

Zusatzvereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen Auftragnehmer

PRAXINO GmbH

Marienstraße 10, 70178 Stuttgart (PRAXINO)

und

dem Auftraggeber/Kunden

1. Gegenstand und Dauer des Auftrags

Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten des Kunden durch PRAXINO im Zusammenhang mit der Bereitstellung der Software „Optica Viva“ (im Folgenden: Software) im Rahmen einer sogenannten „Software-as-a-service“-Lösung (SaaS) in dessen Auftrag und nach dessen Weisung. PRAXINO gewährt dem Kunden den Einsatz der Software auf der Grundlage eines Software-Nutzungsvertrag (im Folgenden: Hauptvertrag).

Diese Vereinbarung konkretisiert insoweit die datenschutzrechtlichen Verpflichtungen der Vertragsparteien im Hinblick auf sämtliche Tätigkeiten, die mit der Leistungserbringung im Zusammenhang stehen und bei denen Mitarbeiter von PRAXINO oder durch PRAXINO beauftragte Dritte mit personenbezogenen Daten des Kunden in Berührung kommen können.

Die im Hauptvertrag vereinbarten Leistungen von PRAXINO beschränken sich auf die Bereitstellung der Software auf einem zentralen Computersystem zur Nutzung durch den Kunden via Internet als SaaS-Lösung, die Gewährung des Zugriffs auf diese Software für den Kunden, die Wartung der Software sowie Supportleistungen. Im Rahmen der Leistungserbringung ist ein Zugriff auf Daten des Kunden grundsätzlich nicht vorgesehen; es ist jedoch nicht auszuschließen, dass PRAXINO zur Erfüllung ihrer vertraglichen Leistungen die Möglichkeit des Zugriffs auf personenbezogene Daten, die der Kunde über die Software verarbeitet, erhält. Insofern finden die nachfolgenden Bestimmungen entsprechend Anwendung.

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben. Eine Kündigung des Hauptvertrages bewirkt automatisch auch eine Kündigung dieser Vereinbarung. Eine isolierte Kündigung dieser Vereinbarung ist ausgeschlossen.

Zusatzvereinbarung zur Auftragsvereinbarung gemäß Art. 28 DSGVO

2. Konkretisierung des Auftragsinhalts

2.1 Art der Daten und Kreis der Betroffenen

Zur Erbringung ihrer Leistungen nach den Vorgaben des Hauptvertrages verarbeitet PRAXINO folgende personenbezogene Daten des Kunden:

KATEGORIEN BETROFFENER PERSONEN	ART DER DATEN
Kunde	Personenstammdaten, Kommunikationsdaten (Telefonnummer, E-Mail-Adresse etc.), Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse), Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Planungs- und Steuerungsdaten
Beschäftigte des Kunden	Name, Geburtsdatum, Kommunikationsdaten, Abteilungsinformationen, Arbeitszeiten, Abwesenheitszeiten-/arten
Patienten des Kunden	E-Mail-Adresse, Rufnummer

2.2 Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten

Umfang, Art und Zweck der Verarbeitung der Daten nach Ziff. 2.1 durch PRAXINO sind im Hauptvertrag konkret beschrieben. Die Daten werden grundsätzlich im Rahmen der Nutzung der Software durch den Kunden selbst eingegeben, berichtet, gelöscht und in der Verarbeitung eingeschränkt.

2.3 Ort der Leistungserbringung

Die Verarbeitung der Daten findet in einem Mitgliedsstaat der Europäischen Union, in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder unter Beachtung der besonderen gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO in einem Drittland statt.

3. Weisungsbefugnisse des Kunden

PRAXINO verarbeitet die Daten ausschließlich in Übereinstimmung mit den Weisungen des Kunden hinsichtlich Art, Umfang und Verfahren der Datenverarbeitung, wie sie in dieser Vereinbarung geregelt sind. Konkretisierende Einzelweisungen des Kunden sind im Rahmen der im Hauptvertrag getroffenen Auftragsbeschreibung und nach Maßgabe der nachfolgenden Regelungen zulässig.

Einzelweisungen des Kunden, die von dem im Hauptvertrag geregelten Leistungsumfang abweichen und zusätzliche Anforderungen stellen, werden als Antrag auf Leistungsänderung behandelt. Soweit die Ausführung der Weisung nicht durch das im Hauptvertrag vereinbarte Entgelt abgedeckt ist, besteht ein Anspruch des Kunden auf Durchführung der Weisung erst nach Zusicherung des Kunden, PRAXINO den Mehraufwand für die Durchführung seiner Weisung zu erstatten. Mündliche Weisungen wird der Kunde unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

PRAXINO unterrichtet den Kunden unverzüglich, wenn sie der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche oder sonst einschlägige gesetzliche Vorgaben. PRAXINO ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Kunden bestätigt oder geändert wird.

Zusatzvereinbarung zur Auftragsvereinbarung gemäß Art. 28 DSGVO

Weisungen, die auf eine strafbare Handlung gerichtet sind oder PRAXINO dem Betroffenen oder einem Dritten gegenüber schadenersatzpflichtig machen würden, hat PRAXINO nicht Folge zu leisten.

4. Technische und organisatorische Maßnahmen

PRAXINO wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. PRAXINO wird gemäß Art. 28 Abs. 3 lit. c und Art. 32 DSGVO technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Kunden treffen, die den einschlägigen gesetzlichen Anforderungen genügen. PRAXINO hat Maßnahmen zu treffen, welche die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung dauerhaft sicherstellen. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 DSGVO zu berücksichtigen.

Eine konkrete Darstellung der vom Kunden als hinreichend akzeptierten technischen und organisatorischen Maßnahmen enthält der Anhang 1 zu dieser Vereinbarung.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. PRAXINO ist berechtigt, alternative adäquate Maßnahmen umzusetzen, sofern sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

5. Berichtigung, Einschränkung und Löschung von Daten

Soweit dies nicht Bestandteil des Auftrags ist, hat PRAXINO personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden, nur nach dokumentierter Weisung des Kunden zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken. Wendet sich ein Betroffener mit der Forderung nach Berichtigung, Löschung, Einschränkung der Verarbeitung oder Auskunft unmittelbar an PRAXINO, wird PRAXINO den Betroffenen an den Kunden verweisen, sofern eine Zuordnung an den Kunden nach den Angaben des Betroffenen möglich ist. PRAXINO leitet hierzu den Antrag des Betroffenen unverzüglich an den Kunden weiter und wird diesen auf Weisung im Rahmen ihrer Möglichkeiten unterstützen. PRAXINO haftet nicht, wenn das Ersuchen des Betroffenen vom Kunden nicht, nicht richtig oder nicht fristgerecht beantwortet wird. Die Umsetzung des Löschkonzepts des Kunden sowie der Betroffenenrechte auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft ist nur insoweit durch PRAXINO unmittelbar sicherzustellen, als dies vom vertraglich vereinbarten Leistungsumfang umfasst ist.

6. Weitere Pflichten von PRAXINO

- PRAXINO verarbeitet die über die Software gespeicherten Daten – vorbehaltlich abweichender Vereinbarungen – nur im Rahmen des Auftrages und der dokumentierten Weisungen des Kunden, es sei denn, das Recht der Europäischen Union oder der Bundesrepublik Deutschland verpflichtet PRAXINO hierzu. Kopien werden ohne Wissen des Kunden nicht erstellt. Hiervon ausgenommen sind Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die zur Einhaltung vertraglicher, gesetzlicher oder satzungsmäßiger Aufbewahrungspflichten erforderlich sind.



Zusatzvereinbarung zur Auftragsvereinbarung gemäß Art. 28 DSGVO

- PRAXINO wird bei der Erbringung ihrer Leistungen nur Mitarbeiter oder andere für PRAXINO tätige Personen einsetzen, die auf die Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b DSGVO sowie – sofern einschlägig – das Sozialgeheimnis verpflichtet wurden oder einer angemessenen gesetzlichen Vertraulichkeit unterliegen und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Vertraulichkeitspflicht besteht auch nach Beendigung der Vereinbarung fort. PRAXINO gewährleistet, dass es den mit der Verarbeitung der Daten des Kunden befassten Mitarbeitern und anderen für PRAXINO tätigen Personen untersagt ist, die Daten außerhalb der Weisungen des Kunden zu verarbeiten. Gesetzliche Offenbarungspflichten von PRAXINO bleiben unberührt.
- PRAXINO verpflichtet sich, ihren gesetzlichen Kontrollpflichten nachzukommen. PRAXINO wird insbesondere regelmäßig kontrollieren, ob die Verarbeitung der personenbezogenen Daten des Kunden in Übereinstimmung mit den vertraglichen Vereinbarungen und den Weisungen des Kunden erfolgt sowie ob die Einhaltung, Nachweisbarkeit und Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sichergestellt ist.
- PRAXINO unterstützt den Kunden im Rahmen ihrer Möglichkeiten bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen sowie unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten des Kunden nach Art. 32 bis 36 DSGVO. Hierzu zählen
 - die Sicherstellung des vereinbarten Schutzniveaus durch technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,
 - die Meldepflicht bei Datenschutzverletzungen gemäß Art. 33 DSGVO, soweit diese im Zusammenhang mit der Erfüllung dieser Vereinbarung geschehen,
 - die Verpflichtung, den Kunden im Rahmen seiner Informationspflicht gegenüber den von einer Datenschutzverletzung Betroffenen gemäß Art. 34 DSGVO zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen,
 - die Unterstützung des Kunden bei dessen Datenschutz-Folgeabschätzung gemäß Art. 35 DSGVO sowie im Rahmen vorheriger Konsultationen gemäß Art. 36 DSGVO.

Für vorstehende Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Hauptvertrages enthalten oder auf ein Fehlverhalten von PRAXINO zurückzuführen sind, kann PRAXINO eine angemessene Vergütung verlangen.

- PRAXINO wird den Kunden unverzüglich über Kontrollhandlungen und Maßnahmen der Datenschutzaufsichtsbehörden informieren, sofern diese Handlungen und Maßnahmen die Verarbeitung von personenbezogenen Daten des Kunden durch PRAXINO zum Gegenstand haben.

Zusatzvereinbarung zur Auftragsvereinbarung gemäß Art. 28 DSGVO

7. Pflichten des Kunden

Für die Einhaltung der einschlägigen datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an PRAXINO, die Rechtmäßigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen im Rahmen dieser Vereinbarung ist allein der Kunde verantwortlich („Verantwortlicher“ im Sinne von Art. 4 Nr. 7 DSGVO). Der Kunde wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen geschaffen werden, damit PRAXINO die vereinbarten Leistungen rechtmäßig erbringen kann.

Der Kunde hat PRAXINO unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

8. Kontrollrechte

PRAXINO stellt gemäß Art. 28 Abs. 3 lit. h DSGVO sicher, dass sich der Kunde von der Einhaltung der gesetzlichen Kontroll- und Prüfpflichten von PRAXINO auf eigene Kosten unter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen und des Datenschutzes selbst oder – im Regelfall – durch einen beruflich zur Verschwiegenheit verpflichteten Prüfer überzeugen kann. Der Kunde stimmt der Benennung eines unabhängigen externen Prüfers durch PRAXINO zu. PRAXINO verpflichtet sich dazu, dem Kunden auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen mit geeigneten Mitteln nachzuweisen. Dabei kann der Nachweis nach Wahl von PRAXINO auch durch

- die Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO),
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren (Art. 42 DSGVO),
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzaudatoren, Qualitätsaudatoren) oder
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz, ISO 27001)

erbracht werden.

Sollten im Einzelfall Inspektionen durch den Kunden oder einen unabhängigen externen Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufes durchgeführt. PRAXINO darf diese von einer vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Für die Unterstützung bei der Durchführung von Inspektionen darf PRAXINO eine angemessene Vergütung verlangen.

Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Kunden eine Inspektion vornehmen, gilt das Vorstehende entsprechend. Die Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn die Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.



Zusatzvereinbarung zur Auftragsvereinbarung gemäß Art. 28 DSGVO

9. Unterauftragnehmer

Als Unterauftragsverhältnisse im Sinne dieser Vereinbarung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der (haupt-)vertraglich vereinbarten Leistungen beziehen. Nicht hierzu gehören Nebenleistungen, die PRAXINO bei der Auftragsdurchführung in Anspruch nimmt, z. B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software der Datenverarbeitungsanlagen. PRAXINO ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Kunden auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

PRAXINO darf Unterauftragnehmer (weitere Auftragnehmer) nur mit dokumentierter Zustimmung des Kunden nach Maßgabe der folgenden Regelungen beauftragen:

- Der Kunde erklärt hiermit seine Zustimmung (allgemeine Genehmigung im Sinne von Art. 28 Abs. 2 DSGVO), dass PRAXINO zur Erfüllung ihrer vertraglich vereinbarten Leistungen verbundene Unternehmen von PRAXINO zur Leistungserfüllung heranzieht bzw. verbundene Unternehmen von PRAXINO mit Leistungen unterbeauftragt. Eine Auflistung sämtlicher verbundener Unternehmen von PRAXINO stellt diese dem Kunden bei Bedarf zur Verfügung.
- Der Kunde erklärt hiermit ferner seine Zustimmung (allgemeine Genehmigung im Sinne von Art. 28 Abs. 2 DSGVO), dass PRAXINO zur Erfüllung ihrer vertraglich vereinbarten Leistungen die im Anhang 2 aufgeführten weiteren Unternehmen zur Leistungserfüllung heranzieht bzw. unterbeauftragt.
- Vor der Heranziehung weiterer oder der Ersetzung eines Unterauftragnehmers wird PRAXINO den Kunden informieren. Der Kunde kann der beabsichtigten Heranziehung oder Ersetzung von Unterauftragnehmern innerhalb einer von PRAXINO gesetzten angemessenen Frist, die in der Regel nicht weniger als zehn Werktage betragen soll, aus wichtigem Grund gegenüber PRAXINO widersprechen. Geht kein Widerspruch innerhalb der Frist bei PRAXINO ein, gilt die Zustimmung zur Heranziehung bzw. Ersetzung als erteilt. Eine Weitergabe von personenbezogenen Daten an den Unterauftragnehmer und dessen erstmaliges Tätigwerden dürfen erst mit Zustimmung des Kunden bzw. mit Ablauf der Widerspruchsfrist erfolgen.
- Erteilt PRAXINO Aufträge an Unterauftragnehmer, so obliegt es PRAXINO, ihre datenschutzrechtlichen Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen. Hierzu wird PRAXINO mit Unterauftragnehmern vertragliche Vereinbarungen gemäß Art. 28 Abs. 2 bis 4 DSGVO treffen.

Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung von PRAXINO. Die Datenschutzpflichten in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

10. Löschung von Daten und Rückgabe von Datenträgern

PRAXINO ist verpflichtet, nach Abschluss der vertraglich vereinbarten Leistungen oder früher, sofern der Kunde dies anweist und dies vom Weisungsrecht erfasst ist, spätestens aber mit Beendigung des Hauptvertrages, sämtliche in ihren Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie



Zusatzvereinbarung zur Auftragsvereinbarung gemäß Art. 28 DSGVO

Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, an den Kunden auszuhändigen oder mit dessen Zustimmung datenschutzkonform zu vernichten. Gleiches gilt für Test- und Ausschussmaterial sowie ggf. angefertigte Sicherungskopien; im Falle von Test- und Ausschussmaterialien ist PRAXINO stets zur Löschung berechtigt.

Eine Pflicht zur Löschung von Daten besteht nicht, soweit PRAXINO gesetzlich, vertraglich oder satzungsmäßig zur Aufbewahrung der personenbezogenen Daten über das Vertragsende hinaus verpflichtet ist. In diesen Fällen sind die Daten erst nach Ablauf der jeweils einschlägigen Aufbewahrungsfristen datenschutzkonform zu löschen. Entsprechend sind Dokumentationen, die dem Nachweis der auftrags- oder ordnungsgemäßen Datenverarbeitung dienen, durch PRAXINO entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. PRAXINO kann diese Dokumentationen zu ihrer Entlastung bei Vertragsende dem Kunden übergeben.

Trifft der Kunde durch Einzelweisungen weitergehende Vorgaben betreffend die Aushändigung oder Löschung der Daten, so hat er die PRAXINO hierbei entstehenden zusätzlichen Kosten zu erstatten.

11. Haftung

Die Haftung von PRAXINO bemisst sich nach den Regelungen des Hauptvertrages.

12. Schlussbestimmungen

Änderungen, Ergänzungen und die Aufhebung dieser Vereinbarung bedürfen der Textform. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses.

Sollten einzelne Bestimmungen dieser Vereinbarung 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 Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den einschlägigen datenschutzrechtlichen Vorgaben genügt. Entsprechendes gilt für die Ausfüllung von Vertragslücken.