Vertrag über die Auftragsverarbeitung personenbezogener Daten (AVV) - Qualu

Version 1.1 - Stand und Wirksamkeit: 28.10.2026

Version 1.1 ersetzt Version 1.0 für Auftraggeber, die Version 1.1 elektronisch annehmen, und gilt für alle ab dem 28.10.2026 neu geschlossenen Verträge. Für Auftraggeber, die ausschließlich Version 1.0 angenommen haben, gilt Version 1.0 fort; Funktionen, die nach Ziffer 3.7 die Annahme von Version 1.1 voraussetzen, stehen erst nach deren Annahme zur Verfügung.

Auftragnehmer: Mohamed Achach, handelnd unter MAC Digital Ventures, Cosimastraße 121, 81925 München, Deutschland
Kontakt: contact@qualu.ai

Auftraggeber: Der jeweilige Geschäftskunde von Qualu, dessen Rechtsträger, Anschrift und vertretungsberechtigte bzw. zum Vertragsschluss autorisierte Person im Qualu-Konto und im elektronischen Annahmenachweis dokumentiert sind. Der Annahmenachweis ist Bestandteil dieses AVV.

Dieser AVV gilt ausschließlich im B2B-Verhältnis und wird Bestandteil des jeweiligen Qualu-SaaS-Vertrags, sobald er durch einen hierzu autorisierten Nutzer des Auftraggebers elektronisch angenommen wird.

1. Geltungsbereich und Form

1.1. Dieser Vertrag regelt die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO im Zusammenhang mit der Bereitstellung und Nutzung von Qualu.

1.2. Er gilt für alle Verarbeitungstätigkeiten, bei denen der Auftragnehmer oder von ihm eingesetzte Unterauftragsverarbeiter personenbezogene Daten des Auftraggebers zur Erbringung der Qualu-Leistungen verarbeiten.

1.3. Begriffe werden entsprechend der DSGVO verwendet. Weisungen, Genehmigungen, Mitteilungen und Vertragsänderungen können in Textform oder in sonstiger elektronischer Form erfolgen, sofern Inhalt, Erklärender, Zeitpunkt und Bezug zum jeweiligen Vertragsstand angemessen nachweisbar sind. Zwingende gesetzliche Formvorschriften bleiben unberührt.

1.4. Dieser AVV kann elektronisch geschlossen werden. Qualu dokumentiert bei elektronischer Annahme insbesondere den Auftraggeber, den handelnden Nutzer, dessen bestätigte Vertretungsbefugnis, den UTC-Zeitpunkt, die AVV-Version und den Bezug zur jeweiligen Subscription bzw. Bestellung.

2. Gegenstand und Dauer der Verarbeitung

2.1. Gegenstand ist die Bereitstellung und der Betrieb der B2B-SaaS Qualu für den dem Auftraggeber zugeordneten Workspace. Qualu unterstützt Immobilienunternehmen bei Erfassung, Strukturierung und Qualifizierung von Immobilienanfragen sowie bei der Ableitung nächster menschlich kontrollierter Schritte.

2.2. Grundlage der Verarbeitung sind der jeweilige Qualu-SaaS-Vertrag, die anwendbaren B2B-AGB und die dokumentierten Weisungen des Auftraggebers.

2.3. Die Verarbeitung beginnt mit Wirksamwerden des Hauptvertrags bzw. dieses AVV und dauert grundsätzlich für die Laufzeit des Hauptvertrags. Rückgabe-, Lösch- und gesetzliche Aufbewahrungspflichten nach Vertragsende bleiben unberührt.

3. Art, Zweck, Datenarten und betroffene Personen

3.1. Qualu verarbeitet im Auftrag insbesondere Immobilienanfragen und dazugehörige Lead-, Intake-, Listing-, Qualifizierungs- und Workflowdaten. Die Verarbeitung kann über öffentliche Intake-Formulare, Intake-Links, öffentliche Workspace-Seiten, Website-Einbettungen und optional über KI-gestützte Intake- oder Qualifizierungsfunktionen ausgelöst werden.

3.2. Die Verarbeitung umfasst insbesondere Erheben, Erfassen, Validieren, Ordnen, Strukturieren, Speichern, Anzeigen, Durchsuchen, Auswerten, Qualifizieren, Zusammenfassen, Übermitteln an genehmigte Unterauftragsverarbeiter, Exportieren, Einschränken und Löschen.

3.3. Zweck ist die Bearbeitung und Qualifizierung von Immobilienanfragen, einschließlich der Bewertung von Vollständigkeit und Kontext, Budget- und Finanzierungsbereitschaft, Qualifikationsergebnissen, Begründungen, Zusammenfassungen, Prioritäts- oder Dringlichkeitshinweisen und empfohlenen nächsten Schritten. Weitere Zwecke sind Workspace- und Benutzerverwaltung, Export, Löschung, transaktionale Kommunikation, die Kommunikation mit anfragenden Personen im Namen und auf Weisung des Auftraggebers ausschließlich zu ihrer jeweiligen Anfrage (insbesondere Bestätigungen sowie Rückfragen zu unklaren oder unvollständigen Angaben; keine Werbung), Sicherheit und Missbrauchsprävention. Entscheidungen über die weitere Bearbeitung verbleiben beim Auftraggeber und seinen berechtigten Nutzern.

3.4. Verarbeitete Datenarten sind insbesondere Namen, E-Mail-Adressen, Telefonnummern, Anfrage- und Kontaktdaten, Immobilien- und Suchkriterien, kundenindividuelle Intake-Antworten, Freitextinhalte, Budget- und Finanzierungsbereitschaft, Quellen- und Kampagnenzuordnung, Einwilligungs- und Sicherheitsmetadaten, Versionen der angezeigten Hinweise, Kontaktanfragen und KI-Wahl, Rückfragen und Antworten auf Rückfragen einschließlich ihrer Herkunft, Versand- und Zustellstatus von E-Mails an anfragende Personen, Abbestellungen und Widersprüche, Workflow- und Auditdaten, KI-generierte Qualifikationsergebnisse, Zusammenfassungen, Begründungen und Handlungsempfehlungen sowie - soweit einschlägig - Kennungen, Rollen und Aktivitätsdaten berechtigter Workspace-Nutzer, technische Request-Metadaten und vom Auftraggeber bereitgestellte Immobilienbilder. Karten- und Bankzahlungsdaten gehören nicht zu den regulären, im Auftrag verarbeiteten Lead-Daten.

3.5. Betroffene Personen sind insbesondere Personen, die Immobilienanfragen über einen Workspace des Auftraggebers übermitteln, Interessenten bzw. potenzielle Käufer, Personen, deren Daten der Auftraggeber in Anfrage- oder Lead-Datensätze einträgt, sowie berechtigte Workspace-Nutzer und eingeladene Mitglieder des Auftraggebers, soweit deren Daten verarbeitet werden.

3.6. Qualu ist nicht dafür vorgesehen, besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO oder Daten nach Art. 10 DSGVO gezielt zu erheben. Der Auftraggeber darf deren gezielte Erhebung oder Übermittlung nicht konfigurieren oder veranlassen, sofern dies nicht zuvor ausdrücklich vereinbart und rechtlich zulässig ist. Eine unerwartete Eingabe solcher Daten in Freitextfeldern kann technisch nicht vollständig ausgeschlossen werden und ist nach dokumentierter Weisung des Auftraggebers sowie den anwendbaren Datenschutzanforderungen zu behandeln.

3.7. Kommunikation mit anfragenden Personen. Funktionen, mit denen Qualu im Namen des Auftraggebers Rückfragen oder vergleichbare Nachrichten an anfragende Personen versendet (insbesondere „Autopilot"), werden nur nach Annahme dieser Version 1.1, nach Annahme der in Qualu angezeigten Nutzungsbedingungen für diese Funktion und nach ausdrücklicher Aktivierung durch einen berechtigten Nutzer des Auftraggebers bereitgestellt. Solche Nachrichten

1. richten sich nur an Personen, die bei Absenden ihrer Anfrage um Kontaktaufnahme zu dieser Anfrage gebeten haben, und betreffen ausschließlich diese Anfrage;
2. enthalten keine Werbung, insbesondere keine weiteren Angebote oder Objekte, keine Newsletter, keine Zufriedenheits- oder Bewertungsanfragen und keine Werbung für Qualu;

3. nennen den Auftraggeber als Verantwortlichen und bieten eine Möglichkeit, weitere Rückfragen abzubestellen oder menschlichen Kontakt zu verlangen;
4. beruhen auf den von Qualu bereitgestellten, inhaltlich begrenzten Vorlagen.

Abbestellungen, Widersprüche und Einschränkungen, die über die vorgesehenen Wege eingehen, setzt Qualu technisch um; danach werden keine weiteren automatisierten Rückfragen zu der betreffenden Anfrage versendet.

3.8. Qualifizierungsergebnisse und KI. Scores, Status, Begründungen, Zusammenfassungen und Empfehlungen sind Entscheidungshilfen für den Auftraggeber. Qualu trifft keine Entscheidungen gegenüber anfragenden Personen, lehnt Anfragen nicht automatisiert ab und teilt anfragenden Personen keine Qualifizierungsergebnisse mit. Der Auftraggeber stellt sicher, dass über die weitere Bearbeitung einer Anfrage ein Mensch entscheidet, und verwendet Qualifizierungsergebnisse nicht als alleinige Grundlage für Entscheidungen, die anfragende Personen rechtlich oder in ähnlicher Weise erheblich beeinträchtigen (Art. 22 DSGVO). KI-Funktionen werden nach dem in der Qualu-Vorlage für Käuferhinweise beschriebenen Modell bereitgestellt: das KI-Interview nur nach Einwilligung der anfragenden Person; KI-gestützte Analyse auf Grundlage der berechtigten Interessen des Auftraggebers mit Widerspruchsmöglichkeit. Anfragen, die unter dem früheren Hinweis „ohne KI-Verarbeitung" eingegangen sind, sowie Anfragen mit Widerspruch oder Einschränkung werden nicht mit KI verarbeitet. Auftragsdaten werden nicht zum Training von KI-Modellen verwendet.

3.9. Käuferhinweise und Rechtsidentität. Qualu stellt für Anfrageformulare eine Vorlage für Datenschutzhinweise nach Art. 13 DSGVO sowie die zugehörigen Bestätigungstexte bereit, die den Auftraggeber als Verantwortlichen nennen. Die Vorlage ist ein technisches Hilfsmittel und keine Rechtsberatung. Der Auftraggeber prüft, ob die Vorlage und das darin beschriebene Rechtsgrundlagenmodell, einschließlich der Interessenabwägung für die KI-gestützte Analyse, auf seine Verarbeitung zutreffen, ergänzt eigene Hinweise, soweit erforderlich, und hält die in Qualu hinterlegten Angaben zu Rechtsträger, Anschrift und Datenschutzkontakt vollständig und richtig. Fehlen diese Angaben, kann Qualu Funktionen nach Ziffer 3.7 sperren.

3.10. Unzulässige Weisungen. Der Auftraggeber wird Qualu nicht anweisen oder so konfigurieren, dass (a) Werbung an anfragende Personen versendet wird, (b) besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO oder Daten nach Art. 10 DSGVO gezielt erfragt werden, (c) Anfragen automatisiert abgelehnt oder anfragenden Personen automatisiert Entscheidungen mitgeteilt werden oder (d) anfragende Personen nach Abbestellung, Widerspruch oder Bitte um menschlichen Kontakt weiter automatisiert kontaktiert werden. Qualu darf technische Begrenzungen vorsehen, die solche Verarbeitungen verhindern. Ziffer 10.3 bleibt unberührt.

4. Pflichten des Auftragnehmers

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers und zur Erbringung der vereinbarten Leistungen, es sei denn, eine gesetzliche Verpflichtung erfordert eine andere Verarbeitung. Soweit gesetzlich zulässig, informiert der Auftragnehmer den Auftraggeber vor einer solchen abweichenden Verarbeitung.

4.2. Der Auftragnehmer wahrt die Vertraulichkeit und stellt sicher, dass Personen mit Zugriff auf im Auftrag verarbeitete Daten angemessen zur Vertraulichkeit verpflichtet sind.

4.3. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen angemessen bei Betroffenenrechten, Datenschutz-Folgenabschätzungen sowie den Pflichten nach Art. 32 bis 36 DSGVO. Hierzu stellt der Auftragnehmer auf Anfrage insbesondere eine Beschreibung der Verarbeitung, eine Vorlage zur Interessenabwägung für die KI-gestützte Analyse und ein Unterstützungspaket für Datenschutz-Folgenabschätzungen zur Verfügung.

4.4. Direkt an den Auftragnehmer gerichtete Betroffenenanfragen, die Daten des Auftraggebers betreffen, werden dem Auftraggeber unverzüglich zugeleitet. Eine inhaltliche Beantwortung erfolgt grundsätzlich nur auf Weisung oder mit Zustimmung des Auftraggebers, soweit keine eigene gesetzliche Verpflichtung des Auftragnehmers besteht.

4.5. Derzeit ist kein Datenschutzbeauftragter benannt. Die gesetzliche Benennungspflicht wird bei wesentlichen Änderungen von Umfang, Art oder Zweck der Verarbeitung oder sonstigen relevanten Voraussetzungen erneut geprüft.

4.6. Verarbeitungen außerhalb der EU/des EWR oder eines Staates mit Angemessenheitsbeschluss erfolgen nur, soweit die Voraussetzungen des Kapitels V DSGVO erfüllt sind.

5. Technische und organisatorische Maßnahmen

5.1. Die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen bilden den vereinbarten Mindeststandard. Sie dürfen an technische Entwicklungen angepasst werden, sofern das Schutzniveau insgesamt nicht abgesenkt wird.

5.2. Kundendaten werden in der mandantenfähigen SaaS logisch von Daten anderer Kunden getrennt. Der Zugriff wird über Authentifizierung, workspacebezogene Rollen und Berechtigungen sowie serverseitige Zugriffskontrollen beschränkt.

5.3. Unnötige lokale Kopien von Kundendatenbanken werden nicht erstellt. Technisch erforderliche Kopien oder Replikate können insbesondere im Rahmen von Provider-Backups, Replikation, Betriebs- und Sicherheitslogs, temporärer Verarbeitung, E-Mail-Versand sowie vom Auftraggeber angeforderten Exporten entstehen. Solche Kopien unterliegen den jeweils anwendbaren Sicherheits- und Löschregeln. Vom Auftraggeber heruntergeladene Exporte liegen außerhalb der Kontrolle des Auftragnehmers.

5.4. Die Administration kann aus einem abgesicherten Homeoffice erfolgen. Dabei werden ausschließlich geschäftlich genutzte, zugriffsgeschützte und verschlüsselte Endgeräte sowie gesicherte Netzwerkverbindungen eingesetzt. Kundendatenbank-Exporte werden im Regelbetrieb nicht lokal gespeichert; Kundendaten werden nicht auf Wechselmedien kopiert und nicht ausgedruckt.

5.5. Dedizierte physische Datenträger des Auftraggebers werden im Regelbetrieb nicht eingesetzt.

5.6. Der Auftraggeber kann die Einhaltung dieses AVV in angemessenem Umfang überprüfen. Prüfungen erfolgen grundsätzlich evidenzbasiert durch aktuelle TOM-Dokumentation, relevante Nachweise, Prüfberichte, Zertifizierungen, schriftliche Auskünfte oder Remote-Prüfungen. Soweit dies im Einzelfall nicht ausreicht und eine weitergehende Prüfung nach Art. 28 Abs. 3 lit. h DSGVO erforderlich ist, ermöglicht bzw. unterstützt der Auftragnehmer eine angemessene Prüfung. Dabei sind Vertraulichkeit, Sicherheit, Rechte anderer Kunden, Schutz von Zugangsdaten und Geschäftsgeheimnissen sowie ein störungsarmer Betrieb zu berücksichtigen. Unkontrollierte Zugriffe auf Produktivsysteme, Zugangsdaten oder Daten anderer Kunden sowie Penetrationstests ohne vorherige ausdrückliche Freigabe sind ausgeschlossen.

6. Berichtigung, Löschung und Einschränkung

6.1. Im Auftrag verarbeitete Daten werden entsprechend diesem Vertrag und dokumentierten Weisungen des Auftraggebers berichtigt, gelöscht oder in ihrer Verarbeitung eingeschränkt.

6.2. Weisungen nach Vertragsende werden nur insoweit ausgeführt, wie die betreffenden Daten noch rechtmäßig und technisch im Einflussbereich des Auftragnehmers vorhanden sind und keine vorrangige gesetzliche Pflicht entgegensteht.

7. Unterauftragsverhältnisse

7.1. Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine vorherige Genehmigung zum Einsatz der in Anlage 2 bzw. der jeweils versionierten öffentlichen Unterauftragsverarbeiterliste aufgeführten Unterauftragsverarbeiter. Der zum Zeitpunkt der elektronischen Annahme dokumentierte Stand ist Bestandteil dieses AVV.

7.2. Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich zu Datenschutzpflichten, die hinsichtlich der Verarbeitung im Auftrag den Anforderungen des Art. 28 DSGVO entsprechen, und bleibt im gesetzlich vorgesehenen Umfang für deren Erfüllung verantwortlich.

7.3. Beabsichtigt der Auftragnehmer, einen Unterauftragsverarbeiter hinzuzufügen oder zu ersetzen, informiert er den Auftraggeber grundsätzlich mindestens 14 Kalendertage vor Beginn der betreffenden Verarbeitung per E-Mail an den dokumentierten Kunden- bzw. Weisungskontakt. Bei zwingenden Sicherheits-, Rechts- oder Verfügbarkeitsgründen kann die Frist angemessen verkürzt werden; die Information erfolgt dann so früh wie vernünftigerweise möglich.

7.4. Der Auftraggeber kann innerhalb der Mitteilungsfrist aus nachvollziehbaren datenschutzrechtlichen Gründen widersprechen. Die Parteien bemühen sich um eine zumutbare Lösung. Ist eine solche Lösung ohne den betreffenden Unterauftragsverarbeiter nicht möglich, kann der Auftragnehmer die betroffene Leistung einstellen oder der betroffene Leistungsteil bzw. der Hauptvertrag nach den anwendbaren Vertragsregeln beendet werden.

7.5. Soweit Verarbeitungen in Drittländern stattfinden, stellt der Auftragnehmer sicher, dass ein zulässiger Übermittlungsmechanismus nach Kapitel V DSGVO besteht.

8. Rechte und Pflichten des Auftraggebers

8.1. Der Auftraggeber ist für die Rechtmäßigkeit der beauftragten Verarbeitung, die Rechtsgrundlagen, Informationspflichten und die Wahrung der Betroffenenrechte verantwortlich. Dazu gehört auch die Prüfung, ob eine Datenschutz-Folgenabschätzung erforderlich ist, insbesondere beim Einsatz von KI-Funktionen, und gegebenenfalls deren Durchführung.

8.2. Weisungen werden dokumentiert erteilt. Elektronische Weisungen über verifizierte Kontakt- oder Kontowege genügen. Mündliche Weisungen in dringenden Fällen sind unverzüglich nachträglich zu dokumentieren.

8.3. Der Auftraggeber informiert den Auftragnehmer unverzüglich über erkannte Fehler, Unregelmäßigkeiten, unzulässige Weisungen oder sonstige Umstände, die die Verarbeitung beeinflussen können.

8.4. Der Auftragnehmer stellt die nach Art. 28 Abs. 3 lit. h DSGVO erforderlichen Informationen bereit und ermöglicht bzw. unterstützt erforderliche Prüfungen nach dem in Ziffer 5.6 beschriebenen angemessenen und sicheren Verfahren.

9. Datenschutzverletzungen

9.1. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Verletzungen des Schutzes personenbezogener Daten, die Daten des Auftraggebers betreffen. Eine erste Mitteilung erfolgt spätestens innerhalb von 24 Stunden ab dem Zeitpunkt, zu dem der Auftragnehmer Kenntnis von Tatsachen erlangt, die vernünftigerweise auf eine relevante Verletzung schließen lassen. Diese Frist ist eine vertragliche Prozessor-zu-Verantwortlichem-Frist und verändert nicht die gesetzlichen Meldefristen des Auftraggebers gegenüber Aufsichtsbehörden.

9.2. Die Erstmitteilung enthält die zu diesem Zeitpunkt verfügbaren Informationen zu Art und Umfang des Vorfalls, betroffenen Datenkategorien und Personengruppen, wahrscheinlichen Folgen, Kontaktstelle sowie

getroffenen oder vorgeschlagenen Abhilfemaßnahmen. Noch nicht verfügbare Informationen werden nachgeliefert.

9.3. Primäre Kontaktstelle des Auftragnehmers für Datenschutzvorfälle ist contact@qualu.ai.

9.4. Der Auftragnehmer unterstützt den Auftraggeber im erforderlichen Umfang bei dessen Pflichten nach Art. 33 und 34 DSGVO.

10. Weisungen

10.1. Der Auftraggeber behält hinsichtlich der Verarbeitung im Auftrag das Weisungsrecht im Rahmen des Hauptvertrags, dieses AVV und des anwendbaren Rechts.

10.2. Weisungsberechtigte bzw. Weisungskontakte werden über den elektronischen Annahmenachweis oder das hierfür vorgesehene Qualu-Konto dokumentiert. Änderungen sind in nachweisbarer Form mitzuteilen.

10.3. Hält der Auftragnehmer eine Weisung für datenschutzrechtlich unzulässig, informiert er den Auftraggeber unverzüglich und kann die Ausführung aussetzen, bis die Weisung bestätigt, geändert oder anderweitig rechtlich geklärt wurde. Eine umfassende materiell-rechtliche Prüfungspflicht des Auftragnehmers wird dadurch nicht begründet.

10.4. Einstellungen, die ein berechtigter Nutzer des Auftraggebers in Qualu vornimmt und die die Verarbeitung ändern, gelten als dokumentierte Weisungen des Auftraggebers. Das betrifft insbesondere die Aktivierung, Deaktivierung und den Modus von Funktionen nach Ziffer 3.7, KI-Funktionen, Absender- und Antwortadressen, die Rechtsidentität nach Ziffer 3.9 sowie Aufbewahrungseinstellungen. Änderungen an Funktionen nach Ziffer 3.7, an der Rechtsidentität und an Aufbewahrungseinstellungen protokolliert Qualu mit Zeitpunkt und handelndem Nutzer.

11. Beendigung, Rückgabe und Löschung

11.1. Bei Beendigung der Leistungen entscheidet der Auftraggeber, ob die im Auftrag verarbeiteten Daten zurückgegeben oder gelöscht werden. Soweit technisch vorgesehen, kann der Auftraggeber vor Vertragsende einen Workspace-Export anfordern. Erfolgt bis zum Wirksamwerden der Beendigung keine abweichende dokumentierte Weisung zur Rückgabe, gilt die Löschung nach dieser Ziffer als vereinbart.

11.2. Aktive, von Qualu kontrollierte Auftragsdaten werden grundsätzlich innerhalb von 30 Kalendertagen nach wirksamer Vertragsbeendigung oder nach einer wirksamen Löschweisung gelöscht, soweit keine andere dokumentierte Weisung oder gesetzliche Pflicht gilt.

11.3. Providerseitige Backups, Replikate, Sicherheits- und Betriebslogs sowie vergleichbare technisch notwendige Kopien können bis zum Ablauf der jeweiligen providerseitigen Lösch- oder Überschreibzyklen fortbestehen. Der Auftragnehmer berücksichtigt deren Löschung im Rahmen seiner vertraglichen und technischen Möglichkeiten und macht keine Zusage einer sofortigen physischen Vernichtung sämtlicher Providerkopien.

11.4. Vom Auftraggeber heruntergeladene Exporte liegen außerhalb der Kontrolle des Auftragnehmers. Daten, die der Auftragnehmer für eigene gesetzliche oder vertragliche Zwecke als Verantwortlicher benötigt, insbesondere Vertrags-, Abrechnungs-, Steuer-, Sicherheits-, Rechtsnachweis- oder Compliance-Unterlagen, werden getrennt von den Auftragsdaten und nur für den jeweiligen eigenen Zweck und die dafür geltende Aufbewahrungsdauer verarbeitet.

11.5. Soweit keine physischen Datenträger verarbeitet werden, werden keine physischen Vernichtungsverfahren zugesagt. Der Auftragnehmer kann auf Anfrage einen angemessenen Nachweis über die durchgeführte Löschung der von ihm kontrollierten Auftragsdaten bereitstellen.

11.6. Während der Vertragslaufzeit legt der Auftraggeber die Speicherdauer der Auftragsdaten fest. Ohne abweichende Weisung gelten die in Qualu dokumentierten Standardfristen; derzeit werden Anfragen, die nicht als gewonnen markiert sind, 24 Monate nach Eingang durch einen täglichen Löschlauf gelöscht. Qualu kann weitere Standardfristen, insbesondere für gewonnene Anfragen, einführen; der Auftraggeber wird hierüber mindestens 60 Tage vor der ersten danach erfolgenden Löschung informiert und kann zuvor exportieren oder im vorgesehenen Rahmen eine abweichende Frist festlegen. Gesetzliche Aufbewahrungspflichten des Auftraggebers, insbesondere handels-, steuer-, gewerbe- und geldwäscherechtliche Pflichten, erfüllt dieser eigenverantwortlich, gegebenenfalls durch Export. Qualu ist kein Archivsystem im Sinne dieser Pflichten. Nachweise über angezeigte Hinweise, Kontaktanfragen, Einwilligungen, Abbestellungen und Widersprüche werden für die Dauer der Speicherung der jeweiligen Anfrage aufbewahrt.

12. Vergütung

12.1. Die gewöhnliche Erfüllung der gesetzlichen und vertraglichen Pflichten dieses AVV ist mit der Vergütung des Hauptvertrags abgegolten.

12.2. Für außergewöhnliche, kundenspezifische Unterstützungsleistungen, die über den üblichen und gesetzlich geschuldeten Umfang hinausgehen, kann eine gesonderte angemessene Vergütung vereinbart werden. Gesetzlich zwingende Pflichten des Auftragnehmers werden dadurch nicht eingeschränkt. Soweit der Mehraufwand durch einen vom Auftragnehmer zu vertretenden Vertrags- oder Datenschutzverstoß verursacht wurde, wird hierfür keine zusätzliche Vergütung verlangt.

13. Haftung

13.1. Die Haftung der Parteien für Verstöße gegen die DSGVO richtet sich insbesondere nach Art. 82 DSGVO und dem sonst anwendbaren Recht.

13.2. Der Auftragnehmer haftet für durch eine Verarbeitung verursachte Schäden gegenüber betroffenen Personen im Rahmen des Art. 82 DSGVO, soweit er gegen speziell ihm als Auftragsverarbeiter auferlegte Pflichten verstoßen oder außerhalb bzw. entgegen rechtmäßigen Weisungen des Auftraggebers gehandelt hat.

13.3. Soweit Auftraggeber und Auftragnehmer gegenüber einer betroffenen Person nach Art. 82 DSGVO gemeinsam haften, bleiben gesetzliche Außenhaftung und vollständiger Schadensersatz unberührt. Im Innenverhältnis erfolgt ein Ausgleich entsprechend dem jeweiligen Verantwortungsanteil, soweit gesetzlich zulässig.

13.4. Weitergehende vertragliche Haftungsregelungen des Hauptvertrags bleiben unberührt, soweit sie mit zwingendem Datenschutzrecht vereinbar sind.

14. Sonderkündigungsrecht

14.1. Der Auftraggeber kann den Hauptvertrag und dieses AVV aus wichtigem Grund außerordentlich kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder dieses AVV vorliegt, eine rechtmäßige Weisung dauerhaft nicht ausgeführt werden kann oder Kontrollrechte vertragswidrig verweigert werden.

14.2. Bei behebbaren, nicht schwerwiegenden Verstößen ist grundsätzlich zunächst eine angemessene Frist zur Abhilfe zu setzen, soweit dies nach Art und Risiko des Verstoßes zumutbar ist.

14.3. Ein nach Ziffer 7.4 nicht lösbarer, begründeter Widerspruch gegen einen neuen Unterauftragsverarbeiter kann hinsichtlich des betroffenen Leistungsteils nach den dort beschriebenen Regeln zu einer Beendigung führen.

15. Sonstiges

15.1. Beide Parteien behandeln Geschäftsgeheimnisse, vertrauliche Informationen und nicht öffentliche Datensicherheitsmaßnahmen der jeweils anderen Partei auch über das Vertragsende hinaus vertraulich.

15.2. Nebenabreden, Änderungen und Ergänzungen dieses AVV können in Textform oder in einer sonstigen elektronischen Form vereinbart werden, die Inhalt, Erklärende, Zeitpunkt und Vertragsversion angemessen nachweisbar macht. Individuelle Vereinbarungen der Parteien bleiben unberührt.

15.3. Ein Zurückbehaltungsrecht an im Auftrag verarbeiteten personenbezogenen Daten wird ausgeschlossen, soweit dem zwingendes Recht nicht entgegensteht.

15.4. Sollten einzelne Bestimmungen dieses AVV unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Zwingende gesetzliche Regelungen gehen vor.

15.5. Anlagen 1 bis 3 sind Bestandteil dieses AVV.

Anlage 1 - Technische und organisatorische Maßnahmen (TOMs)

Die nachfolgenden Maßnahmen beschreiben den für Qualu geltenden Mindeststandard. Technische Details können sich ändern, sofern das Schutzniveau insgesamt nicht abgesenkt wird.

1. **Zugriff und Endgeräte:** Administrative Zugriffe erfolgen nur über zugriffsgeschützte, geschäftlich genutzte und verschlüsselte Endgeräte mit automatischer Sperre und laufenden Sicherheitsupdates.
2. **Authentifizierung und Autorisierung:** Geschützte Funktionen erfordern authentifizierte Sitzungen. Workspace-Zugriffe und Verwaltungsfunktionen werden rollen- und berechtigungsbasiert beschränkt.
3. **Mandantentrennung:** Kundendaten werden logisch nach Workspace getrennt. Serverseitige Zugriffskontrollen und datenbankseitige Schutzmechanismen begrenzen mandantenfremde Zugriffe.
4. **Transportverschlüsselung:** Öffentliche Anwendungs- und Providerverbindungen verwenden verschlüsselte Transportwege (HTTPS/TLS).
5. **Geheimnisse und privilegierte Zugänge:** Privilegierte Zugangsdaten werden serverseitig verwaltet und nicht für öffentliche Client-Anwendungen vorgesehen.
6. **Missbrauchsschutz:** Qualu verwendet technische Schutzmaßnahmen wie Rate Limiting und Bot-/Abuse-Schutz für dafür vorgesehene Abläufe.
7. **Protokollierung:** Relevante Governance-, Sicherheits-, Export- und Löschvorgänge werden in angemessenem Umfang nachvollziehbar protokolliert.
8. **KI-Verarbeitung:** KI-Anbieter werden ausschließlich serverseitig aufgerufen. Vor KI-Aufrufen zu einer Anfrage prüft Qualu Widerspruch, Einschränkung und den bei Eingang angezeigten Hinweisstand und schließt nach Ziffer 3.8 ausgenommene Anfragen aus; bei Prüffehlern unterbleibt der KI-Aufruf. Daten werden je nach Funktion minimiert; KI-Ergebnisse unterstützen die Bearbeitung, ersetzen aber nicht die menschliche Kontrolle des Auftraggebers. Auftragsdaten werden nicht zum Training verwendet.
9. **Datensicherung und Verfügbarkeit:** Qualu nutzt verwaltete Hosting-, Datenbank-, Authentifizierungs- und Storage-Dienste. Providerseitige Backup- und Wiederherstellungsmechanismen richten sich nach den jeweils eingesetzten Diensten und Tarifen.
10. **Export und Löschung:** Berechtigte Nutzer können vorgesehene Export- und Löschfunktionen nutzen. Vertragsbeendigungen werden über einen kontrollierten, dokumentierten Löschprozess abgewickelt.
11. **Incident Response:** Für Datenschutzvorfälle besteht ein dokumentiertes Verfahren mit Eindämmung, Beweissicherung, Bewertung und Kundenkommunikation.
12. **Sichere Entwicklung:** Änderungen an Anwendung und Datenbankschema werden versioniert und durch automatisierte Prüfungen und Tests unterstützt.

13. **Homeoffice und lokale Datenhaltung:** Homeoffice-Administration ist zulässig, sofern die beschriebenen Zugriffsschutzmaßnahmen eingehalten werden. Kundendatenbank-Exporte werden im Regelbetrieb nicht lokal gespeichert; Wechselmedien und Ausdrucke werden für Kundendaten nicht verwendet.
14. **Unterauftragsverarbeiter:** Eingesetzte Unterauftragsverarbeiter werden dokumentiert, vertraglich eingebunden und nach Ziffer 7 dieses AVV verwaltet.
15. **Nachweise bei Anfragen:** Die Version der angezeigten Hinweise, die Kontaktanfrage und die KI-Wahl werden serverseitig je Anfrage mit Zeitpunkt gespeichert; vom Browser übermittelte Versionsangaben werden für aktuelle Formulare nicht übernommen.
16. **Kommunikation mit anfragenden Personen:** Soweit Funktionen nach Ziffer 3.7 aktiviert sind, erfolgen Versand und Antwortannahme nur über die Qualu-Infrastruktur auf Grundlage begrenzter Vorlagen, mit befristeten, auf die einzelne Anfrage beschränkten Links, Abbestellmöglichkeit, Versandprotokoll, Begrenzung von Häufigkeit und Anzahl sowie Sperre nach Abbestellung, Widerspruch oder Bitte um menschlichen Kontakt.

Anlage 2 - Aktuelle Unterauftragsverarbeiter

Stand: 28.10.2026 (Unterauftragsverarbeiterliste Version 1.1)

Anbieter	Dienst	Zweck der Verarbeitung	Primärer Standort / Hinweis	Vertrags-/Transfergrundlage
Supabase	Managed PostgreSQL, Auth und Object Storage	Speicherung und Verarbeitung von Workspace-, Lead-, Intake-, Listing-, Nutzer-, Audit- und Bilddaten	Qualu-Primärregion: West EU (Irland); weitere Verarbeitung nach Anbieter-DPA und Subprocessor-Liste	Supabase DPA; anwendbare SCCs bzw. sonstige zulässige Mechanismen
Vercel	Pro Plan - Application Hosting, Server Runtime und Deployment	Bereitstellung der Qualu-Anwendung und serverseitige Verarbeitung von Requests	Verarbeitung nach Vercel DPA und aktueller Subprocessor-Liste	Vercel DPA für Pro; anwendbare SCCs bzw. sonstige zulässige Mechanismen
OpenAI	API	KI-Interview (nur nach Einwilligung der anfragenden Person) sowie KI-gestützte Extraktion, Qualifizierungsunterstützung, Zusammenfassung, Empfehlungen und Auslegung von Antworten auf Rückfragen (berechtigte Interessen des Auftraggebers, Widerspruch möglich; ausgenommene Anfragen nach Ziffer 3.8)	Für EEA-Kunden Vertragspartner OpenAI Ireland Ltd.; weitere Verarbeitung nach OpenAI DPA	OpenAI DPA; anwendbare Angemessenheitsbeschlüsse und/oder SCCs. API-Daten werden standardmäßig nicht zum Training verwendet.
Microsoft	Microsoft 365 / Exchange Online / Microsoft Graph	Transaktionaler E-Mail-Versand, einschließlich E-Mails an anfragende Personen im Namen und auf Weisung des Auftraggebers (Bestätigungen und Rückfragen zur Anfrage, keine Werbung), sowie Mailboxverarbeitung	Nach Microsoft 365 Tenant- und Servicekonfiguration	Microsoft Products and Services DPA; anwendbare Transfermechanismen nach DPA
Upstash	Redis	Rate Limiting und kurzlebige Sicherheits-/Abuse-Counter	Konfigurierte Redis-Region; weitere Verarbeitung nach Anbieter-DPA	Upstash DPA; anwendbare Transfermechanismen nach DPA

Anbieter	Dienst	Zweck der Verarbeitung	Primärer Standort / Hinweis	Vertrags-/Transfergrundlage
Cloudflare	Turnstile	Bot- und Missbrauchsschutz sowie serverseitige Tokenprüfung	Globaler Dienst; Verarbeitung nach Cloudflare DPA	Cloudflare DPA; anwendbare DPF-/SCC-Mechanismen

Die jeweils aktuelle, versionierte Unterauftragsverarbeiterliste wird unter **/de/unterauftragnehmer** veröffentlicht. Änderungen richten sich nach Ziffer 7 dieses AVV.

Anlage 3 - Weisungskontakte

Auftragnehmer: Mohamed Achach, MAC Digital Ventures, contact@qualu.ai.

Auftraggeber: Der beim elektronischen Abschluss bzw. im Qualu-Konto dokumentierte Rechtsträger sowie der dort hinterlegte autorisierte Weisungskontakt. Änderungen des Weisungskontakts sind vom Auftraggeber über den vorgesehenen Kontoweg oder in nachweisbarer Textform mitzuteilen.

Änderungen gegenüber Version 1.0

Ziffern 3.1, 3.3 und 3.4 (Eingangskanäle, Kommunikation mit anfragenden Personen, Datenarten), neue Ziffern 3.7 bis 3.10 (Rückfragen ohne Werbung, Entscheidungshilfe und KI, Käuferhinweise und Rechtsidentität, unzulässige Weisungen), Ziffern 4.3 und 8.1 (Interessenabwägung und Datenschutz-Folgenabschätzung), neue Ziffern 10.4 (Einstellungen als Weisungen) und 11.6 (Aufbewahrung während der Laufzeit), Anlage 1 Nr. 8, 15 und 16, Anlage 2 (Zwecke OpenAI und Microsoft). Es werden keine neuen Unterauftragsverarbeiter eingesetzt.

Version: 1.1
Wirksam ab: 28.10.2026
Vorversion: 1.0 vom 14.09.2026 (PDF: https://www.qualu.ai/legal/qualu-avv-v1.0.pdf)
Veröffentlichung: https://www.qualu.ai/de/avv
Unterauftragsverarbeiter: https://www.qualu.ai/de/unterauftragnehmer