Auftragsverarbeitungsvertrag gem. Artt. 28, 29 DS-GVO
(entspricht auch den Bedingungen gem. § 80 SGB X, § 29 KDG, § 29 KDR-OG und §30 DSG-EKD)

Adresse oder Stempel des Auftraggebers:

(Verantwortlicher im Sinne der DS-GVO, nachfolgend „**Auftraggeber**“ genannt)

und der

Qodia GmbH
Heimhuder Str. 36
20148 Hamburg
E-Mail: info@qodia.de

(Auftragsverarbeiter im Sinne der DS-GVO, nachfolgend „**Auftragnehmer**“ genannt)

Präambel

Diese Vereinbarung regelt die Maßnahmen zum Schutz von personenbezogenen Daten gem. Art. 4 Nr. 1 DS-GVO, Gesundheitsdaten gem. Art. 4 Nr. 15 DS-GVO und Sozialdaten im Sinne des § 67 Abs. 2 SGB X bei der Datenverarbeitung im Auftrag unter Berücksichtigung der Artt. 28, 29 DS-GVO und der § 80 SGB X sowie § 29 KDG, § 29 KDR-OG und §30 DSG-EKD.

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand
Der Gegenstand des Auftrags ergibt sich aus Anlage 1 zu diesem Auftragsverarbeitungsvertrag.

(2) Dauer
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der vereinbarten Dienstleistung bis zur vollständigen Erfüllung und Abwicklung der vereinbarten Leistungen. Die Geheimhaltungspflicht gilt darüber hinaus unbegrenzt.

Der Auftraggeber kann den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn

a) ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen des Vertrages vorliegt oder
b) der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder
c) der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert oder
d) die Grundlage der Vertragserfüllung wesentlich verändert wird oder ganz entfällt aufgrund einer Änderung der Rechts- oder Gesetzeslage oder wegen aufsichtsrechtlicher Maßnahmen.

Vor der fristlosen Kündigung räumt der Auftraggeber dem Auftragnehmer eine angemessene Frist (maximal 30 Tage) zur Abhilfe ein, es sei denn, der Verstoß ist unheilbar oder eine Aufsichtsbehörde verlangt die Aufhebung.

Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 2 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

- Der Umfang der Tätigkeiten des Auftragnehmers richtet sich nach den Anforderungen des Auftraggebers. Die gesetzliche Grundlage für die Abwicklung des Genehmigungs-verfahrens ist dieser Vertrag gem. Art. 28 DS-GVO.
- Der Auftragnehmer übernimmt für den Auftraggeber folgende Tätigkeiten:
    - Die Konkretisierung des Auftragsinhalts ergibt sich aus Anlage 1 zu diesem Auftragsverarbeitungsvertrag
    - Der Auftragsinhalt ist nicht abschließend. Je nach Wahl von Zusatzdienstleistungen durch den Auftraggeber bei dem Auftragnehmer, kann der Auftragsinhalt über die unter § 2 geregelten Inhalte hinausgehen. In diesem Fall ergibt sich die Konkretisierung aus der Leistungsvereinbarung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder der Schweiz statt. Eine Verarbeitung pseudonymisierter Daten findet bei Dienstleistern in den USA statt, wobei als Serverstandort EU gewählt wurde. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und erfolgt nur, wenn ein Angemessenheitsbeschluss nach Art. 45 DS-GVO vorliegt und der Auftragnehmer durch vertragliche Maßnahmen wie. z. B. EU-Standardvertragsklauseln sichergestellt hat, dass die Bedingungen dieser Vereinbarung auch in einem Drittland gelten bzw. die Verarbeitung der Daten des Auftraggebers mit einem der Verarbeitung angemessenen Sicherheitsniveau stattfindet. In Anlage 3 sind die Standorte, bei denen Daten des Auftraggebers verarbeitet werden, eingetragen. Eine Veränderung der Standorte oder Räumlichkeiten, in denen Daten des Auftraggebers verarbeitet werden, oder ein Verlagern der Auftragsdurchführung an eine andere Örtlichkeit als die mit dem Auftraggeber vereinbarte, bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers.

(2) Art der Daten

Gegenstand der Verarbeitung sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)]

- Die Datenarten bzw. Datenkategorien ergeben sich aus Anlage 1 zu diesem Auftragsverarbeitungsvertrag.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffener Personen umfassen:

- Die Kategorien betroffener Personen ergeben sich aus Anlage 1 zu diesem Auftragsverarbeitungsvertrag

§ 3 Technisch-organisatorische Maßnahmen

(1) 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 schriftlich oder in Textform zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt 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. 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 Abs. 1 DS-GVO zu berücksichtigen. Die technischen und organisatorischen Maßnahmen ergeben sich aus Anlage 2 zu diesem Auftragsverarbeitungsvertrag.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen zu dokumentieren.

(4) Sämtliche Dokumentationen zu den technischen und organisatorischen Maßnahmen, Dokumentationen von Regelungen zum Datenschutz und zur Informationssicherheit und Audit- bzw. Prüfberichte müssen in deutscher oder englischer Sprache verfasst bzw. in deutscher oder englischer Übersetzung bereitgehalten werden.

§ 4 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme in Anlage 4 mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

b) Die Wahrung der Vertraulichkeit und des Daten- sowie Sozialgeheimnisses gemäß Artt. 28 Abs. 3 Satz 2 lit. b, 29, 32 Abs. 4 DS-GVO, § 35 SGB I. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit und zur Geheimhaltung unter Hinweis auf die rechtlichen Folgen einer Pflichtverletzung, insbesondere nach § 203 Abs. 4 StGB, nachweisbar verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Dies umfasst die Verpflichtung zur Geheimhaltung auch über das bestehende Dienst- oder Beschäftigungsverhältnis hinaus. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 lit. c, 32 DS-GVO (Einzelheiten in Anlage 2).

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bzw. Sozialdaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. Die Kontrollen, die Ergebnisse und ggf. umgesetzte Maßnahmen sind zu protokollieren und für mindestens 6 Jahre aufzubewahren.

h) Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 6 dieses Vertrages.

i) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln. Diese Verpflichtung besteht über das Ende des Vertragsverhältnisses hinaus.

j) Personenbezogene Daten des Auftraggebers dürfen nicht im öffentlichen Raum (z.B. Flughafen, Bahn etc.) verarbeitet werden. Die Verarbeitung der personenbezogenen Daten des Auftraggebers außerhalb der Geschäftsräume des Auftragnehmers ist nur im nichtöffentlichen Raum zulässig und nur mit gesicherten firmeneigenen Geräten des Auftragnehmers. Die Bestimmungen zu den technisch-organisatorischen Maßnahmen nach § 3 sind zu beachten.

k) Die Verarbeitung von personenbezogenen Daten in Privatwohnungen ist erlaubt. Dann ist sicherzustellen, dass dies unter Beachtung der technischen und organisatorischen Maßnahmen gemäß § 3 dieser Vereinbarung erfolgt.

l) Die Nutzung von Cloudcomputing durch den Auftragnehmer ist nur zulässig, wenn dieser mit dem jeweiligen Anbieter eine Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO abschließt und die technische und organisatorische Sicherstellung der Infrastruktur des Anbieters den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entspricht und die Anforderungen des § 80 SGB X, insbesondere Abs. 2, bezüglich der räumlichen Beschränkungen der Verarbeitung eingehalten werden.

m) Der Auftragnehmer verpflichtet sich, dass die Daten des Auftraggebers von Daten anderer Auftraggeber streng getrennt werden. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

n) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (z.B. durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren) oder durch sonstige Ereignisse gefährdet werden, hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer ist verpflichtet, alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber zu unterrichten, dass es sich um Daten des Auftraggebers handelt, über die er keinerlei Verfügungs- oder sonstige Bestimmungsgewalt oder Eigentumsrechte gem. § 273 BGB hat.

§ 5 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen, und bei denen ein Zugriff auf personenbezogene Daten bzw. Sozialdaten nicht ausgeschlossen werden kann. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsdienstleister, dem Postgeheimnis unterliegende Post-/Transportdienstleistungen, Gebäudereinigung sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Sicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer ist berechtigt, die in der Anlage 1 zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 3 genannten Voraussetzungen zulässig.

(3) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten bzw. Umsetzen kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer glaubhaften Begründung in Textform binnen drei Wochen nach Zugang der „Information“ zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber bis zum Zeitpunkt der Hinzuziehung des Unterauftragsnehmers kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information“ erfolgt gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

(4) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat, sofern der Unterauftragnehmer zur Benennung eines Datenschutzbeauftragten gesetzlich verpflichtet ist.

(5) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(6) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

§ 6 Kontrollrechte des Auftraggebers und dessen Aufsichtsbehörden

(1) Der Auftraggeber, dessen zuständige Aufsichtsbehörden bzw. ein von ihm beauftragter Dienstleister (im folgenden Auftraggeber) haben das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Sie haben das Recht, sich durch Stichprobenkontrollen von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Das Prüfrecht umfasst insbesondere die Besichtigung von Grundstücken und Geschäftsräumen, Auskünfte zur Vertragsausführung, Einsicht in Papierunterlagen und auch die Einsichtnahme in die beim Auftragnehmer gespeicherten personenbezogene Daten des Auftraggebers, soweit dies im Rahmen des Auftrags zur Überwachung von Datenschutz und Datensicherheit erforderlich ist. Dies gilt insbesondere für den Nachweis der Umsetzung der technischen und organisatorischen Maßnahmen.

(4) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder
b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001 oder BSI-Standards).

(5) Der Auftragnehmer sichert zu, dass er die notwendige personelle und sachliche Unterstützung bei den Prüfungen zur Verfügung stellt.

(6) Eine Kontrolle jährlich und Kontrollen bei Verdacht auf Datenschutzverletzungen sind zu gewährleisten. Aufwände und Kosten, die beim Auftragnehmer im Zuge der Kontrollen durch den Auftraggeber entstehen, trägt allein der Auftragnehmer, wenn die Kontrollen in einem üblichen Umfang und nicht öfter als einmal jährlich stattfinden. Gehen Kontrollen oder Prüfungen umfänglich oder zeitlich über das übliche Maß hinaus, kann der Auftragnehmer die ihm entstehenden tatsächlichen Kosten dem Auftraggeber berechnen.

§ 7 Mitwirkungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO und § 83a bis 84 SGB X genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen der Aufsichtsbehörde. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, 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,

b) die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden. In diesem Falle hat der Auftragnehmer sofort alle erforderlichen Maßnahmen zur Sicherung der Sozialdaten zu treffen und weitere Anweisungen durch den Auftraggeber abzuwarten.

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung,

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

§ 8 Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber hat das Recht, erforderlichenfalls schriftliche Weisungen im Rahmen der Art. 28, 32 DS-GVO zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit zu erteilen. Ferner hat der Auftraggeber das Recht die Abwicklung des erteilten Auftrags zu bestimmen. Erweisen sich die durch den Auftraggeber geforderten Maßnahmen für den Auftragnehmer als nicht umsetzbar (z. B. aus wirtschaftlichen Gründen) stehen sowohl Auftragnehmer als auch Auftraggeber ein Sonderkündigungsrecht zu.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. in Textform).

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 9 Berichtigung, Einschränkung, Löschung und Rückgabe von personenbezogenen Daten

(1) Der Auftragnehmer darf die personenbezogenen Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich oder aufgrund eines anderen Rechts des Betroffenen gem. Artt. 15 – 22 DSGVO unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und den Auftraggeber bei der Erfüllung seiner Verpflichtungen dabei unterstützen.

(2) Soweit vom Leistungsumfang umfasst, ist das Löschkonzept, das Recht auf Vergessenwerden, die Berichtigung von personenbezogenen Daten, die Datenportabilität (soweit einschlägig) und Auskünfte nach schriftlicher oder nachvollziehbarer Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen und revisionssicher zu dokumentieren.

(3) Sämtliche Daten und Unterlagen sowie Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit den im Hauptvertrag genannten Leistungen dieser Datenschutzbestimmungen in die Verfügungsgewalt des Auftragnehmers gelangt sind, hat dieser entsprechend der jeweiligen Vereinbarungen im Einzelfall bzw. nach Abschluss der vertraglichen Arbeiten dem Auftraggeber auszuhändigen bzw. zu übermitteln. Dies gilt nicht für Ergebnisse, die das Geschäfts- oder Betriebsgeheimnis des Auftragnehmers verletzen.

(4) Auf Verlangen des Auftraggebers hat der Auftragnehmer in seinem Besitz befindliche Daten bzw. Datenbestände (z.B. physische Datenträger, elektronische Dateien oder Datenbanken in seinen Datenverarbeitungssystemen) nichtreproduzierbar zu löschen bzw. physisch zu vernichten. Die Vernichtung hat in Abhängigkeit von den verarbeiteten Sozialdaten nach DIN 66399 Teile 1 bis 3 bzw. ISO/IEC 21964 mindestens mit der Schutzklasse 3 mindestens mit Sicherheitsstufe 4 in der jeweils einschlägigen Materialklasse zu erfolgen. Die Datenlöschung hat nach anerkanntem BSI-Standard (Bundesamt für Sicherheit in der Informationstechnik) oder anderweitiger adäquater Regelungen für vertrauliche Daten in der jeweils aktuellen Fassung zu erfolgen. Dies gilt auch für Test- und Zwischenergebnisse.

Ist eine Löschung auf Sicherungskopien wegen der besonderen Art der Speicherung nur mit einem unverhältnismäßig hohen Aufwand möglich, sind die Daten nach Abstimmung mit dem Auftraggeber für jede weitere Verarbeitung einzuschränken.

(5) Die Löschung und Vernichtung hat der Auftragnehmer in geeigneter Weise zu protokollieren. Im Zweifelsfall sind geeignete Maßnahmen mit dem Auftraggeber abzustimmen. Hinsichtlich sämtlicher Löschvorgänge hat der Auftragnehmer dem Auftraggeber Löschprotokolle auf Verlangen zu übergeben.

(6) Endet das Vertragsverhältnis, hat der Auftragnehmer gegenüber dem Auftraggeber schriftlich zu erklären, dass die nicht mehr erforderlichen Daten und Datenträger ordnungsgemäß im Sinne dieses Vertrages gelöscht bzw. vernichtet wurden und welche Daten aus gesetzlichen Gründen über das Ende des Auftragsverhältnisses hinaus aufbewahrt werden müssen.

§ 10 Ansprechpartner

Ansprechpartner des Auftraggebers ergeben sich aus Anlage 4.

§ 11 Haftung

(1) Der Auftragnehmer haftet gegenüber dem Auftraggeber im Rahmen der gesetzlichen Bestimmungen für Schäden, die infolge schuldhaften Verhaltens gegen Datenschutzbestimmungen und gegen diese Datenschutzvereinbarung entstehen. Ebenso haftet er für schuldhaftes Verhalten seiner Unterauftragnehmer sowie deren Unterauftragnehmer.

(2) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

§ 12 Sonstiges

(1) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder nach Vereinbarungsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit der Vereinbarung im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen, die die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

(2) Sollten sich datenschutzrechtliche Änderungen während der Vertragslaufzeit ergeben, die zu einer Vertragsanpassung führen müssen, verpflichten sich die Vertragspartner Vertragsverhandlungen mit dem Ziel der Einigung aufzunehmen.

(3) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

(4) Dem Auftragnehmer ist bekannt, dass der Auftraggeber bezüglich der Berufsgeheimnisdaten das Schweigerecht nach §53a StPO hat. Ebenso unterliegen diese Daten dem Beschlagnahmeverbot gemäß § 97 Abs. 1 und 3 StPO. Im Fall einer versuchten Sicherstellung ist dieser daher durch den Auftragnehmer zu widersprechen. Der Verantwortliche ist daneben unverzüglich zu informieren, wenn eine Beschlagnahme der Daten zu erwarten ist oder bevorsteht. Zur Sicherung dieser Daten beim Auftragnehmer kann seitens des Auftragnehmers auf Anfrage des Auftraggebers eine Verpflichtungserklärung gem. § 203 Abs. 3 StGB abgegeben werden. Darüber hinaus ist die Einrede des Zurückbehaltungsrechtes i.S.v. § 273 BGB hinsichtlich der personenbezogenen Daten / Sozialdaten und der dazugehörigen Datenträger ausgeschlossen.

(5) Sämtliche Kommunikation zwischen dem Auftragnehmer und dem Auftraggeber sowie zwischen dem Auftragnehmer und den Aufsichten/Prüfdiensten haben in deutscher Sprache zu erfolgen.

§ 13 Inkrafttreten

(1) Diese Datenschutzbestimmungen treten mit Inkrafttreten des Dienstleistungsvertrags in Kraft.

(2) Es gilt die Gerichtsstandvereinbarung des Dienstleistungsvertrags.

Hamburg, 09.12.2025

_____	_____
Ort, Datum, Unterschrift Auftraggeber	Ort, Datum Unterschrift Auftragnehmer Qodia GmbH

Anlagen:

Anlage 1: Gegenstand und Konkretisierung des Auftragsinhalts, Datenarten/Datenkategorien, Kategorien betroffener Personen, Untervertragsverhältnisse

Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3: Standorte des Auftragnehmers

Anlage 4: Ansprechpartner des Auftragnehmers

Anlage 1 zum Auftragsverarbeitungsvertrag zwischen dem Auftraggeber und der Qodia GmbH (Auftragnehmer)

Gegenstand und Konkretisierung des Auftrags, Datenarten/Datenkategorien, Kategorien betroffener Personen, Untervertragsverhältnisse

Aus der Übersicht geht das genutzte Produkt des Auftraggebers, der Gegenstand und die Konkretisierung des Auftragsinhalts, die verschiedenen Datenarten bzw. Datenkategorien, die Kategorien betroffener Personen sowie etwaige Untervertragsverhältnisse hervor.

Erstellen von Rechnungen an Privatversicherte nach GOÄ	
Gegenstand des Auftrags	Erstellen von Rechnungen an Privatversicherte nach GOÄ mit Hilfe eines KI-Systems
Konkretisierung des Auftragsinhalts	Der Auftragnehmer stellt dem Auftraggeber eine Lösung zur effizienten Prüfung privatärztlicher Rechnungsdateien (PAD / PADnext) zur Verfügung. Dazu installiert der Auftragnehmer bei Auftraggeber eine Software (OnPrem) die die Daten aus der Datenbank / Systeminfrastruktur des Auftraggebers pseudonymisiert extrahiert. Die pseudonymisierten Daten werden dann mit Hilfe einer KI (SaaS) analysiert und die neuen Rechnungspositionen werden ermittelt. Anschließend werden die Daten aus der KI-Verarbeitung wieder zurück in die OnPrem Software beim Auftraggeber gespielt und die Positionen werden wieder an die Datenbank / Systeminfrastruktur des Auftraggebers übergeben. Die Arbeitsweise ist folgende: Die Qodia-Anwendung besteht aus einer lokalen Komponente innerhalb der Systemumgebung des Auftraggebers und einem Cloud-Dienst und funktioniert folgendermaßen: • Die vollständigen Patientendaten (z. B. Name, Anschrift, Versichertennummer etc.) werden ausschließlich lokal in der Systemumgebung des Auftraggebers verarbeitet und verlassen diese nicht. • Für die KI-gestützte Abrechnungsprüfung werden lediglich die hierfür erforderlichen Informationen (u. a. Gebührenordnungspositionen, Diagnosen, Altersangaben) zusammen mit einer lokalen Fall-ID/pseudonymisierte Kennung an Qodia API übermittelt. • Die Zuordnungstabelle zwischen dieser Fall-ID und der tatsächlichen Identität des Patienten verbleibt ausschließlich in der Systemumgebung des Auftraggebers (OnPrem). Weder Qodia selbst noch Unterauftragnehmer (z. B. Cloud-Anbieter) haben Zugriff auf diese Zuordnungstabelle oder auf die identifizierbaren Patientendaten.

	• Die pseudonymisierten Daten werden durch die KI verarbeitet und anschließend wieder zurück über die Qodia API übertragen. • Die durch die KI ausgewerteten Daten werden in der Systemumgebung des Auftraggebers (OnPrem) über die Fall-ID/pseudonymisierte Kennung den personenbezogen Daten wieder zugeordnet und damit komplettiert.	
Kategorien betroffener Personen	Kunden / Patienten des Auftraggebers (Betroffene im Sinn der DSGVO)	
Datenarten bzw. Datenkategorien des Kunden	Kunde: Namen, Kontaktdaten, Rechnungsdaten, Vertragsdaten, Bankdaten Betroffene: Namen, Adressdaten, Kontaktdaten, Gesundheitsdaten bzw. Daten aus der Behandlung	
Unterauftragnehmer	Adresse	Funktion
Amazon Web Services Germany GmbH (AWS)	Krausenstraße 38 10117 Berlin	Data Storage und Cloud Computing (Datenbank und Backend)
OpenAI	1455 3rd Street San Francisco Kalifornien, USA	LLM zur Auswertung der Daten und Erstellung der Rechnung
Google	600 Amphitheatre Parkway Mountain View Kalifornien, USA	Google Cloud für OCR, Gemini und Cloud Computing

Anlage 2 zum Auftragsverarbeitungsvertrag zwischen dem Auftraggeber und der Qodia GmbH (Auftragnehmer)

Präambel

Die in dieser Anlage aufgeführten technischen und organisatorischen Maßnahmen werden allgemein aufgeführt. Es versteht sich von selbst, dass die Qodia GmbH nur wenig technische und organisatorische Maßnahmen ergreifen muss, da die eigentliche Datenverarbeitung beim Auftraggeber (OnPrem) und in der Cloud (SaaS) stattfindet.

Das Datenflussdiagramm mit den einzelnen Datenfeldern ergänzen die TOM und verdeutlichen die Datenverarbeitung.

Technische und organisatorische Maßnahmen

Diese Auflistung der bei der Qodia GmbH getroffenen technischen und organisatorischen Maßnahmen im Datenschutz (TOM) orientiert sich an den Vorgaben des § 64 BDSG, der für nicht öffentliche Stellen keine Gültigkeit hat, gleichzeitig aber eine strukturierte Dokumentation der TOMs ermöglicht, da es weder in der EU-Datenschutzgrundverordnung (DSGVO) noch im Bundesdatenschutzgesetz (BDSG) dazu Vorgaben für nicht öffentliche Stellen gibt. Diese Angaben dokumentieren auch die Forderungen des § 26 KDG, § 26 KDR-OG, §6 KDO und des Art. 32 der DSGVO. Es soll Verantwortlichen (Auftraggebern) dazu dienen, ihre Prüf- und Dokumentationspflicht bei Auftragsverarbeitung gem. Art. 28, 29 DSGVO, § 29 KDG, § 29 KDR-OG, § 8 KDO und § 80 SGB X zu erleichtern.

Diese Aufstellung ist auch als Ergänzung zu einem bestehenden oder neuen, Art. 28, 29 DSGVO bzw. § 29 KDG, § 29 KDR-OG, § 8 KDO konformen Dienstleistungsvertrag gedacht und kann jedem Verantwortlichen (Auftraggeber) auf Anforderung zur Verfügung gestellt werden. Die getroffenen Maßnahmen unterliegen dem technischen Fortschritt und werden somit fortlaufend aktualisiert, wobei das bisher vorhandene Sicherheitsniveau nicht verringert werden darf.

Die Technischen und organisatorische Maßnahmen der Unterauftragnehmer können hier eingesehen werden. Es ist zu erwähnen, dass die Auftragnehmer nur pseudonymisierte Daten erhalten (siehe: „Konkretisierung des Auftragsinhalts“ in Anlage 1).
Pseudonymisierte Daten können unter Umständen wie anonymisierte Daten behandelt werden, nämlich dann, wenn für den Empfänger (Unterauftragnehmer) keine realistische Möglichkeit besteht, die betroffene Person zu identifizieren. Die ist hier der Fall.

Unterauftragnehmer	Technische und organisatorische Maßnahmen
Amazon Web Services Germany GmbH (AWS)	https://docs.aws.amazon.com/de_de/whitepapers/latest/navigating-gdpr-compliance/navigating-gdpr-compliance.pdf#protecting-your-data-on-aws
OpenAI	https://openai.com/de-DE/policies/row-privacy-policy/ https://openai.com/de-DE/policies/data-processing-addendum/
Google	https://support.google.com/a/answer/60762?hl=de https://support.google.com/googlecloud/answer/6056694?sjid=11533644184329204728-EU https://support.google.com/googlecloud/answer/6056650?hl=de&ref_topic=6055719&sjid=11533644184329204728-EU

Technische und organisatorische Maßnahmen (TOM)

Version:	1.2
Datum der Version:	04.12.2025
Erstellt durch:	Joachim Kramer, Datenschutz Kramer & Kramer GmbH
Genehmigt durch:	Ole Reinpold, Geschäftsführer

Änderungs-Historie

Datum	Version	Erstellt durch	Beschreibung der Änderung
04.06.2025	1.1	Joachim Kramer	Neuerstellung nach Aufnahme der TOM im Rahmen dieses AV-Vertrags
04.12.2025	1.2	Joachim Kramer	Aufnahme der TOM der Unterauftragnehmer

Vertraulichkeit (Art. 32 Abs. 1b DSGVO)

In unserem Haus ist die räumliche **Zutrittskontrolle** folgendermaßen sichergestellt:
Maßnahmen, durch die Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird.

Technische Maßnahmen:	**Organisatorische Maßnahmen:**
Es gelten die Maßnahmen der SaaS Betreiber.	Qodia hat keine eigenen Server.
	Laptops werden nie im Büro gelassen, sondern von den Mitarbeiter mitgeführt.

Um das unbefugte Eindringen in unsere Systeme und Datenverarbeitungssysteme zu verhindern, verwenden wir folgende **Zugangskontrollen**:
Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert werden.

Technische Maßnahmen:	**Organisatorische Maßnahmen:**
Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen
Separate Administrationspasswörter	Erstellen von Benutzerprofilen
Firewall	Zentrale Passwortvergabe
Automatische Desktopsperre	Richtlinie „Sicheres Passwort“

Wie wird der Zugriff (**Zugriffskontrolle**) auf verschiedene Daten bzw. Systeme geregelt:
Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen:	**Organisatorische Maßnahmen:**
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	Minimale Anzahl an Administratoren
	Verwaltung Benutzerrechte durch Administratoren
	Prozess zur Genehmigung von Zugriffsrechten

Um Daten, die zu unterschiedlichen Zwecken erhoben wurden oder um die Daten von Mandanten voneinander zu trennen (**Trennungskontrolle**), haben wir folgende Maßnahmen ergriffen:
Maßnahmen, die sicherstellen, dass Daten die zu unterschiedlichen Zwecken übermittelt wurden, auch getrennt verarbeitet werden.

Technische Maßnahmen:	**Organisatorische Maßnahmen:**
Trennung von Produktiv- und Testumgebung	Steuerung über Berechtigungskonzept
Mandantenfähigkeit relevanter Anwendungen	Festlegung von Datenbankrechten
	Einmaliges Attribut jedes Datensatzes (z. B. autom. vergebene Kundennummer)

Um Daten möglichst sicher zu verarbeiten und vor unberechtigtem Zugriff Dritter zu schützen haben wir folgende **Pseudonymisierung**smaßnahmen gem. Art. 32 Abs. 1 lit. a) DSGVO i. V. m. Art. 25 Abs. 1 DSGVO ergriffen:
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.

Technische Maßnahmen:	**Organisatorische Maßnahmen:**
Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (verschlüsselt)	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren

Integrität (Art. 32 Abs. 1b DSGVO)

Wir kontrollieren die Weitergabe (**Weitergabekontrolle**) personenbezogener Daten bei Übermittlung bzw. Übertragung oder bei Transport mit folgenden Maßnahmen:
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z. B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen:	**Organisatorische Maßnahmen:**
Protokollierung der Zugriffe und Abrufe	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
Bereitstellung über verschlüsselte Verbindungen wie sftp, https	

Wir gewähren die Nachvollziehbarkeit bzw. Dokumentation der Wartungsarbeiten bzw. Systemzugriffe mit folgenden Maßnahmen (**Eingabekontrolle**). Dadurch kann nachvollzogen werden, wer auf ein System bzw. Daten zugegriffen hat und wann:
Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können.

Technische Maßnahmen:	**Organisatorische Maßnahmen:**
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
Manuelle Kontrolle der Protokolle	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	Klare Zuständigkeiten für Löschungen

Die Aufträge (**Auftragskontrolle**) unserer Kunden kontrollieren wir anhand folgender Möglichkeiten:
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen:	**Organisatorische Maßnahmen:**
	Kontrolle der Ergebnisse durch die Kunden im Rahmen der Auftragsverarbeitung

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

Folgende Sicherheitsmaßnahmen (**Verfügbarkeitskontrolle**) haben wir gegen zufällige oder mutwillige Zerstörung und gegen Verlust bzw. Sabotage von Daten ergriffen:
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen:	**Organisatorische Maßnahmen:**
Recovery Maßnahmen von AWS, OpenAi und Google (SaaS) – keine eigenen Server bei Qodia	Backup & Recovery-Konzept (ausformuliert)
	Kontrolle des Sicherungsvorgangs

Überprüfung, und Evaluierung der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1d DSGVO)

Folgende Maßnahmen treffen wir (**Organisationskontrolle**) um den Datenschutzanforderungen gerecht zu werden:
Es ist zu gewährleisten, dass Verantwortlichkeiten festgelegt und die technischen und organisatorischen Maßnahmen regelmäßig überprüft und evaluiert werden.

Technische Maßnahmen:	**Organisatorische Maßnahmen:**
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf	Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
	Regelmäßige Sensibilisierung der Mitarbeiter
	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
	AV-Verträge bzw. DPA mit AWS, Google und OpenAi

Incident-Management-System (IMS)

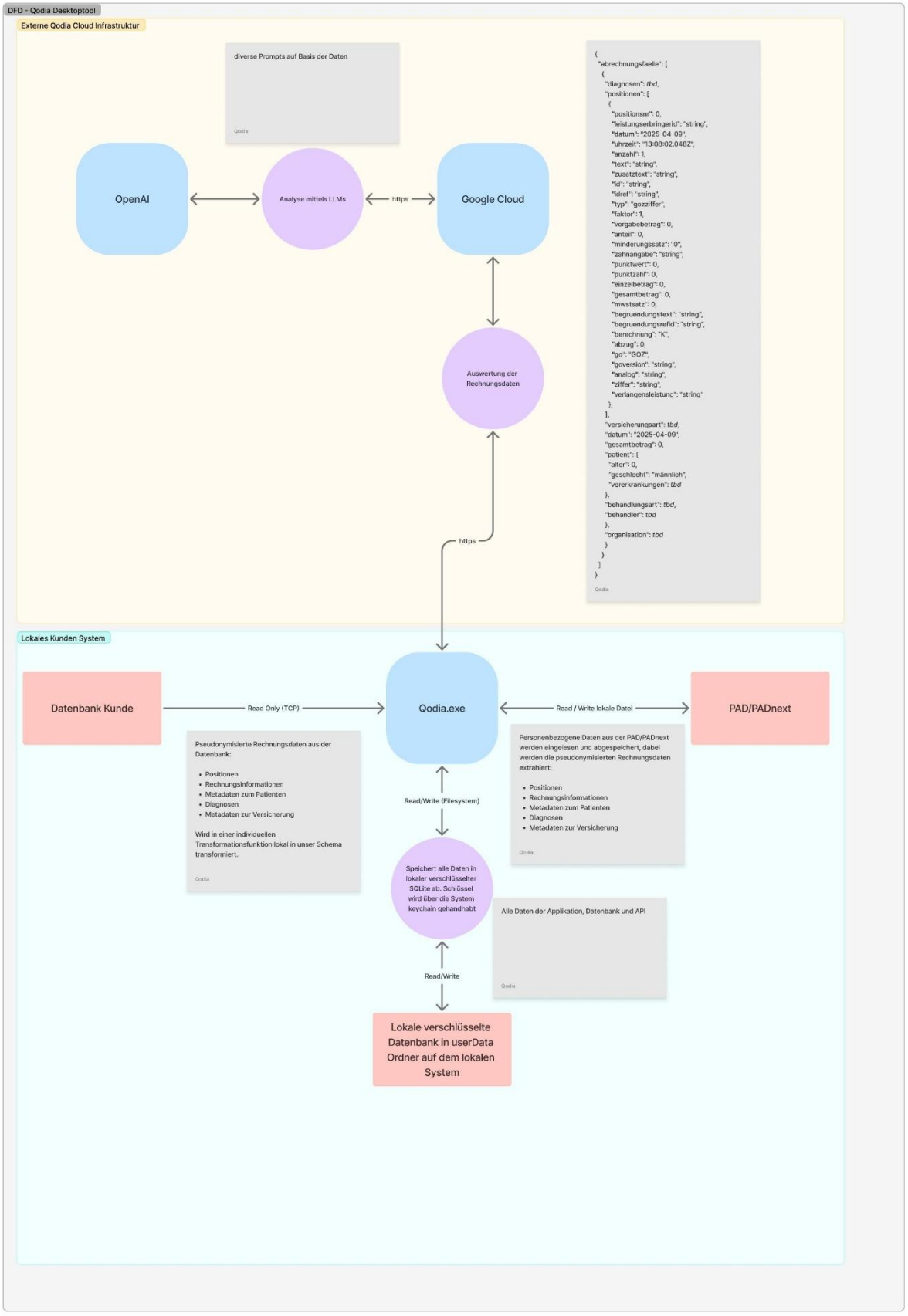
Überwachung und Management der gesamten organisatorischen und technischen IT-Prozesse und der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Betriebsstörungen in IT-Bereichen (**Incident-Management-System**):
Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

Technische Maßnahmen:	**Organisatorische Maßnahmen:**
Einsatz von Firewall und regelmäßige Aktualisierung	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

Bei der Entwicklung und Programmierung berücksichtigen wir folgende Punkte um die Forderungen (**privacy by design und by default**) nachzukommen:

Technische Maßnahmen:	**Organisatorische Maßnahmen:**
	Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
	Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen


DFD - Qodia Desktoptool
Externe Qodia Cloud Infrastruktur
diverse Prompts auf Basis der Daten
Qodia
OpenAI
Analyse mittels LLMs
https
Google Cloud
Auswertung der Rechnungsdaten
https
{
"abrechnungsfaelle": [
{
"diagnosen": tbd,
"positionen": [
{
"positionsnr": 0,
"leistungserbringerid": "string",
"datum": "2025-04-09",
"uhrzeit": "13:08:02.048Z",
"anzahl": 1,
"text": "string",
"zusatztext": "string",
"id": "string",
"idref": "string",
"typ": "gozziffer",
"faktor": 1,
"vorgabebetrag": 0,
"anteil": 0,
"minderungssatz": "0",
"zahnangabe": "string",
"punktwert": 0,
"punktzahl": 0,
"einzelbetrag": 0,
"gesamtbetrag": 0,
"mwstsatz": 0,
"begruendungstext": "string",
"begruendungsrefid": "string",
"berechnung": "K",
"abzug": 0,
"go": "GOZ",
"goversion": "string",
"analog": "string",
"ziffer": "string",
"verlangensleistung": "string"
},
],
"versicherungsart": tbd,
"datum": "2025-04-09",
"gesamtbetrag": 0,
"patient": {
"alter": 0,
"geschlecht": "männlich",
"vorerkrankungen": tbd
},
"behandlungsart": tbd,
"behandler": tbd
},
"organisation": tbd
}
}
]
}
Qodia
Lokales Kunden System
Datenbank Kunde
Read Only (TCP)
Qodia.exe
Read / Write lokale Datei
PAD/PADnext
Pseudonymisierte Rechnungsdaten aus der Datenbank:
Positionen
Rechnungsinformationen
Metadaten zum Patienten
Diagnosen
Metadaten zur Versicherung
Wird in einer individuellen Transformationsfunktion lokal in unser Schema transformiert.
Qodia
Personenbezogene Daten aus der PAD/PADnext werden eingelesen und abgespeichert, dabei werden die pseudonymisierten Rechnungsdaten extrahiert:
Positionen
Rechnungsinformationen
Metadaten zum Patienten
Diagnosen
Metadaten zur Versicherung
Qodia
Read/Write (Filesystem)
Speichert alle Daten in lokaler verschlüsselter SQLite ab. Schlüssel wird über die System keychain gehandhabt
Alle Daten der Applikation, Datenbank und API
Qodia
Read/Write
Lokale verschlüsselte Datenbank in userData Ordner auf dem lokalen System

Anlage 3 zum Auftragsverarbeitungsvertrag zwischen dem Auftraggeber und der Qodia GmbH (Auftragnehmer)

Verzeichnis zu Standorten der Geschäftsräume des Auftragnehmers

Aus der Übersicht sollen alle Standorte der Geschäftsräume des Auftragnehmers hervorgehen, welche für die Erhebung, Verarbeitung und Nutzung der Daten des Auftraggebers im Rahmen des vereinbarten Auftragsverhältnisses genutzt werden. Nicht enthalten sind die Standorte eventueller Unterauftragnehmer.

Standorte	**postalische Anschrift**	**Telefonnummer/ Fax-Nr./ E-Mail-Adresse**
Qodia GmbH	Heimhuder Straße 36 20148 Hamburg	Telefon: +49 151 1531 1887 E-Mail: info@qodia.de
Gibt es weitere Standorte für diese Auftragsverarbeitung sind diese bei den Unterauftragnehmern in Anlage 1 zu diesem AV-Vertrag erwähnt.		

Anlage 4 zum Auftragsverarbeitungsvertrag
zwischen dem Auftraggeber
und der Qodia GmbH (Auftragnehmer)

Ansprechpartner des **Auftragnehmers** ist/sind:

Fachliche Zuständigkeit:	
Name, Vorname:	Ole Reinpold
Funktionsbezeichnung:	Geschäftsführung
E-Mail:	ole.reinpold@qodia.de
Telefon:	+49 151 1531 1887

Ansprechpartner des **Auftraggebers** ist/sind:

Fachliche Zuständigkeit:	
Name, Vorname:	
Funktionsbezeichnung:	
E-Mail:	
Telefon:	

Datenschutzbeauftragter:	
Name, Vorname:	
Funktionsbezeichnung:	
Adresse:	
Kontaktdaten:	