

AUFTRAGSVERARBEITUNGSVERTRAG

– Rahmenvertrag –
Stand: September 2026

zwischen der

Letizia GmbH

Rabinstr. 1

53111 Bonn

– nachfolgend „Auftragnehmer“ genannt –

und

Praxis

– nachfolgend „Auftraggeber“ genannt –

Präambel

Dieser Vertrag regelt als einheitlicher, modularer Rahmenvertrag die Auftragsverarbeitung personenbezogener Daten im Sinne von Art. 28 DSGVO zwischen dem Auftragnehmer und dem Auftraggeber. Er löst den bisherigen, auf den Rechnungsversand beschränkten Auftragsverarbeitungsvertrag „Übernahme Rechnungsversand“ (Stand 15.12.2024) vollständig ab, der hiermit gegenstandslos wird.

Der Auftragnehmer erbringt für den Auftraggeber verschiedene, in einem gesonderten Beratungsvertrag im Einzelnen beauftragte Leistungen. Dieser Rahmenvertrag deckt jeweils nur diejenigen der nachfolgenden Module ab, die der Auftraggeber tatsächlich gebucht hat und die in Anlage 0 (Modulübersicht) als gebucht gekennzeichnet sind. Module, die nicht gebucht sind, entfalten keine Wirkung; eine Verarbeitung außerhalb der gebuchten Module ist dem Auftragnehmer untersagt.

Folgende Module stehen zur Auswahl:

- Modul 1 – Finanz- und Verwaltungsmanagement
- Modul 2 – Personalverwaltung und Recruiting
- Modul 3 – Privatabrechnung (ohne Forderungsmanagement)
- Modul 4 – Marketing und Leadmanagement
- Modul 5 – KI-gestützte Verarbeitung

Die allgemeinen Bestimmungen dieses Vertrags (§§ 1 bis 9) gelten für sämtliche gebuchten Module einheitlich. Die modulspezifischen Regelungen zu Gegenstand, Zweck, Datenkategorien, Betroffenenkategorien und Löschfristen der Verarbeitung ergeben sich aus Anlage 0.

§ 1 Gegenstand und Umfang der Verarbeitung

Der Auftraggeber beauftragt den Auftragnehmer im Rahmen der jeweils gebuchten Module (Anlage 0) mit der Verarbeitung personenbezogener Daten nach Maßgabe dieses Vertrages. Der Dienstleistungsumfang im Übrigen ist in einem separaten Beratungsvertrag geregelt.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Eine Übermittlung personenbezogener Daten in Drittländer außerhalb der EU/des EWR findet nach gegenwärtigem Stand der eingesetzten Auftragsverarbeiter und Werkzeuge (Anlage 3) nicht statt.

Durch die Erbringung der Dienstleistung erhält der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend „Auftraggeberdaten“ genannt). Gegenstand, Art und Zweck der Verarbeitung sowie die Kategorien betroffener Personen und die Kategorien verarbeiteter Daten ergeben sich im Einzelnen je Modul aus Anlage 0.

Dem Auftragnehmer ist jede abweichende oder über die Festlegungen dieses Vertrags und der Anlage 0 hinausgehende Verarbeitung untersagt. Dies gilt auch für die Verwendung anonymisierter Daten.

Modul 1 – Finanz- und Verwaltungsmanagement

Der Auftragnehmer übernimmt im Rahmen dieses Moduls folgende Tätigkeiten:

- Bearbeitung von Lieferantenrechnungen, die über ein zentrales E-Mail-Postfach eingehen; Vertragspartner dieses Postfachs ist die Praxis, die eine Weiterleitung an den Auftragnehmer einrichtet, sodass dieser eine Kopie der Rechnungen erhält.
- Ablage und Verwaltung von Belegen und Unterlagen über die Dokumentenmanagement-Software ELO.
- Einsatz von GetMyInvoices zur Belegverarbeitung; Vertragspartner von GetMyInvoices ist ausschließlich der Auftragnehmer.
- Erstellung und Bearbeitung von Überweisungsdateien sowie Belegtransfer.
- Unterstützende Auswertungstätigkeiten auf Grundlage des direkten Zugriffs des Auftragnehmers auf DATEV Unternehmen online; eine darüberhinausgehende BWA-Erstellung mit Zugriff auf weitere steuerlich relevante Daten wird durch den Auftragnehmer nicht angeboten und bleibt unberührte Aufgabe des Steuerberaters der Praxis.
- Vertrags- und Fristenmanagement.
- Liquiditätsauswertungen.

Betroffene Personen sind Patienten, Vertragspartner und Beschäftigte des Auftraggebers, soweit deren Daten im Rahmen der vorgenannten Tätigkeiten verarbeitet werden. Verarbeitete Datenkategorien sind insbesondere Rechnungs-, Zahlungs-, Vertrags- und Kontodaten.

Für die im Rahmen dieses Moduls verarbeiteten Daten gelten die in Anlage 1 der AGB der Letizia GmbH (Stand September 2026) bereits festgelegten Löschfristen entsprechend; eigenständige Löschfristen werden im Rahmen dieses Moduls nicht gesondert definiert.

Modul 2 – Personalverwaltung und Recruiting

Der Auftragnehmer übernimmt im Rahmen dieses Moduls folgende Tätigkeiten:

- Führung digitaler Personalakten.
- Bearbeitung von Arbeitsverträgen und Ausbildungsverträgen.
- Verarbeitung von Gehalts- und Arbeitszeitdaten sowie Personalkostendaten.
- Bewerbermanagement einschließlich Vorauswahl; die hierfür eingesetzten Systeme sind ELO und E-Mail, jeweils mit dem Auftragnehmer als Vertragspartner.

Eine Übermittlung von Personaldaten an externe Steuerberater oder Kammern im Namen des Auftraggebers durch den Auftragnehmer ist nicht Gegenstand dieses Moduls und findet im Rahmen dieses Vertrages nicht statt.

Der Auftraggeber bleibt für die Zulässigkeit der Verarbeitung von Personal- und Bewerberdaten nach § 26 BDSG verantwortlich. Dieser Vertrag stellt hierfür keine eigene Rechtsgrundlage dar.

Bewerberdaten werden abweichend von den sonstigen Löschfristen dieses Vertrages spätestens sechs Monate nach Abschluss des jeweiligen Bewerbungsverfahrens gelöscht. Eine Ausnahme hiervon (etwa im Rahmen eines Talentpools oder einer verlängerten Aufbewahrung mit gesonderter Einwilligung der betroffenen Person) besteht nicht.

Modul 3 – Privatabrechnung (ohne Forderungsmanagement)

Der Auftragnehmer übernimmt im Rahmen dieses Moduls folgende Tätigkeiten:

- Erstellung der privatärztlichen Rechnung (GOÄ-Rechnung) im Auftrag der Praxis, auf deren Geschäftspapier und über deren Konto.
- Verarbeitung dokumentierter Befunde, soweit diese Bestandteil der jeweiligen GOÄ-Rechnung sind; eine gesonderte, über die Rechnung hinausgehende Dokumentation von Befunden erfolgt durch den Auftragnehmer nicht.
- Zahlungsüberwachung, Mahnwesen und Verwaltung von Ratenzahlungen.
- Adressermittlung bei Zahlungsverzug.

Ausdrücklich nicht Gegenstand dieses Moduls und dieses Vertrages ist das Forderungsmanagement im engeren Sinne, insbesondere die Beauftragung externer Inkassodienstleister sowie die Durchführung eines gerichtlichen Mahn- oder Vollstreckungsverfahrens. Diese Tätigkeiten werden – soweit gewünscht – von der Praxis selbst oder durch von ihr gesondert beauftragte Dritte veranlasst und liegen außerhalb dieses Vertrages. Klarstellend gilt: Der Auftragnehmer erwirbt keine Forderungen der Praxis gegen deren Patienten; die Rechnungsstellung erfolgt ausschließlich im Auftrag und für Rechnung der Praxis.

Da die im Rahmen dieses Moduls verarbeiteten dokumentierten Befunde besonders sensible Gesundheitsdaten im Sinne von Art. 9 DSGVO darstellen, weist der Auftragnehmer besonders auf die allgemeinen technisch-organisatorischen Maßnahmen gemäß Anlage 2 sowie die Verschwiegenheitsverpflichtung nach § 203 StGB gemäß § 4 dieses Vertrages hin; gesonderte, über Anlage 2 hinausgehende Maßnahmen werden für dieses Modul nicht vereinbart.

Da dokumentierte Befunde beim Auftragnehmer nicht separat, sondern ausschließlich als Bestandteil der Privatrechnungen verarbeitet werden, gelten für sie dieselben Löschfristen wie für die übrigen im Rahmen dieses Moduls verarbeiteten Abrechnungsdaten (Verweis auf Anlage 1 der AGB der Letizia GmbH, Stand September 2026); ein gesondertes, längeres Fristenregime (etwa entsprechend § 630f BGB) wird nicht vereinbart.

Externe Dienstleister, die zur Adressermittlung bei Zahlungsverzug eingesetzt werden könnten (z. B. Melderegisterauskünfte), sind nicht Gegenstand dieses Vertrages und werden nicht als Unterauftragsverarbeiter aufgenommen.

Modul 4 – Marketing und Leadmanagement

Der Auftragnehmer erstellt Vorschläge für Marketing-Aktivitäten, die dem Auftraggeber jeweils zur Freigabe vorgelegt werden; nur vom Auftraggeber freigegebene Inhalte werden veröffentlicht. Im Einzelnen:

- Landingpages: Der Auftraggeber entscheidet über Inhalt, Gestaltung und Zielgruppenansprache; der Auftragnehmer setzt die Vorgaben lediglich technisch um.
- Patienten- und Bewerberanfragen: Eingehende Formularanfragen werden vom Auftragnehmer lediglich im Auftrag des Auftraggebers entgegengenommen und an diesen weitergeleitet.
- Kampagnenauswertung: Der Auftragnehmer wertet die Kampagnendaten ausschließlich für die einzelne Praxis aus; eine praxisübergreifende Nutzung findet nicht statt.

Bewertungsmanagement und Social-Media-Betreuung werden vom Auftragnehmer nicht übernommen und sind nicht Gegenstand dieses Moduls.

Zur Umsetzung setzt der Auftragnehmer folgende Werkzeuge ein, bei denen jeweils der Auftragnehmer Vertragspartner ist: das CRM-/Marketing-Tool ActiveCampaign, die Landingpage-Plattform Onepage sowie das Video-Tool Skool. Weitere Marketing-Tools werden derzeit nicht eingesetzt.

Datenübermittlungen in Drittländer außerhalb der EU/des EWR finden bei den eingesetzten Tools nach gegenwärtigem Stand nicht statt; sollte sich dies ändern, gilt § 6 dieses Vertrages entsprechend.

Modul 5 – KI-gestützte Verarbeitung

Der Auftragnehmer setzt im Rahmen dieses Moduls KI-gestützte Werkzeuge ausschließlich für folgende Anwendungsfälle ein: Dokumentenaufbereitung, Protokollerstellung, Erstellung von Standardtexten sowie Auswertungen. Eine darüberhinausgehende Nutzung ist nicht Gegenstand dieses Moduls.

Als KI-Plattform wird Ollama eingesetzt, die den Betrieb eines Sprachmodells (aktuell: Mistral) vollständig auf einem eigenen, im Auftrag des Auftragnehmers betriebenen Server ermöglicht (Self-Hosting). Eine Trainingsnutzung der eingegebenen Praxisdaten zur Weiterentwicklung der KI-Modelle durch Dritte ist vertraglich ausgeschlossen.

Da Betrieb und Verarbeitung vollständig selbst gehostet erfolgen, findet keine Datenübermittlung in Drittländer außerhalb der EU/des EWR statt; Standardvertragsklauseln oder andere Garantien nach Art. 44 ff. DSGVO sind daher nicht erforderlich.

§ 2 Laufzeit

Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des separaten Beratungsvertrags; sie ist mithin täglich kündbar. Die Kündigung eines einzelnen Moduls ist im gleichen Umfang möglich, wie das zugrundeliegende Leistungsmodul im Beratungsvertrag gekündigt werden kann; im Übrigen bleibt dieser Rahmenvertrag für die verbleibenden gebuchten Module bestehen.

§ 3 Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet die Auftraggeberdaten nur im Rahmen der jeweils gebuchten Module und ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 28 DSGVO (Auftragsverarbeitung); dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Der Auftraggeber hat insoweit das alleinige Recht, Weisungen über Art, Umfang und Methode der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch „Weisungsrecht“).

Weisungen werden vom Auftraggeber grundsätzlich schriftlich erteilt. Die weisungs- und empfangsberechtigten Personen ergeben sich aus Anlage 1. Bei einem Wechsel oder einer längerfristigen Verhinderung der in Anlage 1 benannten Personen ist der anderen Partei unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten durch den Auftragnehmer, Mitarbeiter oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich, in der Regel innerhalb von 48 Stunden nach Kenntniserlangung, informieren, damit der Auftraggeber seinerseits die Frist des Art. 33 Abs. 1 DSGVO gegenüber der zuständigen Aufsichtsbehörde einhalten kann. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutzaufsichtsbehörde. Die Meldungen enthalten jeweils zumindest die in Art. 33 Abs. 3 DSGVO genannten Angaben.

Der Auftragnehmer wird den Auftraggeber im Falle des vorstehenden Absatzes bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen im Rahmen des Zumutbaren unterstützen. Der Auftragnehmer wird insbesondere unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen durchführen, den Auftraggeber hierüber informieren und diesen um weitere Weisungen ersuchen.

Sollten die Auftraggeberdaten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat 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 DSGVO liegt.

§ 4 Technische und organisatorische Maßnahmen; Vertraulichkeit

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Der Auftragnehmer wird insbesondere die in Anlage 2 dargestellten Maßnahmen ergreifen und für die Dauer dieses Vertrages aufrechterhalten.

Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (nachfolgend „Mitarbeiter“ genannt), in Schriftform zur Vertraulichkeit verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und die Einhaltung dieser Verpflichtung mit der gebotenen Sorgfalt sicherstellen.

Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Dokumentationen sind für die Dauer dieses Vertrages aufzubewahren.

Der Auftragnehmer verpflichtet sich sowie seine Mitarbeitenden und die von ihm nach § 6 eingesetzten Unterauftragsverarbeiter und mitwirkenden Dienstleister ausdrücklich zur Geheimhaltung nach § 203 StGB, soweit diese im Rahmen der Vertragsdurchführung Kenntnis von Patientengeheimnissen erlangen. Der Auftraggeber begrenzt seinerseits den Zugriff des Auftragnehmers auf das für die jeweiligen Module Erforderliche.

§ 5 Kontrollrechte

Der Auftraggeber ist nach angemessener Vorankündigung – in der Regel zwei Wochen – berechtigt, sich von der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen gemäß § 4 dieser Vereinbarung, zu überzeugen. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers prüfen.

Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen. Die üblichen Geschäftszeiten sind zu beachten und Störungen im Betriebsablauf des Auftragnehmers zu vermeiden. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig.

Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

Die Prüfungen dürfen auch durch einen von dem Auftraggeber beauftragten Dritten, der von Berufs wegen oder gemäß wirksamer Vereinbarung zur Verschwiegenheit verpflichtet ist, durchgeführt werden, sofern dieser Dritte nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

§ 6 Unterauftragsverarbeitung

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, Bewachungsdienste, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

Im Übrigen erteilt der Auftraggeber dem Auftragnehmer mit Abschluss dieses Vertrages die allgemeine schriftliche Genehmigung zur Beauftragung der in Anlage 3 aufgeführten, aktuell eingesetzten Unterauftragsverarbeiter. Der Auftragnehmer legt den Unterauftragsverarbeitern im Wesentlichen dieselben Datenschutzpflichten auf, die ihm nach diesem Vertrag obliegen.

Beabsichtigt der Auftragnehmer, weitere Unterauftragsverarbeiter zu beauftragen oder einen bestehenden Unterauftragsverarbeiter auszuwechseln, informiert er den Auftraggeber hierüber vorab in Textform mit angemessener Frist. Widerspricht der Auftraggeber der beabsichtigten Änderung nicht innerhalb dieser Frist, gilt die Änderung als genehmigt (Opt-out-Verfahren). Widerspricht der Auftraggeber form- und fristgerecht, wird der betreffende Unterauftragsverarbeiter für die Verarbeitung von Auftraggeberdaten nicht eingesetzt; die Parteien stimmen sich in diesem Fall über das weitere Vorgehen ab.

§ 7 Löschung und Rückgabe personenbezogener Daten

Der Auftragnehmer wird dem Auftraggeber nach Beendigung dieses Vertrages oder jederzeit auf dessen Verlangen alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers, sofern nicht eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich löschen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen. Solche Dokumentationen sind vom Auftragnehmer für eine Dauer von drei Jahren aufzubewahren. Der Auftragnehmer kann die Dokumentation dem Auftraggeber aushändigen, um sich von den diesbezüglichen Pflichten zu befreien.

Im Übrigen gelten für die Löschung der im Rahmen der einzelnen Module verarbeiteten Daten die in § 1 dieses Vertrages sowie die in Anlage 1 der AGB der Letizia GmbH (Stand September 2026) genannten Fristen entsprechend.

Der Auftragnehmer wird dem Auftraggeber die Löschung schriftlich bestätigen.

§ 8 Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Die Haftung des Auftragnehmers ist der Höhe nach auf die Deckungssumme seiner Berufshaftpflichtversicherung begrenzt, die 5.000.000 EUR je Schadensfall und 10.000.000 EUR für sämtliche Schadensfälle eines Versicherungsjahres beträgt; dies entspricht der in § 3 der AGB der Letizia GmbH (Stand September 2026) genannten Haftungshöchstsumme. Die verschuldensunabhängige Haftung nach Art. 82 DSGVO gegenüber betroffenen Personen bleibt hiervon unberührt.

§ 9 Schlussbestimmungen

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

Wenn Bestimmungen dieses Vertrages ganz oder teilweise nicht wirksam und/oder nicht durchführbar sind, wird dadurch die Gültigkeit der anderen Bestimmungen nicht berührt. Das Gleiche gilt, wenn dieser Vertrag eine Regelungslücke enthält. Die Vertragsparteien sind im Falle einer unwirksamen oder undurchführbaren Bestimmung verpflichtet, über eine wirksame und zumutbare Ersatzregelung zu verhandeln, die der unwirksamen bzw. undurchführbaren Bestimmung bei wirtschaftlicher Betrachtungsweise am besten entspricht. Entsprechendes gilt im Falle einer Regelungslücke.

Mündliche Nebenabreden bestehen nicht. Änderungen und Ergänzungen bedürfen der Schriftform. Dies gilt auch für eine Vereinbarung, die das Schriftformerfordernis aufhebt.

Es gilt das Recht der Bundesrepublik Deutschland.

Dieser Auftragsverarbeitungsvertrag ergänzt die AGB der Letizia GmbH (Stand September 2026), insbesondere § 6 sowie Anlage 1 der AGB. Im Falle von Widersprüchen zwischen diesem Vertrag und den AGB geht dieser Vertrag als spezielleres Regelwerk für die Auftragsverarbeitung vor.

Ort, Datum	Unterschrift Praxisinhaber:in 1
------------	---------------------------------

Ort, Datum	Unterschrift Praxisinhaber:in 2
------------	---------------------------------

Ort, Datum	Unterschrift Praxisinhaber:in 3
------------	---------------------------------

Ort, Datum	Unterschrift Praxisinhaber:in 4
------------	---------------------------------

Ort, Datum	Unterschrift Letizia GmbH
------------	---------------------------

Anlage 0 – Modulübersicht

Für den Auftraggeber sind folgende Module dieses Rahmenvertrags gebucht (zutreffendes bitte kennzeichnen):

Modul	Gebucht (ja/nein)
Modul 1 – Finanz- und Verwaltungsmanagement	
Modul 2 – Personalverwaltung und Recruiting	
Modul 3 – Privatabrechnung (ohne Forderungsmanagement)	
Modul 4 – Marketing und Leadmanagement	
Modul 5 – KI-gestützte Verarbeitung	

Gegenstand, Art und Zweck der Verarbeitung, die Kategorien betroffener Personen sowie die Kategorien verarbeiteter Daten je Modul ergeben sich aus § 1 dieses Vertrages.

Anlage 1 – Weisungs- und empfangsberechtigte Personen

Auftraggeber: [Name und Anschrift der Praxis]

Auftragnehmer: Letizia GmbH, Rabinstr. 1, 53111 Bonn

- Herr Cono Letizia
- Frau Céline Oreiller
- Frau Sandra Ullrich

Anlage 2 – Technisch-organisatorische Maßnahmen

Vertraulichkeit

Die nachfolgenden Regelungen, die sich insbesondere auf räumliche Maßnahmen beziehen, gelten nicht für Maßnahmen im Homeoffice. Sofern in evtl. genutzten Heimbüros spezielle Räumlichkeiten gelten, sind diese explizit aufgeführt.

Zutrittskontrolle:

Das Gelände/Gebäude ist außen gut beleuchtet. Die Geschäftsräume befinden sich im 3. Obergeschoss. Bewegungsmelder lösen einen Alarm aus, wenn sich Personen außerhalb der Geschäftszeiten in den Räumen bewegen. Die Funktion der Alarmanlage wird regelmäßig überprüft. Besucher und Lieferanten müssen sich anmelden und werden abgeholt und begleitet. Die Ausgabe von Codekarten wird schriftlich dokumentiert. Die Server sind extern in einem Rechenzentrum stationiert.

Zugangskontrolle:

Die jeweiligen Personen haben ein Zutrittsrecht zum Gebäude/Büro und können sich somit den Computern/Akten nähern. Der Zugang zu den eigentlichen Daten wird gleichwohl verwehrt bzw. eingeschränkt, sodass unbefugte Nutzung verhindert wird. Auch im Homeoffice stellen die dort tätigen Mitarbeiter eine Zugangskontrolle sicher.

Bei ausnahmslos allen Computern (auch in Heimarbeit) ist die Auswahl eines Benutzerkontos und die Angabe eines Passworts notwendig, um das Betriebssystem zu starten. Jeder Benutzer muss sich individuell mit seinem Benutzernamen anmelden. Die Mindestlänge des Passworts beträgt 8 Zeichen. Die Mitarbeiter sind angewiesen, Passwörter vertraulich zu halten und nicht ohne wichtigen Grund an Kollegen weiterzugeben. Wichtige Gründe sind hier Urlaubs- und Krankheitsvertretung.

Zugriffskontrolle:

Der Zugang kann nur über ein Zugangskontrollsystem erfolgen. Technische Absicherungen erfolgen über Firewalls.

Trennung:

Die Daten verschiedener Mandanten/Kunden werden in eigenen Verzeichnissen gespeichert. Die Zugriffsrechte werden entsprechend vergeben, sodass eine selektive Sicherung bzw. Löschung pro Mandant möglich ist.

Integrität

Eingabekontrolle:

Eine Eingabekontrolle ist in einigen Programmen möglich (der eingesetzte SQL-Server prüft die Datenintegrität automatisch).

Weitergabekontrolle:

Sensible Dateianhänge werden über die Enterprise-Content-Management-Unternehmenssoftware der Firma ELO Digital Office mit einer 256-Bit-Verschlüsselung versendet. Der Zugriff auf die Software wird mit einem Passwort geschützt.

Verfügbarkeit und Belastbarkeit

Es soll gewährleistet sein, dass Daten erhalten bleiben, damit den betroffenen Personen kein Nachteil erwächst. Mögliche Ursachen für einen Datenverlust sind u. a. Wasser, Hitze, Hardware-Ausfall, Fehlbedienung oder Stromausfall.

Die M2soft GmbH stellt die IT-Infrastruktur in einem Rechenzentrum zur Verfügung.

Datensicherung:

Es werden die letzten 5 Backups vorgehalten, danach wird das älteste Backup wieder mit einem aktuellen überschrieben.

- Virtuelle Server 1: Montag – Freitag, Imagesicherung
- Virtuelle Server 2: Montag – Freitag, Imagesicherung
- Virtuelle Server 3: Montag – Freitag, Imagesicherung
- Virtuelle Server 4: 1 x monatlich, Imagesicherung
- Virtuelle Server 5: 1 x monatlich, Imagesicherung

Wartungsarbeiten Rechenzentrum:

Wartungen werden außerhalb der normalen Arbeitszeiten (8:00 – 18:00 Uhr) durchgeführt. Sicherheitsrelevante Wartungen, welche die Sicherheit des Rechenzentrums betreffen, werden sofort durchgeführt und können dementsprechend nicht angemeldet werden. Das Rechenzentrum ist gehalten, das Zeitfenster solcher Wartungen klein zu halten.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Es ist ein Datenschutz-Management-System implementiert. Ein externer Datenschutzbeauftragter ist bestellt und überwacht die Einhaltung der gesetzlichen Pflichten. Eine Übersicht über die Verarbeitungstätigkeiten liegt vor. Vereinbarungen über Auftragsverarbeitungen werden gemäß den gesetzlichen Anforderungen abgeschlossen und regelmäßig kontrolliert. Alle zum Datenschutz implementierten Prozesse werden regelmäßig überprüft und Abläufe ggf. verbessert.

Anlage 3 – Unterauftragnehmerliste

Der Auftragnehmer setzt zum Zeitpunkt des Vertragsschlusses folgende Unterauftragsverarbeiter ein. Änderungen richten sich nach dem in § 6 dieses Vertrages beschriebenen Opt-out-Verfahren.

Unterauftragsverarbeiter	Leistung	Betroffene Module
ecm.online GmbH	Hosting, Support und Fernwartung der Dokumentenmanagement-Software ELO	Module 1–3
GetMyInvoices	Digitale Belegverarbeitung	Modul 1
M2soft GmbH	Rechenzentrum / Server- und Backup-Infrastruktur	Alle Module
Microsoft 365	Zentrales E-Mail-Postfach	Alle Module
Ollama / Mistral	Self-gehostete KI-Plattform und Sprachmodell	Modul 5

ActiveCampaign	CRM- und Marketing-Automation	Modul 4
Deutsche Post AG / Deutsche Post E-POST Solutions GmbH (E-POST Mailer)	Druck und Versand	Modul 1, Modul 3

Freie Mitarbeitende oder externe Teams mit eigenständigem Zugriff auf Auftraggeberdaten werden vom Auftragnehmer nicht eingesetzt.

Hinsichtlich des Versands über die Deutsche Post AG und die Deutsche Post E-POST Solutions GmbH (E-POST Mailer) gelten ergänzend die jeweils aktuellen AGB dieser Anbieter.