbezogene Daten in Drittstaaten verarbeitet werden, stellt Calmio sicher, dass die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO eingehalten werden und geeignete Garantien, insbesondere Standardvertragsklauseln der Europäischen Kommission oder ein Angemessenheitsbeschluss, vorliegen.

§12 Löschung

Nach Beendigung des Hauptvertrages wird Calmio sämtliche personenbezogenen Daten nach Wahl des Kunden löschen oder zurückgeben, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Die Löschung erfolgt datenschutzgerecht und unter Berücksichtigung anerkannter technischer Standards.

Produktiv gespeicherte personenbezogene Daten werden grundsätzlich innerhalb von 30 Tagen gelöscht oder zurückgegeben.

Daten in Sicherungskopien (Backups) werden im Rahmen der regulären Backup-Zyklen überschrieben oder spätestens innerhalb von 180 Tagen gelöscht, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Soweit der Kunde vor Löschung keine Herausgabe der Daten verlangt, ist Calmio berechtigt, die personenbezogenen Daten entsprechend den gesetzlichen Vorgaben zu löschen.

§13 Unterstützungspflichten

Calmio unterstützt den Kunden bei:

- Betroffenenanfragen
- Datenschutzvorfällen
- behördlichen Anforderungen

Calmio unterstützt den Kunden darüber hinaus im angemessenen Umfang bei

- Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO,
- Konsultationen mit Datenschutzaufsichtsbehörden,
- Nachweisen gegenüber Aufsichtsbehörden,
- Nachweisen über die Umsetzung technischer und organisatorischer Maßnahmen,

soweit eine solche Unterstützung nach Art. 28 DSGVO gesetzlich erforderlich ist.

Calmio unterstützt den Kunden im Rahmen der gesetzlichen Anforderungen bei der Erfüllung der Rechte betroffener Personen nach Kapitel III DSGVO, soweit dies unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen möglich ist.

Auf Verlangen des Kunden stellt Calmio die im Auftrag verarbeiteten personenbezogenen Daten in einem gängigen maschinenlesbaren Format zur Verfügung, soweit dies technisch möglich und gesetzlich zulässig ist. Ein Anspruch auf Herausgabe proprietärer Softwarebestandteile, Algorithmen, Modelle oder Geschäftsgeheimnisse besteht nicht.

§14 Vertraulichkeit

Calmio stellt sicher, dass sämtliche mit der Verarbeitung personenbezogener Daten betrauten Personen auf Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Zugriff auf personenbezogene Daten erfolgt ausschließlich durch Personen, soweit dies zur Erfüllung ihrer jeweiligen Aufgaben erforderlich ist.

§15 Laufzeit

Dieser Auftragsverarbeitungsvertrag tritt mit Abschluss des Hauptvertrages in Kraft und endet automatisch mit dessen Beendigung, sofern nicht gesetzliche Aufbewahrungspflichten oder einzelne Bestimmungen dieses Vertrages eine darüber hinausgehende Geltung vorsehen.

Anlage 1 - Technische und Organisatorische Maßnahmen (TOMs)

Sicherheit ist uns wichtig.

Der Schutz personenbezogener Daten endet nicht bei Verträgen – er wird vor allem durch geeignete technische und organisatorische Maßnahmen umgesetzt. Diese Anlage beschreibt die wesentlichen Sicherheitsmaßnahmen, mit denen Calmio ein dem Risiko angemessenes Schutzniveau gemäß Art. 32 DSGVO sicherstellt.

Worum geht es in Kürze?

- Wir schützen personenbezogene Daten durch technische und organisatorische Sicherheitsmaßnahmen.
- Unsere Maßnahmen werden regelmäßig überprüft und an den Stand der Technik angepasst.
- Die beschriebenen Maßnahmen dienen dem Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit unserer Systeme und Prozesse.
- Da sich technische und organisatorische Sicherheitsmaßnahmen kontinuierlich weiterentwickeln, kann Calmio diese Maßnahmen fortlaufend verbessern, sofern das Datenschutzniveau hierdurch nicht abgesenkt wird.

Geltungsbereich

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen, die Calmio zum Zeitpunkt der Erstellung dieser Anlage umgesetzt hat. Die Maßnahmen orientieren sich an den Anforderungen des Art. 32 DSGVO und können unter Berücksichtigung des technischen Fortschritts sowie neuer Sicherheitsanforderungen angepasst oder weiterentwickelt werden, sofern hierdurch das Datenschutzniveau nicht abgesenkt wird.

1. Allgemeine Sicherheitsorganisation

Calmio verfolgt ein ganzheitliches Sicherheitskonzept, um personenbezogene Daten vor Verlust, Manipulation, unbefugtem Zugriff und sonstigen Sicherheitsrisiken zu schützen.

Hierzu gehören insbesondere:

- definierte Verantwortlichkeiten für Datenschutz und Informationssicherheit
- regelmäßige Überprüfung und Weiterentwicklung der Sicherheitsmaßnahmen
- dokumentierte interne Sicherheitsprozesse
- risikoorientierte Auswahl technischer und organisatorischer Maßnahmen
- Berücksichtigung gesetzlicher Anforderungen und des Stands der Technik

Sämtliche Sicherheitsmaßnahmen werden risikoorientiert ausgewählt und orientieren sich an Art, Umfang, Umständen und Zweck der Verarbeitung sowie den Eintrittswahrscheinlichkeiten und Schwere möglicher Risiken für die Rechte und Freiheiten betroffener Personen.

2. Vertraulichkeit

2.1 Zutrittskontrolle

Der physische Zutritt zu Systemen, auf denen personenbezogene Daten verarbeitet werden, ist gegen unbefugten Zugriff geschützt.

Calmio setzt hierzu insbesondere folgende Maßnahmen ein:

- [Hostinganbieter]
- [Rechenzentrumszertifizierungen (z. B. ISO 27001)]
- [physische Zutrittskontrollen]
- [Videoüberwachung]

sowie weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen.

2.2 Zugangskontrolle

Nur berechtigte Personen erhalten Zugriff auf IT-Systeme.

Calmio setzt hierzu insbesondere folgende Maßnahmen ein:

- individuelle Benutzerkonten
- starke Passwortrichtlinien
- Mehr-Faktor-Authentifizierung (soweit eingesetzt)
- automatische Sperrmechanismen

sowie weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen.

2.3 Zugriffskontrolle

Der Zugriff auf personenbezogene Daten erfolgt ausschließlich nach dem Need-to-know-Prinzip.

Calmio setzt hierzu insbesondere folgende Maßnahmen ein:

- rollenbasierte Berechtigungen

- Rechtevergabe nach Aufgabenbereich
- regelmäßige Überprüfung von Berechtigungen
- Protokollierung administrativer Zugriffe

sowie weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen.

2.4 Vertraulichkeitsverpflichtung

Alle Personen mit Zugriff auf personenbezogene Daten sind zur Vertraulichkeit verpflichtet.

Calmio setzt hierzu insbesondere folgende Maßnahmen ein:

- Verpflichtung auf Vertraulichkeit
- Datenschutzunterweisungen
- Berechtigungsentzug beim Ausscheiden

sowie weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen.

3. Integrität

3.1 Weitergabekontrolle

Personenbezogene Daten werden gegen unbefugte Kenntnisnahme während der Übertragung geschützt.

Calmio setzt hierzu insbesondere folgende Maßnahmen ein:

- TLS-verschlüsselte Kommunikation
- HTTPS
- verschlüsselte API-Kommunikation
- gesicherte Verbindungen zu Unterauftragsverarbeitern

sowie weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen.

3.2 Eingabekontrolle

Verarbeitungsvorgänge sollen nachvollziehbar sein.

Calmio setzt hierzu insbesondere folgende Maßnahmen ein:

- Protokollierung relevanter Änderungen
- Benutzerzuordnung
- Zeitstempel
- Audit-Logs

sowie weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen.

4. Verfügbarkeit und Belastbarkeit

Calmio trifft Maßnahmen, um Systeme und Daten dauerhaft verfügbar zu halten.

Calmio setzt hierzu insbesondere folgende Maßnahmen ein:

- Monitoring
- Backup-Konzept
- Redundanzen
- Schutz vor Datenverlust
- Notfallmanagement
- Schutz vor Schadsoftware
- DDoS-Schutz
- Kapazitätsüberwachung
- Notfallplanung

sowie weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen.

5. Wiederherstellbarkeit

Nach einem Sicherheitsvorfall oder technischen Ausfall soll eine Wiederherstellung innerhalb angemessener Zeit möglich sein.

Calmio setzt hierzu insbesondere folgende Maßnahmen ein:

- regelmäßige Datensicherungen
- getestete Wiederherstellungsverfahren
- definierte Aufbewahrungsfristen

sowie weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen.

Die Integrität und Vollständigkeit wiederhergestellter Daten wird im Rahmen der Wiederherstellungsverfahren überprüft.

Wiederherstellungsverfahren werden regelmäßig überprüft und bei Bedarf getestet.

6. Trennung der Verarbeitung

Personenbezogene Daten verschiedener Kunden werden logisch voneinander getrennt verarbeitet.

Calmio setzt hierzu insbesondere folgende Maßnahmen ein:

- Mandantentrennung
- getrennte Entwicklungs- und Produktivumgebungen
- Testdaten möglichst anonymisiert oder pseudonymisiert

sowie weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen.

7. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Calmio berücksichtigt Datenschutz bereits bei der Entwicklung sowie bei der Konfiguration der Plattform.

Calmio setzt hierzu insbesondere folgende Maßnahmen ein:

- Privacy by Design
- Privacy by Default
- Datenminimierung
- rollenbasierte Standardberechtigungen

sowie weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen.

8. Auftragskontrolle

Personenbezogene Daten werden ausschließlich entsprechend den Weisungen des Kunden verarbeitet.

Calmio setzt hierzu insbesondere folgende Maßnahmen ein:

- dokumentierte Weisungsprozesse
- vertragliche Verpflichtung von Mitarbeitenden
- AVV mit Unterauftragsverarbeitern
- regelmäßige Überprüfung der Dienstleister

sowie weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen.

9. Sicherheitsvorfälle und Incident Management

Calmio verfügt über Prozesse zur Erkennung, Bewertung und Behandlung von Sicherheitsvorfällen.

Calmio setzt hierzu insbesondere folgende Maßnahmen ein:

- Erkennung und Dokumentation von Sicherheitsvorfällen
- definierte Meldeprozesse
- Ursachenanalyse
- Maßnahmen zur Wiederherstellung
- Information betroffener Kunden gemäß AVV
- interne Eskalationsprozesse

sowie weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen.

10. Schwachstellen- und Änderungsmanagement

Zur Aufrechterhaltung eines angemessenen Sicherheitsniveaus werden Systeme regelmäßig überprüft und aktualisiert.

Calmio setzt hierzu insbesondere folgende Maßnahmen ein:

- Sicherheitsupdates
- Patchmanagement
- regelmäßige Wartung und Aktualisierung der Systeme
- Überprüfung eingesetzter Software

sowie weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen.

Sicherheitsupdates werden risikoorientiert und zeitnah eingespielt.

11. Regelmäßige Überprüfung

Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird regelmäßig überprüft und bei Bedarf angepasst.

Hierzu gehören insbesondere:

- regelmäßige interne Überprüfungen
- Bewertung neuer Risiken
- Anpassung an den Stand der Technik
- kontinuierliche Verbesserung der Sicherheitsmaßnahmen

12. Unterauftragsverarbeiter

Soweit Calmio Unterauftragsverarbeiter einsetzt, werden diese sorgfältig ausgewählt und vertraglich zur Einhaltung mindestens gleichwertiger Datenschutz- und Sicherheitsstandards verpflichtet.

Hierzu gehören insbesondere:

- Abschluss eines AVV
- Prüfung der Datenschutzstandards
- regelmäßige Bewertung
- Auswahl geeigneter Anbieter
- Kontrolle der Einhaltung gesetzlicher Anforderungen
- laufende Überwachung wesentlicher Unterauftragsverarbeiter

Die beschriebenen Maßnahmen stellen den aktuellen Stand zum Zeitpunkt der Erstellung dieser Anlage dar. Calmio überprüft die Wirksamkeit der Maßnahmen regelmäßig und entwickelt diese unter Berücksichtigung technischer, organisatorischer und gesetzlicher Anforderungen kontinuierlich weiter, sofern hierdurch das Datenschutzniveau nicht abgesenkt wird.