

Vertrag über die Auftragsverarbeitung personenbezogener Daten

Zwischen

der Praxis Dr. med. Max Mustermann

im Folgenden: **Auftraggeber**

und

der Firma

Prakt-IQ UG (haftungsbeschränkt)

Margarete-Böhme-Str. 3

25813 Husum, Deutschland

vertreten durch den Geschäftsführer: Dr. Christian Klaproth

im Folgenden: **Auftragnehmer**

1. Einleitung, Geltungsbereich, Definitionen

- 1.1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und Auftragnehmer (im Folgenden gemeinsam „Parteien“) im Rahmen der Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO im Zusammenhang mit der Nutzung der cloudbasierten Software-as-a-Service-Lösung „PraktIQ“ (nachfolgend „Software“).
- 1.2. Die Software ist nach dem Grundsatz der Datenminimierung so konzipiert, dass medizinische Inhalte vor externer Weiterverarbeitung grundsätzlich lokal im Einflussbereich des Auftraggebers von direkten Identifikatoren und identifizierenden Kontextangaben bereinigt und (pseudo)anonymisiert werden. Im Regelbetrieb ist die Software darauf ausgelegt, dass der Auftragnehmer keine identifizierbaren Patientendaten verarbeitet. Soweit ein Personenbezug im Einzelfall nicht ausgeschlossen werden kann, erfolgt die Verarbeitung vorsorglich auf Grundlage dieses AVV.
- 1.3. Dieser Vertrag findet vorsorglich auf alle Verarbeitungsvorgänge Anwendung, bei denen im Zusammenhang mit der Nutzung der Software ausnahmsweise personenbezogene Daten im Auftrag des Auftraggebers verarbeitet werden, insbesondere im Rahmen von Support und Fehlerbehebungsprozessen, technisch unvermeidbaren Verarbeitungen oder sonstigen dokumentierten Ausnahmefällen.
- 1.4. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DatenschutzGrundverordnung (DSGVO) zu verstehen. Der Auftraggeber ist „Verantwortlicher“, der Auftragnehmer „Auftragsverarbeiter“. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint; im Übrigen genügt Textform, soweit eine angemessene Nachweisbarkeit gewährleistet ist und zwingendes Recht nichts anderes verlangt.

2. Gegenstand und Dauer der Verarbeitung

2.1. Gegenstand

Der Auftragnehmer übernimmt folgende Verarbeitungen:

- Der Auftragnehmer stellt eine cloudbasierte Software zur Verfügung, die medizinische Inhalte vor externer Weiterverarbeitung lokal im Einflussbereich des Auftraggebers von direkten Identifikatoren und identifizierenden Kontextangaben bereinigt (Vor anonymisierung/Pseudonymisierung) und die technische Strukturierung, Aufbereitung und Orchestrierung von Anfragen an externe KIDienste übernimmt. Die inhaltliche Aufbereitung der so (pseudo)anonymisierten Texte erfolgt durch externe KISysteme; der Auftragnehmer erbringt insoweit ausschließlich technische Unterstützungs- und Vermittlungsleistungen und nimmt keine eigenständige medizinische Bewertung oder Entscheidungsfindung vor.

- Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Vertrag über die Nutzung der cloudbasierten Software-as-a-Service-Lösung „Prakt-IQ“ (nachfolgend „Software“) vom tt.mm.jjjj (im Folgenden „Hauptvertrag“).

2.2. Dauer

Die Verarbeitung beginnt am tt.mm.jjjj und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

3. Art, Zweck und Betroffene der Datenverarbeitung:

3.1. Art und Zweck der Verarbeitung

Die Software ist so gestaltet, dass medizinische Inhalte vor externer Weiterverarbeitung grundsätzlich lokal beim Auftraggeber von Personenstammdaten bereinigt und mindestens pseudonymisiert sowie von direkten Identifikatoren und identifizierenden Kontextangaben befreit werden. Die Datenverarbeitung erfolgt ausschließlich im Auftrag und nach Weisung des Auftraggebers.

3.2. Art der Daten

1. Nicht Gegenstand dieses Vertrages sind die in eigener datenschutzrechtlicher Verantwortlichkeit des Auftragnehmers verarbeiteten Daten, insbesondere:
 - Stammdaten der Nutzerkonten (Name, berufliche Rolle/Funktion, Praxis/ Unternehmensbezeichnung),
 - geschäftliche Kontaktdaten (Adresse, E-Mail, Telefonnummer),
 - Vertrags-, Nutzungs-, Kontingent- und Abrechnungsdaten,
 - Zahlungs- und Transaktionsdaten im Rahmen der Zahlungsabwicklung
 - LANR (Einheitliche Fortbildungsnummer zur beruflichen Identifikation).

Diese Daten werden nach Maßgabe der Datenschutzerklärung des Auftragnehmers verarbeitet.

Im Rahmen dieses Vertrages können in dokumentierten Ausnahme und Supportfällen insbesondere folgende Kategorien personenbezogener Daten im Auftrag verarbeitet werden:

- Inhalts und Kommunikationsdaten, die der Auftraggeber oder seine Nutzer im Rahmen von Support, Fehleranalyse oder sonstigen dokumentierten Ausnahmeprozessen bereitstellen,
- ausnahmsweise vom Auftraggeber eingebrachte personenbezogene Patientendaten, soweit diese entgegen der vorgesehenen (Pseudo) Anonymisierung in identifizierbarer Form verarbeitet werden müssen,
- zugehörige Nutzungs- und Protokolldaten, soweit sie sich auf die im Auftrag verarbeiteten Inhalte oder Vorgänge beziehen.

3.3. Kategorien betroffener Personen

Von den im Rahmen dieses Vertrages im Auftrag verarbeiteten personenbezogenen Daten können insbesondere betroffen sein:

- Patienten des Auftraggebers, jedoch nur in dokumentierten Ausnahme und Supportfällen gemäß Ziffer (2) oben,
- Nutzer und Mitarbeiter des Auftraggebers, soweit deren personenbezogene Daten ausnahmsweise im Rahmen von Support, Fehleranalyse oder sonstigen dokumentierten Ausnahmeprozessen im Auftrag verarbeitet werden.

Die Verarbeitung personenbezogener Daten von Nutzern und Mitarbeitern des Auftraggebers zu Zwecken der Vertragsdurchführung, Nutzerverwaltung, Systemsicherheit und Abrechnung erfolgt im Übrigen in eigener Verantwortlichkeit des Auftragnehmers und ist nicht Gegenstand dieses Vertrages.

4. Technische und organisatorische Maßnahmen

- 4.1. Der Auftragnehmer hat die Verarbeitung von personenbezogenen Daten so zu gestalten, dass ein Bezug zu einer natürlichen Person nur unter Zuhilfenahme zusätzlicher Daten möglich ist, Art. 32 Abs. 1 lit. a) DS-GVO.
- 4.2. Vor einer externen Weiterverarbeitung medizinischer Inhalte werden nach der vorgesehenen Systemarchitektur lokal beim Auftraggeber insbesondere folgende direkten Identifikatoren entfernt oder unkenntlich gemacht:
Vor- und Nachname,
 - Geburtsdatum,
 - Anschrift,
 - Telefonnummer,
 - E-Mail-Adresse,
 - Versicherungsnummer,
 - sonstige eindeutig identifizierende Angaben.
- 4.3. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. 3Soweit die Prüfung bzw. ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

- 4.4. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c und lit. e Hs. 1, Art. 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1, 2 DSGVO, herzustellen. 2Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme und Dienste. 3Dabei 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 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anlage 4].
- 4.5. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung.
5. Pflichten des Auftragnehmers
- 5.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke, es sei denn die betroffenen Personen willigen ausdrücklich in eine weitere Verarbeitung ihrer personenbezogenen Daten ein.
- 5.2. Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
- 5.3. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
- 5.4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
- 5.5. Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzerfordernungen laufend angemessen angeleitet und überwacht werden.

- 5.6. Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten, bei Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde. Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.
- 5.7. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
- 5.8. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.
- 5.9. Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.
- 5.10. Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit ausdrücklicher Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.
- 5.11. Ist der Auftragnehmer nicht in der Europäischen Union niedergelassen, bestellt er, soweit verpflichtet, einen verantwortlichen Ansprechpartner in der Europäischen Union gem. Art. 27 Datenschutz-Grundverordnung. Die Kontaktdaten des Ansprechpartners sowie sämtliche Änderungen in der Person des Ansprechpartners sind dem Auftraggeber unverzüglich mitzuteilen.
6. Sicherheit der Verarbeitung
- 6.1. Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.
-

- 6.2. Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.
 - 6.3. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
 - 6.4. Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
 - 6.5. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
 - 6.6. Die Verarbeitung von Daten in Privatwohnungen ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.
 - 6.7. Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.
 - 6.8. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebes zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers.
7. Regelungen zur Berichtigung, Löschung und Sperrung von Daten
 - 7.1. Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
 - 7.2. Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

8. Unterauftragsverhältnisse

- 8.1. Der Auftraggeber erteilt eine allgemeine Genehmigung für die in Anlage 2 genannten Unterauftragnehmer. Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragnehmern rechtzeitig in Textform. Der Auftraggeber kann der Änderung aus wichtigem Datenschutz richtigen Grund widersprechen.
- 8.2. Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten, vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
- 8.3. Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.
- 8.4. Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.
- 8.5. Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.
- 8.6. Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.
- 8.7. Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer - dokumentiert - davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.
- 8.8. Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel 4 (10) und (11) dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist. Soweit aktuell gültige Standardvertragsklauseln auf Basis einer Entscheidung der EU-Kommission (z.B. gemäß Kommissionsentscheidung 2010/87/EU) oder Standarddatenschutzklauseln gem. Art. 46 DSGVO als angemessene Garantien eingesetzt werden, bevollmächtigt der Auftraggeber den Auftragnehmer unter Befreiung vom Verbot der Doppelvertretung gemäß § 181 BGB, zur Vornahme aller hierfür erforderlichen Handlungen sowie zur Abgabe und Entgegennahme von Willenserklärungen gegenüber dem Subunternehmer. Ferner ist der Auftragnehmer berechtigt, die Rechte und Befugnisse des Auftraggebers aus dieser Vereinbarung gegenüber dem Subunternehmer auszuüben.

- 8.9. Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber unaufgefordert vorzulegen. Der Auftragnehmer bewahrt die Dokumentation über durchgeführte Prüfungen mindestens bis zum Ablauf des dritten Kalenderjahres nach Beendigung der Auftragsverarbeitung auf und legt diese dem Auftraggeber auf Verlangen jederzeit vor.
- 8.10. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.
- 8.11. Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.
- 8.12. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.
- 8.13. Externe Dienste (z.B. OpenAI, Stripe) erhalten nur pseudonymisierte Inhalte. OpenAI (USA) bedient sich EU-US Data Privacy Framework (DPF) bzw. SCC, Stripe (USA) ist DPF-zertifiziert. Weitere Dienste arbeiten mit SCC (Anlage 3).
9. Rechte und Pflichten des Auftraggebers
- 9.1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
- 9.2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
- 9.3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

- 9.4. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.
- 9.5. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

10. Mitteilungspflichten

- 10.1. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes im Auftrag verarbeiteter personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 - eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

- 10.2. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
- 10.3. Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
- 10.4. Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

11. Weisungen

- 11.1. Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
- 11.2. Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.
- 11.3. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
- 11.4. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
- 11.5. Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

12. Beendigung des Auftrags

- 12.1. Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten oder Kopien derselben noch in der Verfügungsgewalt des Auftragnehmers, hat dieser des nach Wahl des Auftraggebers die Daten entweder zu vernichten oder an den Auftraggeber zu übergeben. Die Wahl hat der Auftraggeber innerhalb von 2 Wochen nach entsprechender Aufforderung durch den Auftragnehmer zu treffen. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt mindestens Schutzklasse 1.
- 12.2. Der Auftragnehmer ist verpflichtet, die unverzügliche Vernichtung bzw. Rückgabe auch bei Subunternehmern herbeizuführen.
- 12.3. Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

12.4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer mindestens bis zum Ablauf des dritten Kalenderjahres nach Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber übergeben.

13. Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

14. Haftung

14.1. Die Parteien haften gegenüber betroffenen Personen nach Maßgabe von Art. 82 DSGVO als Gesamtschuldner für Schäden, die durch eine nicht den datenschutzrechtlichen Vorschriften entsprechende Verarbeitung personenbezogener Daten im Rahmen dieses Vertrages verursacht wurden.

14.2. Im Innenverhältnis zwischen den Parteien haftet jede Partei entsprechend ihrem jeweiligen Verantwortungs und Verursachungsanteil. Der Auftragnehmer haftet gegenüber dem Auftraggeber nur für Schäden, die auf eine von ihm zu vertretende und tatsächlich im Rahmen dieses Vertrages durchgeführte Verarbeitung personenbezogener Daten zurückzuführen sind. Entsprechendes gilt umgekehrt für den Auftraggeber.

14.3. Soweit Verarbeitungsvorgänge ausschließlich (pseudo)anonymisierte Inhalte ohne Personenbezug im Sinne der DSGVO betreffen, findet Art. 82 DSGVO keine Anwendung; in diesen Fällen richtet sich die Haftung der Parteien nach den allgemeinen gesetzlichen und vertraglichen Bestimmungen des Hauptvertrags.

14.4. Macht ein Dritter eine Forderung nach Art. 82 DSGVO gegen eine Partei geltend, so wird die in Anspruch genommene Partei die andere Partei unverzüglich informieren und ihr Gelegenheit geben, sich an der Verteidigung zu beteiligen. Die Parteien unterstützen sich gegenseitig bei der Abwehr unberechtigter Ansprüche und bei der Aufklärung des Sachverhalts.

14.5. Weitergehende Haftungsregelungen des Hauptvertrags bleiben unberührt, soweit sie zwingendem Datenschutzrecht nicht widersprechen.

15. Sonderkündigungsrecht

15.1. Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

- 15.2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
- 15.3. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.
- 15.4. Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrages oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Auftraggeber entstehen.

16. Sonstiges

- 16.1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
- 16.2. Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
- 16.3. Für Nebenabreden sind die Schriftform und die ausdrückliche Bezugnahme auf diese Vereinbarung erforderlich.
- 16.4. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- 16.5. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Unterschriften

Ort, Datum

Ort, Datum

Auftraggeber

Auftragnehmer

Anlage 1 – technische und organisatorische Maßnahmen

Im Folgenden werden die auftragsbezogenen technischen und Organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pfortner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Datenschutz-Management; inkl. der geforderten regelmäßigen Überprüfung, Bewertung und Evaluierung der Datenschutzmaßnahmen!
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
- Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Anlage 2 – Zugelassene Subdienstleister/ Empfänger im Rahmen der Leistungserbringung

1. IONOS SE

Funktion: Hosting / Server-Infrastruktur / Speicherung auftraggeberbezogener Daten

Sitz: Deutschland

Rolle: Unterauftragsverarbeiter für gespeicherte personenbezogene Daten, soweit solche beim Auftragnehmer verarbeitet oder gespeichert werden

2. OpenAI OpCo, LLC bzw. OpenAI Ireland Ltd.

Funktion: KI-/Inference-Dienst

Rolle: Einbindung nur insoweit, als übermittelte Inhalte im Einzelfall datenschutzrechtlich noch als personenbezogen oder pseudonymisiert einzustufen sind; Drittlandübermittlung nur auf Grundlage der Voraussetzungen nach Kapitel V DSGVO

OpenAI stellt für Business-Services ein DPA bereit und verweist auf seine Subprocessor-Struktur.

Anlage 3 – Weisungsberechtigte Personen, Adresse zur Meldung von Datenschutzverletzungen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

Auftraggeberin:

Auftragnehmer:

Prakt-IQ UG (haftungsbeschränkt)

Margarete-Böhme-Str. 3; 25813 Husum; Deutschland

Vertreten durch den Geschäftsführer: Dr. Christian Klaproth

Kontakt zur Meldung über die Verletzung personenbezogener Daten:

Anlage 4 – Sicherstellung der Anonymisierung/ Pseudonymisierung

In diesem Dokument werden die verbindlichen technischen und organisatorischen Maßnahmen beschrieben, die im Zusammenhang mit den durchgeführten Auftragsverarbeitungsvorgängen zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt wurden. Diese dargestellten Maßnahmen spiegeln das Datenschutz- und Datensicherheitskonzept der Prakt-IQ UG wider.

Der folgende Maßnahmenkatalog beschreibt die im Rahmen der Auftragsverarbeitung zu treffenden technischen und organisatorischen Einzelmaßnahmen nach Art. 24 Abs. 1 EU-DSGVO. Die EU-DSGVO verpflichtet Unternehmen, die Datenverarbeitung personenbezogener Daten durch angemessene, technische und organisatorische Maßnahmen abzusichern und personenbezogene Daten nach Möglichkeit zu pseudonymisieren. Die getroffenen Maßnahmen müssen dabei dem Risiko des jeweiligen Datenverarbeitungsvorgangs Rechnung tragen und dem derzeitigen Stand der Technik entsprechen. Diese Anforderungen erfüllt die Prakt-IQ UG durch ein wirksames Zusammenspiel aus Datenschutzmanagement und Informationssicherheitsmanagement und hat angemessene Maßnahmen zur Absicherung der Datenverarbeitungsvorgänge getroffen. Besondere Beachtung in jedem Datenverarbeitungsvorgang finden die Schutzwerte Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit. Für diese Schutzwerte gelten die folgenden informationssicherheitsrelevanten Definitionen:

Anonymisierungsmodul:

1. Datenimport

Quellen:

- PVS (z. B. Tomedo via Schnittstelle / Export)
- Freitextdokumente (Arztbriefe, Befunde)
- strukturierte Daten (optional)

Verarbeitung:

- temporäre lokale Verarbeitung
- keine persistente Speicherung im Anonymisierungsmodul

2. Identifikation direkter Identifikatoren

2.1. Regelbasierte Erkennung

Erkannte Kategorien:

- Personennamen
- Geburtsdaten
- Adressen
- Telefonnummern
- E-Mail-Adressen
- Versicherungsnummern

2.2 Fuzzy Matching (Damerau-Levenshtein)

Ziel: Erkennung von Varianten und Tippfehlern

Beispiele:

- „Müller“ → „Mueller“
- „Schmidt“ → „Schmid“
- Vertipper, OCR-Fehler

1. Technik:

- Berechnung der Edit-Distance
- Schwellenwertbasierte Klassifikation

3. Löschrategie

Alle identifizierten Elemente werden:

- vollständig entfernt oder
- durch neutrale Platzhalter ersetzt

Beispiele:

- „Max Mustermann“ → **[NAME]**
- „geb. 12.03.1975“ → **[GEBURTSDATUM]**

4. Datenfluss

Übertragung ausschließlich:

- pseudonymisierter/anonymisierter Texte
- ohne Metadaten (IP, IDs, Referenzen)
- keine Speicherung der Rohdaten im KI-System
- temporäre Speicherung im Zwischenspeicher
- keine dauerhafte lokale Speicherung
- Überschreibung vorhandener Daten durch jede neue Aktion
- keine Rückführungsmöglichkeit im Systemdesign

5. Logging und Nachvollziehbarkeit

Erfasst werden:

- Zeitstempel der Verarbeitung
- Nutzer-/Praxis-ID-Version