Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO

Version 1.5 · Stand 23.11.2026

Gilt für den Pilotvertrag Qalvy und für spätere kostenpflichtige Abonnements von Qalvy und der Qalcurate-Plattform.

Parteien

Firma _____, Anschrift _____,

vertreten durch Name _____, Funktion _____

– nachfolgend „Verantwortlicher“ –

und

Value4p GmbH, Schulstr. 27, 26759 Hinte, vertreten durch den Geschäftsführer Roland Jungenkrüger, eingetragen im Handelsregister des Amtsgerichts Aurich unter HRB 206940 – nachfolgend „Auftragsverarbeiter“ –

---

§ 1 Gegenstand und Dauer

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen, um Qalvy und die Qalcurate-Plattform bereitzustellen (Hauptvertrag).
2. Dieser AVV gilt, solange der Auftragsverarbeiter Daten aus dem Hauptvertrag verarbeitet. Er gilt einschließlich der Phase für Export und Löschung nach Vertragsende.

§ 2 Art, Zweck und Umfang der Verarbeitung

Punkt	Beschreibung
Zweck	Bereitstellung des KI-Arbeitsplatzes: Chat, Wissensspeicher, Agenten, zeitgesteuerte Abläufe, Sprache und Notizen
Art der Verarbeitung	Erheben, Speichern, Ordnen, Auslesen, Verarbeiten mit KI-Modellen, Übermitteln an Unterauftragsverarbeiter nach Anlage B, auch in Drittländer nach § 7, Löschen
Ort der Verarbeitung	Betrieb und Speicherung in Deutschland. Bei der Nutzung bestimmter KI-Modelle und Dienste werden Daten an Anbieter außerhalb der EU übermittelt, insbesondere in die USA (§ 7, Anlage B).
Arten der Daten	Kontakt- und Kontodaten der Nutzer; Eingaben (Prompts), hochgeladene Dokumente und Ergebnisse; Sprachaufnahmen und Transkripte; Nutzungs- und Protokolldaten
Betroffene Personen	Beschäftigte und Beauftragte des Verantwortlichen; Personen, deren Daten in Eingaben, Dokumenten oder Sprachaufnahmen vorkommen (zum Beispiel Kunden, Lieferanten, Gesprächspartner)

Punkt	Beschreibung
Besondere Kategorien (Art. 9 DSGVO)	Nicht vorgesehen. Der Verantwortliche verarbeitet solche Daten nur nach vorheriger Abstimmung.

§ 3 Weisungen

1. Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf die Übermittlung in ein Drittland. Ausgenommen sind Verarbeitungen, zu denen er nach dem Recht der Union oder eines Mitgliedstaats verpflichtet ist (Art. 28 Abs. 3 lit. a DSGVO). In diesem Fall teilt er dem Verantwortlichen diese Pflicht vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.
2. Der Hauptvertrag und die Einstellungen, die der Verantwortliche in Qalvy vornimmt, gelten als Weisung. Das gilt auch für die Auswahl und Freigabe von KI-Modellen und Suchmaschinen nach § 7 Abs. 8, für die Einstellungen zur Pseudonymisierung (Anlage A Abschnitt 1) und für die Angaben des Verantwortlichen im Onboarding-Fragebogen.
3. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich.
4. Der Auftragsverarbeiter nutzt die Daten nicht für eigene Zwecke. Insbesondere trainiert er mit ihnen keine KI-Modelle. Das gilt auch für alle Unterauftragsverarbeiter.

§ 4 Vertraulichkeit

Der Auftragsverarbeiter setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind.

§ 5 Technische und organisatorische Maßnahmen

1. Der Auftragsverarbeiter trifft die Maßnahmen nach Art. 32 DSGVO, die Anlage A beschreibt. Bei Übermittlungen in Drittländer trifft er zusätzlich die Maßnahmen nach Anlage A, Abschnitt 2.
2. Er darf die Maßnahmen weiterentwickeln, solange das Schutzniveau nicht sinkt.

§ 6 Unterauftragsverarbeiter

1. Der Verantwortliche genehmigt die Unterauftragsverarbeiter, die in Anlage B aufgeführt sind.
2. Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage vorher in Textform, wenn er einen Unterauftragsverarbeiter hinzufügt oder ersetzt. Die Mitteilung nennt auch den Ort der Verarbeitung und die Grundlage einer Drittlandübermittlung.
3. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen. Widerspricht er, setzt der Auftragsverarbeiter den Unterauftragsverarbeiter nicht für die Verarbeitung im Auftrag des Verantwortlichen ein; für andere Kunden darf er ihn weiter einsetzen. Ist die Leistung ohne diesen Unterauftragsverarbeiter nicht vollständig möglich und können sich die Parteien nicht einigen, darf der Verantwortliche den Hauptvertrag außerordentlich kündigen.

4. Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten.
5. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung dieser Pflichten (Art. 28 Abs. 4 Satz 2 DSGVO).
6. Auf Anfrage stellt der Auftragsverarbeiter eine Kopie der Datenschutzvereinbarungen mit den Unterauftragsverarbeitern zur Verfügung, einschließlich der Standardvertragsklauseln nach § 7. Geschäftsgeheimnisse darf er unkenntlich machen.

§ 7 Übermittlung in Drittländer

1. Die Plattform wird in Rechenzentren in Deutschland betrieben. Die Daten und die Datensicherungen werden in Deutschland gespeichert.
2. Einige KI-Modelle und Dienste, die der Verantwortliche auswählen kann, stammen von Anbietern mit Sitz oder Verarbeitung außerhalb der EU und des Europäischen Wirtschaftsraums (Drittland), insbesondere in den USA. Nutzt der Verantwortliche ein solches Modell, werden Eingaben, Dokumentinhalte, Sprachdaten und Ergebnisse an diesen Anbieter übermittelt und dort verarbeitet.
3. Eine Übermittlung in ein Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, und zwar auf einer der folgenden Grundlagen:
    1. Angemessenheitsbeschluss nach Art. 45 DSGVO. Für die USA gilt dies nur für Empfänger, die nach dem EU-U.S. Data Privacy Framework zertifiziert sind (Durchführungsbeschluss (EU) 2023/1795). Der Auftragsverarbeiter prüft die Zertifizierung vor der ersten Übermittlung und danach regelmäßig, mindestens jährlich, und dokumentiert die Prüfung.
    2. Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914, Modul drei (Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter), die der Auftragsverarbeiter mit dem Unterauftragsverarbeiter abschließt.
4. Der Auftragsverarbeiter vereinbart die Standardvertragsklauseln nach Abs. 3 Nr. 2 auch mit Empfängern, die nach dem EU-U.S. Data Privacy Framework zertifiziert sind. So bleibt die Übermittlung abgesichert, falls der Angemessenheitsbeschluss aufgehoben oder für ungültig erklärt wird.
5. Soweit die Übermittlung auf Standardvertragsklauseln beruht, beurteilt der Auftragsverarbeiter vor der ersten Übermittlung, ob Recht und Praxis des Drittlands die Einhaltung der Klauseln verhindern, insbesondere durch Zugriffsrechte von Behörden (Klausel 14 der Standardvertragsklauseln, Transfer-Folgenabschätzung). Er dokumentiert die Beurteilung und stellt sie dem Verantwortlichen und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung.
6. Der Auftragsverarbeiter verpflichtet die Unterauftragsverarbeiter in Drittländern, ihn unverzüglich zu informieren, wenn sie ein rechtlich bindendes Ersuchen einer Behörde um Offenlegung der Daten erhalten oder von einem direkten Zugriff einer Behörde erfahren (Klausel

15 der Standardvertragsklauseln). Er leitet diese Information unverzüglich an den Verantwortlichen weiter, soweit dies rechtlich zulässig ist.

7. Entfällt die Grundlage für eine Übermittlung, zum Beispiel weil ein Angemessenheitsbeschluss aufgehoben wird, eine Zertifizierung endet oder ein Unterauftragsverarbeiter die Klauseln nicht mehr einhalten kann, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich. Er setzt die Übermittlung an diesen Anbieter aus und sperrt das betroffene Modell, bis eine andere Grundlage nach Abs. 3 besteht.
8. Modelle mit Verarbeitung außerhalb der EU sind in der Oberfläche gekennzeichnet, mit Angabe des Anbieters und des Landes. Zu Beginn sind alle verfügbaren Modelle freigegeben, soweit der Verantwortliche im Onboarding-Fragebogen nichts anderes angibt. Auf Wunsch des Verantwortlichen deaktiviert der Auftragsverarbeiter Modelle außerhalb der EU. Bei Verantwortlichen, die einer gesetzlichen Berufsverschwiegenheit unterliegen, sind zu Beginn nur Modelle mit Verarbeitung in der EU freigegeben; Modelle außerhalb der EU kann der Verantwortliche im Onboarding-Fragebogen auswählen oder in den Einstellungen selbst aktivieren. Die Plattform protokolliert jede Aktivierung mit Zeitpunkt, Nutzer und Modell. Die Administratoren des Verantwortlichen, bei Einzelnutzern der Nutzer selbst, können in den Einstellungen einzelne Modelle abwählen und die Nutzung auf Modelle beschränken, die Daten ausschließlich in der EU verarbeiten. Nutzer können im Rahmen dieser Vorgaben weitere Modelle für sich abwählen. Abgewählte Modelle können weder im Chat noch über Agenten genutzt werden.
9. Der Auftragsverarbeiter stellt dem Verantwortlichen die Angaben zur Verfügung, die dieser für seine Informationspflichten nach Art. 13 Abs. 1 lit. f und Art. 14 Abs. 1 lit. f DSGVO braucht (Empfänger, Land, Grundlage der Übermittlung), und auf Anfrage eine Kopie der Standardvertragsklauseln.

§ 8 Unterstützung des Verantwortlichen

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen, wenn betroffene Personen ihre Rechte nach Art. 12–23 DSGVO geltend machen.
2. Er unterstützt ihn außerdem bei den Pflichten nach Art. 32–36 DSGVO, also bei Sicherheit, Meldungen, Datenschutz-Folgenabschätzung und Konsultation der Aufsichtsbehörde.
3. Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter. Er beantwortet sie nicht selbst, es sei denn, der Verantwortliche hat ihn dazu ermächtigt.

§ 9 Meldung von Datenschutzverletzungen

1. Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden, nachdem er sie bemerkt hat.
2. Die Meldung enthält die Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie bekannt sind.
3. Das gilt auch für Verletzungen bei Unterauftragsverarbeitern, einschließlich solcher in Drittländern.

§ 10 Löschung und Rückgabe

1. Nach dem Ende des Hauptvertrags kann der Verantwortliche seine Daten 30 Tage lang exportieren.
2. Danach löscht der Auftragsverarbeiter alle Daten, auch bei den Unterauftragsverarbeitern, soweit keine gesetzliche Pflicht zur Aufbewahrung besteht.
3. Auf Anfrage bestätigt er die Löschung in Textform.

§ 11 Nachweise und Kontrollen

1. Der Auftragsverarbeiter stellt dem Verantwortlichen die Informationen zur Verfügung, die er braucht, um die Einhaltung dieses AVV nachzuweisen.
2. Er ermöglicht Überprüfungen durch den Verantwortlichen oder einen von ihm beauftragten Prüfer. Dafür gelten folgende Bedingungen:
    - Ankündigung mit angemessener Frist, in der Regel 14 Tage;
    - Durchführung während der Geschäftszeiten;
    - ohne Störung des Betriebs.
3. Bei Unterauftragsverarbeitern, insbesondere in Drittländern, kann der Nachweis auch durch aktuelle Zertifikate oder Prüfberichte unabhängiger Stellen erbracht werden (zum Beispiel ISO 27001, SOC 2).

§ 12 Haftung und Schlussbestimmungen

1. Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gilt die Haftungsregelung des Hauptvertrags.
2. Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag geht dieser AVV vor, soweit es um den Datenschutz geht.
3. Die Qalcurate UG (haftungsbeschränkt) befindet sich in Gründung. Der Verantwortliche stimmt bereits jetzt zu, dass der Auftragsverarbeiter diesen AVV zusammen mit dem Hauptvertrag nach der Eintragung der Gesellschaft in das Handelsregister auf sie überträgt. Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage vorher in Textform und nennt dabei Sitz, Registergericht und Registernummer. Die technischen und organisatorischen Maßnahmen und die Unterauftragsverarbeiter bleiben unverändert, soweit keine Mitteilung nach § 6 Abs. 2 erfolgt. Der Verantwortliche kann den Hauptvertrag und diesen AVV bis zum Wirksamwerden der Übertragung außerordentlich kündigen.
4. Es gilt deutsches Recht.

Verantwortlicher: Ort _____, Datum _____

Name _____, Funktion _____

Auftragsverarbeiter: Hinte, Datum _____

Roland Jungenkrüger, Geschäftsführer Value4p GmbH

Dieser AVV wird im elektronischen Format geschlossen (Art. 28 Abs. 9 DSGVO): durch die Anmeldung des Verantwortlichen über das Anmeldeformular und die Bestätigung des Auftragsverarbeiters per E-Mail. Eine Unterschrift ist nicht erforderlich.

Anlage A: Technische und organisatorische Maßnahmen (TOM)

1. Allgemeine Maßnahmen

Ziel nach Art. 32 DSGVO	Maßnahmen
Vertraulichkeit: Zutritt	Rechenzentren der Hosting-Anbieter in Deutschland mit Zutrittskontrolle (Anlage B; Nachweis: Zertifikat des Anbieters, z. B. ISO 27001)
Vertraulichkeit: Zugang	Anmeldung mit persönlichem Konto und Passwortrichtlinie. Zwei-Faktor-Anmeldung: verpflichtend für Mandanten von Berufsgeheimnisträgern (zum Beispiel Rechtsanwälte, Steuerberater, Wirtschaftsprüfer, Ärzte). Für alle anderen Mandanten freiwillig; der Administrator kann sie für den Mandanten erzwingen, und zwar für einzelne Nutzer, bei jeder Anmeldung oder in regelmäßigen Abständen. Ohne Vorgabe entscheidet jeder Nutzer selbst: bei jeder Anmeldung, in regelmäßigen Abständen oder nicht. Single Sign-on wird im Piloten nicht angeboten. Server-Zugriff nur per SSH-Schlüssel; Firewall
Vertraulichkeit: Zugriff	Rollen und Rechte je Mandant; Trennung der Mandanten; administrativer Zugriff nur für benannte Personen; Protokollierung
Trennung	Logische Trennung der Daten je Organisation; getrennte Umgebungen für Entwicklung und Betrieb
Integrität: Weitergabe	Verschlüsselte Übertragung (TLS); Übermittlung an Modellanbieter nur über verschlüsselte Schnittstellen
Pseudonymisierung bei der Websuche	Namen, Anschriften, Kontaktdaten, Kennungen und Kontonummern in Suchanfragen werden vor dem Senden an Suchmaschinen automatisch durch Platzhalter ersetzt; die Zuordnung besteht nur im Arbeitsspeicher für die Dauer der Anfrage und wird nicht gespeichert. Drei Stufen: ohne Pseudonymisierung, Pseudonymisierung ohne Bestätigung, Pseudonymisierung mit Bestätigung vor dem Senden (der Nutzer sendet, ändert oder verwirft die pseudonymisierte Suchanfrage). Voreinstellung: Pseudonymisierung mit Bestätigung. Bei automatischen Abläufen ohne anwesenden Nutzer entfällt die Bestätigung; die Suchanfrage wird pseudonymisiert gesendet, soweit der Verantwortliche nichts anderes festlegt. Der Verantwortliche kann eine Mindeststufe für alle Nutzer verbindlich vorgeben. Ist die Prüfung der Suchanfrage nicht möglich, fragt die Plattform den Nutzer, ob die Suche ohne Pseudonymisierung ausgeführt werden soll; ohne seine Zustimmung und bei automatischen Abläufen wird sie nicht ausgeführt.

Ziel nach Art. 32 DSGVO	Maßnahmen
Pseudonymisierung bei Anfragen an KI-Modelle	Vor dem Senden an ein KI-Modell werden dieselben Angaben durch Platzhalter ersetzt; in der Antwort setzt die Plattform die Angaben wieder ein. Die Zuordnung besteht nur im Arbeitsspeicher für die Dauer der Anfrage und wird nicht gespeichert. Einstellbar je Modellklasse (Modelle außerhalb der EU, Modelle in der EU). Drei Stufen: aus, eingeschaltet ohne Bestätigung, eingeschaltet mit Bestätigung vor dem Senden. Voreinstellung im Piloten: eingeschaltet mit Bestätigung für alle Modelle. Bei automatischen Abläufen ohne anwesenden Nutzer entfällt die Bestätigung; die Anfrage wird pseudonymisiert gesendet, soweit der Verantwortliche nichts anderes festlegt. Bei eingeschalteter Pseudonymisierung prüft eine auf den Servern des Auftragsverarbeiters betriebene Bilderkennung Bilder vor dem Senden: Bilder ohne personenbezogene Angaben werden gesendet; bei Bildern mit solchen Angaben wird stattdessen eine pseudonymisierte Beschreibung des Bildinhalts mit der Anfrage gesendet, die der Nutzer bei der Stufe mit Bestätigung vorher sieht. Andere Dateien im Originalformat werden nicht an das Modell gesendet, und Modelle mit eigener Websuche sind gesperrt. Ist die Pseudonymisierung für Modelle außerhalb der EU eingeschaltet, werden auch die Angaben an angebundene MCP-Server pseudonymisiert. Ist die Erkennung nicht verfügbar, fragt die Plattform den Nutzer, ob er die Anfrage ohne Pseudonymisierung senden will; ohne seine Zustimmung und bei automatischen Abläufen wird sie nicht gesendet.
Grenzen der Pseudonymisierung	Die automatische Erkennung kann einzelne Angaben übersehen. Die Pseudonymisierung ergänzt die übrigen Maßnahmen dieser Anlage und ersetzt sie nicht.
Integrität: Eingabe	Protokollierung von Anmeldungen und administrativen Änderungen
Verfügbarkeit	Tägliche Datensicherung aller Datenbanken und Dateien; Aufbewahrung von 14 täglichen, 4 wöchentlichen und 3 monatlichen Sicherungen; verschlüsselte Kopie außerhalb des Hauptservers auf gesonderten Servern in Rechenzentren in Deutschland (bis zum Umzug bei Hostinger International Ltd., Frankfurt am Main; danach in verteilten Rechenzentren der NMMN GmbH in Deutschland); Überwachung mit Alarm bei Fehlern; monatlicher Wiederherstellungstest; Notfall- und Wiederherstellungsplan
Verschlüsselung	Übertragung mit TLS 1.2 oder höher; Verschlüsselung der gespeicherten Daten auf den Datenträgern (AES-256); Datensicherungen vor dem Speichern verschlüsselt (AES-256); Schlüssel nur bei benannten Personen des Auftragsverarbeiters
Überprüfung	Regelmäßige Überprüfung der Maßnahmen; Aktualisierung von Software und Abhängigkeiten; Verpflichtung der Beschäftigten auf Vertraulichkeit

2. Zusätzliche Maßnahmen bei Übermittlungen in Drittländer (§ 7)

Ziel	Maßnahmen
Datenminimierung	An Modellanbieter werden nur die Inhalte übermittelt, die für die jeweilige Anfrage nötig sind (Eingabe und ausgewählter Kontext). Kontodaten, Namen und E-Mail-Adressen der Nutzer werden nicht mitgesendet. Zur Missbrauchserkennung erhält der Anbieter nur eine pseudonyme interne Nutzerkennung. Ist die Pseudonymisierung eingeschaltet (Abschnitt 1), werden personenbezogene Angaben in Eingaben, Dokumenten und Agenten-Anweisungen vor dem Senden durch Platzhalter ersetzt, Bilder mit personenbezogenen Angaben durch eine pseudonymisierte Beschreibung; ist sie ausgeschaltet, gelangen solche Angaben zum Anbieter, soweit sie enthalten sind. Der Auftragsverarbeiter prüft dies regelmäßig anhand von Stichproben der ausgehenden Daten.
Kein Training, kurze Speicherung	Vertragliche Zusage jedes Modellanbieters, Eingaben und Ergebnisse nicht zum Training zu nutzen. Speicherung beim Anbieter nur so kurz wie technisch nötig; wo angeboten, Vereinbarung ohne Speicherung („Zero Data Retention“). Angaben je Anbieter in Anlage B.
Datenstandort der KI-Modelle	Wo ein Modellanbieter die Verarbeitung in der EU anbietet, wird diese genutzt. Stand 09.11.2026: IONOS verarbeitet in Berlin. OpenAI bietet die Verarbeitung in der EU für freigegebene Konten an; der Auftragsverarbeiter nutzt sie, sobald OpenAI sie für sein Konto freigibt. Anthropic und Perplexity bieten über ihre direkten Schnittstellen keine Verarbeitung in der EU an. Der Verantwortliche kann die Nutzung auf Modelle mit Verarbeitung in der EU beschränken (§ 7 Abs. 8).
Steuerung durch den Verantwortlichen	Freigabe je Modell und je Suchmaschine durch Administratoren; Einstellung „nur Verarbeitung in der EU“; Kennzeichnung von Modellen und Suchmaschinen außerhalb der EU; Einstellungen zur Pseudonymisierung (Abschnitt 1); Protokollierung, welches Modell eine Anfrage verarbeitet hat; Protokollierung jeder Aktivierung von Modellen und Suchmaschinen außerhalb der EU
Verschlüsselung	Übertragung an Modellanbieter nur über TLS 1.2 oder höher; Verschlüsselung der in Deutschland gespeicherten Daten (siehe Abschnitt 1)
Behördenersuchen	Festgelegter Ablauf für Ersuchen von Behörden: rechtliche Prüfung, Anfechtung bei Rechtswidrigkeit, Herausgabe nur der Mindestmenge, Dokumentation und Information des Verantwortlichen (Klausel 15 der Standardvertragsklauseln)
Laufende Kontrolle	Prüfung der Zertifizierung nach dem EU-U.S. Data Privacy Framework vor der ersten Übermittlung und mindestens jährlich; Aktualisierung der Transfer-Folgenabschätzung bei Änderungen der Rechtslage

Anlage B: Unterauftragsverarbeiter

Stand 23.11.2026. Die Angaben zu Training und Speicherung beruhen auf den Vertrags- und Hilfeseiten der Anbieter (geprüft am 09.11.2026, Atlassian am 20.11.2026).

Unterauftrags-verarbeiter	Leistung	Sitz / Ort der Verarbeitung	Grundlage bei Drittland	Training / Speicherung beim Anbieter
NMMN GmbH, Haferweg 46, 22769 Hamburg	Betrieb der Server der Plattform ab Beginn des Piloten; nach dem Umzug auch Speicherung der verschlüsselten Datensicherungen	Hamburg / Rechenzentren in Deutschland	–	–
Hostinger International Ltd.	Betrieb einzelner Dienste der Plattform, solange sie noch nicht zur NMMN GmbH umgezogen sind; dies kann auch nach Beginn des Piloten der Fall sein; bis zum Umzug auch Speicherung der verschlüsselten Datensicherungen auf gesonderten Servern	Larnaka, Zypern (EU) / Rechenzentrum Frankfurt am Main	–	–
IONOS SE	Ausschließlich Bereitstellung von KI-Diensten (IONOS AI Model Hub): europäische KI-Modelle, Reranking für die Dokumentsuche, Spracherkennung; keine Speicherung von Datensicherungen oder Serverkopien	Montabaur / Rechenzentrum Berlin	–	kein Training; Eingaben und Ergebnisse werden nicht gespeichert, sondern nur während der Anfrage im Arbeitsspeicher verarbeitet; gespeichert werden nur Metadaten (Zeitpunkt, Modell, Tokenzahl)
Anthropic Ireland, Limited, und Anthropic, PBC	Verarbeitung von Eingaben durch KI-Modelle (Claude)	Dublin, Irland, und San Francisco, USA / USA	SCC 2021/914 (im Anthropic-DPA); Anthropic ist nicht nach dem EU-U.S. Data Privacy Framework zertifiziert	kein Training; Löschung binnen 30 Tagen
OpenAI, L.L.C.	Verarbeitung von Eingaben durch KI-Modelle (GPT)	San Francisco, USA / USA	SCC 2021/914, Modul drei (im OpenAI-DPA)	kein Training; Protokolle bis 30 Tage
Perplexity AI, Inc.	Verarbeitung von Eingaben durch KI-Modelle (Sonar, Antworten mit Websuche)	San Francisco, USA / USA	SCC 2021/914, Modul drei (im Perplexity-DPA)	kein Training; Speicherung bis zur Löschung, spätestens 30 Tage nach Ende der Leistung; keine Vereinbarung ohne Speicherung

Unterauftrags-verarbeiter	Leistung	Sitz / Ort der Verarbeitung	Grundlage bei Drittland	Training / Speicherung beim Anbieter
Microsoft Ireland Operations Ltd.	Versand von Systemnachrichten und E-Mail-Verkehr mit dem Support (Microsoft 365)	Dublin, Irland (EU) / EU (EU Data Boundary)	–	–
Atlassian Pty Ltd	Bearbeitung von Support-Anfragen und Fehlermeldungen im Ticketsystem (Jira)	Sydney, Australien / Rechenzentren von Amazon Web Services, auch in den USA	SCC 2021/914, Modul drei (im Atlassian-DPA); verbundene US-Gesellschaften sind nach dem EU-U.S. Data Privacy Framework zertifiziert	Speicherung bis zur Löschung des Tickets; Nutzung der Daten nur zur Leistungserbringung, zur Verbesserung der Produkte nur in de-identifizierter und aggregierter Form (Atlassian-DPA)

Der Umzug der Plattform zur NMMN GmbH ist zum Beginn des Piloten vorgesehen. Einzelne Dienste können auch danach noch auf Servern von Hostinger International Ltd. laufen. Beide Anbieter betreiben Rechenzentren in Deutschland. Sobald alle Dienste zur NMMN GmbH umgezogen sind, entfällt Hostinger International Ltd. als Unterauftragsverarbeiter.

Selbst betrieben auf den Servern des Auftragsverarbeiters, ohne weitere Unterauftragsverarbeiter: Embeddings für die Dokumentsuche, Sprachausgabe, die Bilderkennung zur Pseudonymisierung von Bildern, eine Spracherkennung als Ausweichlösung sowie die Websuche und das Lesen von Webseiten.

Empfänger, die keine Unterauftragsverarbeiter sind

Nutzt ein Nutzer die Websuche, leitet die Plattform die Suchbegriffe an öffentliche Suchmaschinen weiter, auch an Anbieter in Drittländern. Die Suchmaschinen verarbeiten die Suchbegriffe als eigene Verantwortliche und nicht im Auftrag des Auftragsverarbeiters. Die Plattform übermittelt dabei keine Nutzerkennung und nicht die IP-Adresse des Nutzers. Die Websuche wird nur genutzt, wenn der Nutzer sie im Chat einschaltet oder einen Agenten verwendet, den der Verantwortliche mit Websuche eingerichtet oder freigegeben hat; dies gilt als Weisung nach § 3 Abs. 2. Ist die Pseudonymisierung bei der Websuche eingeschaltet, werden personenbezogene Angaben in den Suchbegriffen vorher durch Platzhalter ersetzt (Anlage A Abschnitt 1). Der Verantwortliche kann Suchmaschinen mit Sitz außerhalb der EU abwählen oder die Websuche abschalten. Bei Verantwortlichen, die einer gesetzlichen Berufsverschwiegenheit unterliegen, sind zu Beginn nur Suchmaschinen mit Sitz in der EU freigegeben; weitere kann der Verantwortliche aktivieren, und die Plattform protokolliert die Aktivierung. Nutzer sollen keine personenbezogenen Daten in Suchbegriffe aufnehmen. Suchmaschinen sind nicht zur Verschwiegenheit verpflichtet. Verantwortliche, die einer gesetzlichen Berufsverschwiegenheit unterliegen, nehmen keine Geheimnisse ihrer Mandanten oder Patienten in Suchbegriffe auf.

Bindet der Verantwortliche eigene MCP-Server oder andere Schnittstellen (API) an Qalvy an oder lässt er sie vom Auftragsverarbeiter einrichten, gehen Daten an das angebundene System. Dessen Betreiber wird im Auftrag oder in der Verantwortung des Verantwortlichen tätig und ist kein Unterauftragsverarbeiter des Auftragsverarbeiters. Die Anbindung und ihre Nutzung durch Agenten gelten als Weisung nach § 3 Abs. 2.