Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

Version: 2.2 **Stand:** 06/11/2026

Diese Vereinbarung zur Auftragsverarbeitung gilt zwischen der oneAI GmbH, Eisenbahnstraße 50, 72072 Tübingen, Deutschland (nachfolgend „Auftragsverarbeiter") und dem jeweiligen Kunden, der die Nutzungsbedingungen (EULA) und Allgemeinen Geschäftsbedingungen (AGB) der oneAI GmbH akzeptiert (nachfolgend „Auftraggeber"). Auftraggeber und Auftragsverarbeiter werden nachfolgend einzeln auch „Partei" und gemeinsam „Parteien" genannt. Diese Vereinbarung wird automatisch und ohne gesonderte Unterzeichnung Bestandteil des Vertragsverhältnisses zwischen der oneAI GmbH und jedem Kunden mit Annahme der Nutzungsbedingungen.

Präambel

Zur Konkretisierung der Rechte und Pflichten, die sich aus dem Auftragsverarbeitungsverhältnis im Rahmen der gesetzlichen Vorgaben des Art. 28 DSGVO ergeben, schließen die Parteien die nachfolgende Vereinbarung. Diese Vereinbarung ergänzt die zwischen den Parteien bestehenden Nutzungsbedingungen (EULA) und Allgemeinen Geschäftsbedingungen (AGB) der oneAI GmbH, die gemeinsam die vertragliche Grundlage für die Nutzung der oneAI SaaS-Plattform bilden (nachfolgend gemeinsam „Hauptvertrag").

1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand des Auftrags

Gegenstand des Auftrags ist die Durchführung folgender Aufgaben:

Der Auftragsverarbeiter erbringt für den Auftraggeber die Bereitstellung und den Betrieb der OneAI SaaS-Plattform (hub.oneai.eu) auf Grundlage des Hauptvertrags. Dies umfasst insbesondere die KI-gestützte Text- und Chatverarbeitung, die RAG-basierte Dokumentensuche, die Verwaltung von Spaces und hochgeladenen Inhalten sowie das Audit-Logging. Hinsichtlich der einzelnen Leistungen wird auf die Leistungsbeschreibung des Hauptvertrages verwiesen.

Die Verarbeitung personenbezogener Daten erfolgt nach Maßgabe des vom Auftraggeber gewählten Modellbetriebs:

- Standardmodelle (self-hosted) sowie Private Models – Verarbeitung ausschließlich innerhalb der Infrastruktur des Auftragsverarbeiters bzw. des Auftraggebers;
- „EU-Modelle“ (EU-Flagge-Modelle) – Verarbeitung über Google Vertex AI Model Garden in der EU-Region;
- Public Models – vom Auftraggeber aktiv auszuwählende externe Modellanbieter; insoweit gelten zusätzlich die in Anlage 1 ausgewiesenen Garantien.

Auf ausdrücklichen Wunsch des Auftraggebers oder sofern dies im Hauptvertrag bzw. im jeweiligen Einzelauftrag ausdrücklich vereinbart ist insbesondere wenn die Installation nicht durch einen vom Auftraggeber beauftragten Implementierungspartner erfolgt, erbringt der

Auftragsverarbeiter zusätzlich folgende optionale Leistung: Der Auftraggeber stellt dem Auftragsverarbeiter eine betriebsbereite, isolierte virtuelle Maschine (Linux-VM) innerhalb seines eigenen Netzwerks zur Verfügung. Der Auftragsverarbeiter verbindet sich mit dieser VM ausschließlich zum Zweck der Installation und Konfiguration eines Relay-Docker-Containers, der die Anbindung lokaler SMB-Freigaben des Auftraggebers an die oneAI Cloud Plattform ermöglicht. Der Auftragsverarbeiter erstellt oder betreibt die virtuelle Maschine selbst nicht; Bereitstellung, Betrieb und Absicherung der VM obliegen dem Auftraggeber. Der Auftragsverarbeiter hat im Rahmen dieser Tätigkeit keinen Zugriff auf die SMB-Freigabe selbst, da die hierfür erforderlichen Zugangsdaten dem Auftragsverarbeiter nicht vorliegen; der Zugriff beschränkt sich auf die Netzwerkebene der bereitgestellten VM zum Zweck der Container Installation und Konfiguration. Ein Drittlandtransfer ist hiermit nicht verbunden. Nach erfolgreicher Installation und Konfiguration wird der dem Auftragsverarbeiter eingeräumte Zugriff auf die virtuelle Maschine beendet; ein erneuter Zugriff (z. B. für Updates oder Wartungsarbeiten) erfolgt nur nach erneuter Freigabe durch den Auftraggeber.

1.2 Dauer des Auftrags

Die Dauer dieses Auftrags entspricht der Laufzeit des zugrunde liegenden Hauptvertrages. Der Auftraggeber kann diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter einen schwerwiegenden Verstoß gegen diese Vereinbarung oder die anwendbaren Datenschutzvorschriften begeht, eine Weisung des Auftraggebers nicht ausführt, die Erteilung erforderlicher Auskünfte verweigert oder dem Auftraggeber im Rahmen von Kontrollen den Zutritt bzw. Zugang verweigert. Nach Beendigung darf der Auftragsverarbeiter keine personenbezogenen Daten des Auftraggebers mehr verarbeiten.

1.3 Vergütung

Sämtliche Leistungen des Auftragsverarbeiters im Zusammenhang mit der Erfüllung seiner Pflichten aus dieser Vereinbarung sind mit der Vergütung aus dem zugrunde liegenden Hauptvertrag abgegolten.

2 Angaben zum Inhalt des Auftrags

2.1 Art, Zweck und Zulässigkeit der Verarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag und der zugehörigen Leistungsbeschreibung. Für die Beurteilung der Zulässigkeit der Verarbeitung ist allein der Verantwortliche verantwortlich.

2.2 Kategorien personenbezogener Daten

Gegenstand der Verarbeitung sind sämtliche personenbezogenen Daten, die der Auftraggeber bzw. die von ihm autorisierten Nutzer im Rahmen der Nutzung der Plattform eingeben, hochladen oder anderweitig verarbeiten lassen. Dies kann je nach Nutzung insbesondere umfassen: Namens- und Kontaktdaten, Kommunikationsinhalte, Dokumenteninhalte, Daten zum IT-Zugriff und Berechtigungsmanagement, Metadaten der IT-Nutzung sowie sonstige vom Auftraggeber oder seinen Nutzern eingegebene Inhalte. Die Bestimmung der tatsächlich verarbeiteten Datenkategorien obliegt allein dem Auftraggeber als Verantwortlichem im Rahmen seiner eigenen Nutzungsentscheidungen. Bei Nutzung von Public Models ist der Auftraggeber verpflichtet, keine besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO (z. B. Gesundheitsdaten) ohne angemessene Rechtsgrundlage in Prompts zu

übermitteln (vgl. Hauptvertrag/Nutzungsbedingungen). Stellt der Auftraggeber dem Auftragsverarbeiter im Rahmen bestimmter Konnektoren (z. B. SMB-Netzwerkfreigaben) Zugangsdaten zu eigenen Drittsystemen bereit, gelten hierfür ergänzend die besonderen Regelungen in Anlage 2 Ziff. 1.6.

2.3 Kategorien betroffener Personen

Der Kreis der betroffenen Personen bestimmt sich nach der eigenen Nutzung der Plattform durch den Auftraggeber und kann insbesondere umfassen: Beschäftigte des Auftraggebers, Kunden und Geschäftspartner des Auftraggebers, Bewerber sowie sonstige natürliche Personen, deren personenbezogene Daten der Auftraggeber oder die von ihm autorisierten Nutzer im Rahmen der Nutzung der Plattform eingeben. Die Bestimmung der tatsächlich betroffenen Personenkategorien obliegt allein dem Auftraggeber als Verantwortlichem.

3 Technische und organisatorische Maßnahmen

3.1 Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten, wie sie Art. 28 Abs. 3 S. 2 lit. c DSGVO i. V. m. Art. 32 Abs. 1 DSGVO verlangt, um die Sicherheit der auftragsgemäßen Verarbeitung zu gewährleisten. Hierzu stellt der Auftragsverarbeiter sicher:

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

3.2 Die Parteien vereinbaren für diese Vereinbarung die in Anlage 2 („Technische und organisatorische Maßnahmen“) im Einzelnen festgelegten Maßnahmen. Diese gelten für den gesamten Betrieb der OneAI-Plattform; soweit Teile der Infrastruktur durch einen Unterauftragsverarbeiter (siehe Anlage 1) bereitgestellt werden, sind dessen Maßnahmen in das beschriebene Schutzniveau einbezogen.

3.3 Die Maßnahmen unterliegen dem technischen Fortschritt. Dem Auftragsverarbeiter ist es gestattet, alternative adäquate Maßnahmen nach dem jeweiligen Stand der Technik umzusetzen, sofern das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und dem Verantwortlichen in Textform mitzuteilen.

4 Drittlandtransfer

4.1 Bei Nutzung selbst gehosteter Standardmodelle, von „EU-Modellen“ (EU-Flagge-Modelle) (Google Vertex AI Model Garden, EU-Region) sowie von Private Models erfolgt die Verarbeitung ausschließlich innerhalb der Europäischen Union oder eines Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum; ein Drittlandtransfer findet insoweit nicht statt.

4.2 Eine Übermittlung in ein Drittland ist nur unter folgenden Voraussetzungen zulässig:

- Es liegt für das betreffende Land ein Angemessenheitsbeschluss nach Art. 45 DSGVO vor;

- der Auftragsverarbeiter bietet geeignete Garantien nach Art. 46 oder 47 DSGVO (insbesondere EU-Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914);
- die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit konkreten behördlichen, gerichtlichen oder aufsichtsrechtlichen Verfahren erforderlich; oder
- die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person erforderlich.

4.3 Eine Übermittlung an ein außerhalb der EU/des EWR ansässiges Public Model (z. B. OpenAI, USA) erfolgt ausschließlich infolge der bewussten Auswahl eines nicht als „EU“ (EU-Flagge) gekennzeichneten Public Models durch den Auftraggeber bzw. dessen Nutzer. Standardmodelle (self-hosted), „EU“ (EU-Flagge)-Modelle und Private Models lösen keinen Drittlandtransfer aus. Mit der Auswahl eines solchen Public Models erteilt der Auftraggeber dem Auftragsverarbeiter die dokumentierte Weisung gemäß Art. 28 Abs. 3 S. 2 lit. a DSGVO, die betreffenden Daten an den gewählten Anbieter zu übermitteln; über das Ob und Wohin der Übermittlung entscheidet damit allein der Auftraggeber als Verantwortlicher. Unterbleibt eine solche Auswahl, findet kein Drittlandtransfer statt. Der Auftraggeber kann zudem über die Administrationsfunktionen der Plattform technisch steuern, welche Modelle seinen Nutzern zur Verfügung stehen, und insbesondere nicht als „EU“ (EU-Flagge) gekennzeichnete Public Models sowie Private Models organisationsweit deaktivieren (technisch ausschließen). Macht der Auftraggeber hiervon Gebrauch, ist ein Drittlandtransfer über die Modellauswahl technisch ausgeschlossen.

4.4 Der mit einer solchen Auswahl verbundene Transfer erfolgt auf Grundlage der in Anlage 1 ausgewiesenen Garantien (EU-Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914 i. V. m. den jeweiligen Data Processing Addenda der Anbieter). Jede Übermittlung hat allen vertraglichen Verpflichtungen dieser Vereinbarung, insbesondere der Zweckbindung, zu entsprechen. Die Beurteilung der Zulässigkeit der Übermittlung im konkreten Einzelfall – insbesondere im Hinblick auf die jeweils eingegebenen Inhalte – obliegt dem Auftraggeber als Verantwortlichem, gegebenenfalls im Rahmen seiner Datenschutz-Folgenabschätzung (Art. 35 DSGVO).

5 Berichtigung, Löschung und Sperrung von Daten

5.1 Der Auftragsverarbeiter darf die im Auftrag verarbeiteten Daten nur nach Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken (Art. 28 Abs. 3 S. 2 lit. a DSGVO).

5.2 Wendet sich eine betroffene Person mit dem Begehren auf unverzügliche Berichtigung oder Löschung ihrer personenbezogenen Daten unmittelbar an den Auftragsverarbeiter, so leitet dieser das Begehren unverzüglich an den Auftraggeber weiter.

5.3 Soweit vom Leistungsumfang umfasst, hat der Auftragsverarbeiter nach dokumentierter Weisung des Auftraggebers die Rechte auf Löschung, auf Vergessenwerden, auf Berichtigung, auf Datenübertragbarkeit und auf Auskunft unverzüglich sicherzustellen.

6 Kontrollen und andere Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu den Pflichten aus dieser Vereinbarung die gesetzlichen Pflichten gemäß Art. 28 bis 33 DSGVO einzuhalten; insbesondere:

a) Datenschutzbeauftragter des Auftragsverarbeiters ist Herr Henrik Simmack, Hinter Gärten 8, 72459 Albstadt, E-Mail: dpo@oneai.eu. Für allgemeine Fragen zum Datenschutz ist der Auftragsverarbeiter zudem unter privacy@oneai.eu erreichbar. Änderungen in der Person oder den Kontaktdaten des Datenschutzbeauftragten werden dem Auftraggeber unverzüglich in Textform mitgeteilt.

b) Der Auftragsverarbeiter und jede ihm unterstellte Person, die Zugang zu personenbezogenen Daten des Auftraggebers hat, dürfen diese Daten ausschließlich nach Weisung des Auftraggebers gemäß Ziffer 10 dieser Vereinbarung verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet (Art. 28 Abs. 3 S. 2 lit. a, Art. 29 DSGVO).

c) Der Auftragsverarbeiter setzt nur Personen ein, die zur Vertraulichkeit verpflichtet und mit den einschlägigen Datenschutzvorschriften vertraut gemacht wurden (Art. 28 Abs. 3 S. 2 lit. b DSGVO). Diese Verpflichtung gilt auch nach Beendigung dieser Vereinbarung und/oder des Hauptvertrages fort.

d) Der Auftragsverarbeiter wirkt bei der Erfüllung der Aufgaben der Aufsichtsbehörde mit.

e) Der Auftragsverarbeiter unterrichtet den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

f) Der Auftragsverarbeiter unterstützt den Auftraggeber nach besten Kräften bei aufsichtsbehördlichen Kontrollen, Ordnungswidrigkeits- oder Strafverfahren, Schadenersatzansprüchen betroffener Personen oder Dritter sowie sonstigen Ansprüchen im Zusammenhang mit der Verarbeitung.

g) Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich dem geltenden Datenschutzrecht entspricht und die Rechte der betroffenen Personen gewahrt werden.

h) Der Auftragsverarbeiter weist dem Auftraggeber im Rahmen der Kontrollrechte gemäß Ziffer 8 die getroffenen technischen und organisatorischen Maßnahmen nach.

7 Unterauftragsverhältnisse

7.1 Unterauftragsverhältnisse im Sinne dieser Vereinbarung sind solche Leistungen, die unmittelbar mit der Erbringung der Hauptleistung in Zusammenhang stehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z. B. als Telekommunikations-, Post-/Transport- oder Entsorgungsdienstleistung in Anspruch nimmt. Der Auftragsverarbeiter ist jedoch verpflichtet, auch bei solchen Nebenleistungen den Datenschutz und die Datensicherheit der Daten des Auftraggebers durch angemessene und rechtskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu gewährleisten.

7.2 Der Auftragsverarbeiter ist berechtigt, die in Anlage 1 genannten Unterauftragsverarbeiter zur Verarbeitung personenbezogener Daten des Auftraggebers einzusetzen. Die Hinzuziehung weiterer oder anderer Unterauftragsverarbeiter wird dem Auftraggeber in Textform mitgeteilt. Widerspricht der Auftraggeber nicht innerhalb von 30 Tagen

nach Zugang dieser Mitteilung in Textform, gilt die Änderung als genehmigt. Ein Widerspruch ist nur wirksam und beachtlich, wenn der Auftraggeber innerhalb dieser Frist in Textform objektiv und nachvollziehbar darlegt, dass und aus welchen konkreten Gründen der Einsatz des neuen oder geänderten Unterauftragsverarbeiters das nach dieser Vereinbarung, der DSGVO oder der Verordnung (EU) 2024/1689 (EU AI Act) geschuldete Schutz- bzw. Sicherheitsniveau herabsetzt oder gegen zwingende Vorgaben dieser Vorschriften verstößt. Nicht substantiierte Widersprüche sowie Widersprüche, die sich ausschließlich auf wirtschaftliche, wettbewerbliche, strategische oder sonstige nicht datenschutz- oder sicherheitsrechtlich begründete Erwägungen stützen, sind unwirksam. Kommt bei einem wirksamen Widerspruch innerhalb einer weiteren Frist von 14 Tagen keine einvernehmliche Lösung zustande, steht dem Auftraggeber ein außerordentliches Kündigungsrecht hinsichtlich des von der Unterbeauftragung betroffenen Leistungsteils zu.

7.3 Erbringt der Auftragsverarbeiter die vereinbarte Leistung unter Einbindung von Unterauftragsverarbeitern außerhalb der EU/des EWR, so stellt er sicher, dass die datenschutzrechtliche Zulässigkeit – insbesondere durch Garantien nach Ziffer 4 – gewährleistet ist. Der Unterauftragsverarbeiter ist denselben Datenschutzpflichten zu unterwerfen, die in dieser Vereinbarung festgelegt sind, mit hinreichenden Garantien geeigneter technischer und organisatorischer Maßnahmen (Art. 28 Abs. 4 S. 1 DSGVO).

8 Kontrollrechte des Auftraggebers

8.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch einen zur Vertraulichkeit verpflichteten Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, in der Regel einmal jährlich oder bei konkretem Anlass, von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen (Art. 28 Abs. 3 S. 2 lit. h DSGVO).

8.2 Der Auftragsverarbeiter stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten überzeugen kann. Er ist verpflichtet, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen (Art. 28 Abs. 3 S. 2 lit. h DSGVO).

8.3 Der Nachweis solcher Maßnahmen kann durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Datenschutzauditor, Qualitätsauditor), eine geeignete Zertifizierung (z. B. IT-Sicherheits- oder Datenschutzaudit) oder durch andere geeignete Maßnahmen erbracht werden.

9 Unterstützung des Auftraggebers, Mitteilung bei Verstößen des Auftragsverarbeiters

Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, zu Meldepflichten bei Datenpannen, zu Datenschutz-Folgenabschätzungen und vorherigen Konsultationen. Hierzu gehört insbesondere:

a) die Gewährleistung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere möglicher Rechtsverletzungen berücksichtigen und eine sofortige Feststellung relevanter Verletzungsereignisse ermöglichen;

b) die Verpflichtung, dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich zu dokumentieren und mitzuteilen (Art. 33 Abs. 2 DSGVO) sowie in Abstimmung mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen zu treffen;

c) die Unterstützung des Auftraggebers (Art. 28 Abs. 3 S. 2 lit. e DSGVO) im Rahmen seiner Meldepflicht gegenüber der Aufsichtsbehörde bzw. der betroffenen Person;

d) die Unterstützung des Auftraggebers bei dessen Informationspflicht gegenüber der betroffenen Person und die Bereitstellung sämtlicher relevanter Informationen auf Anforderung.

10 Weisungsbefugnisse des Auftraggebers, weisungsgebundene Verarbeitung

10.1 Der Auftraggeber hat ein umfassendes Weisungsrecht gegenüber dem Auftragsverarbeiter hinsichtlich Art, Umfang und Verfahren der Datenverarbeitung.

10.2 Die Daten dürfen ausschließlich im Rahmen dieser Vereinbarung und nach den Weisungen des Auftraggebers verarbeitet werden. Dem Auftragsverarbeiter ist es untersagt, die Daten zu anderen Zwecken zu verwenden oder ohne Kenntnis des Auftraggebers an Dritte weiterzugeben. Kopien oder Abschriften werden ohne Wissen des Auftraggebers nicht erstellt; ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Verarbeitung erforderlich sind.

10.3 Weisungen des Auftraggebers sind vom Auftragsverarbeiter zu dokumentieren. Mündlich erteilte Weisungen sind unverzüglich in Text- oder Schriftform zu bestätigen.

10.4 Änderungen des Verarbeitungsgegenstands und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Eine Weitergabe verarbeiteter personenbezogener Daten an Dritte oder die betroffene Person erfolgt nur nach vorheriger Zustimmung des Auftraggebers in Textform.

10.5 Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, so hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird (Art. 28 Abs. 3 S. 3 DSGVO).

10.6 Kein Training auf Kundendaten. Der Auftragsverarbeiter verwendet die personenbezogenen Daten des Auftraggebers niemals zum Training eigener oder fremder KI-Modelle. Bei selbst gehosteten Standardmodellen ist dies technisch durchgesetzt; bei Public Models ist dies vertraglich über die jeweiligen Data Processing Addenda der Anbieter (No-Training-Klauseln, bei Mistral zusätzlich durch aktivierten Trainings-Opt-out) abgesichert.

11 Haftung

11.1 Die Haftung der Parteien richtet sich nach den gesetzlichen Bestimmungen, insbesondere nach Art. 82 DSGVO. Der Auftragsverarbeiter haftet für einen durch die Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO oder dieser Vereinbarung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Weisungen des Auftraggebers bzw. gegen diese gehandelt hat (Art. 82 Abs. 2 S. 2 DSGVO).

11.2 Im Innenverhältnis tragen die Parteien den Schaden nach dem Maß ihres jeweiligen Verantwortungs- und Verschuldensbeitrags (Art. 82 Abs. 5 DSGVO). Soweit der Auftraggeber als Verantwortlicher Weisungen erteilt, Inhalte in die Plattform eingibt oder Modelle bzw. Public-Model-Anbieter auswählt, trägt er die hieraus resultierende datenschutzrechtliche Verantwortung.

11.3 Eine Partei ist von der Haftung befreit, wenn sie nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist (Art. 82 Abs. 3 DSGVO).

11.4 Etwaige Haftungsbeschränkungen und -höchstgrenzen des Hauptvertrages gelten auch für Ansprüche aus oder im Zusammenhang mit dieser Vereinbarung, soweit dies gesetzlich zulässig ist. Sie gelten nicht bei Vorsatz und grober Fahrlässigkeit, bei der Verletzung von Leben, Körper oder Gesundheit sowie für unmittelbare gesetzliche Ansprüche betroffener Personen und Sanktionen nach Art. 83 DSGVO.

12 Löschung von Daten und Rückgabe von Datenträgern

12.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind erforderliche Sicherungskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung sowie Daten, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

12.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder auf Anforderung des Auftraggebers – spätestens mit Beendigung des Hauptvertrages – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen sowie erstellte Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers zurückzugeben oder zu löschen (Art. 28 Abs. 3 S. 2 lit. g DSGVO). Dies gilt auch für Testdaten und verworfenes Material. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

12.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

13 Sonstiges, Anpassung dieser Vereinbarung

13.1 Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die unwirksame oder undurchführbare Bestimmung ist durch diejenige wirksame und durchführbare Regelung zu ersetzen, die dem wirtschaftlichen Zweck der ursprünglichen Bestimmung am nächsten kommt. Entsprechendes gilt für etwaige Regelungslücken.

13.2 Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand für Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung ist – soweit gesetzlich zulässig – Tübingen.

13.3 Änderungen dieser Vereinbarung werden dem Auftraggeber per E-Mail oder über die Plattform mit einer Frist von mindestens sechs (6) Wochen vor dem vorgesehenen Inkrafttreten angekündigt. Die Zustimmung des Auftraggebers gilt als erteilt, wenn er der Änderung nicht vor

dem vorgesehenen Zeitpunkt schriftlich widerspricht; auf diese Rechtsfolge wird der Auftraggeber in der Änderungsmitteilung gesondert hingewiesen. Eine wesentliche Änderung des Vertragsgegenstands (Hauptleistungspflichten) im Wege einseitiger Anpassung ist ausgeschlossen. Unberührt bleibt die Verpflichtung der Parteien, diese Vereinbarung anzupassen, soweit dies aufgrund einer Änderung der anwendbaren Datenschutzgesetze oder verbindlicher Vorgaben der Europäischen Kommission oder der zuständigen Aufsichtsbehörden erforderlich wird. Für die Hinzuziehung oder den Austausch von Unterauftragsverarbeitern gilt ausschließlich die Regelung in Ziffer 7.2; die vorstehenden Absätze dieser Ziffer 13.3 finden hierauf keine Anwendung.

Anlage 1 – Liste der Unterauftragsverarbeiter

Liste der vom Auftragsverarbeiter mit Zustimmung des Auftraggebers eingesetzten Unterauftragsverarbeiter (mit verifizierten Geschäftsanschriften). Die Liste ist nachstehend aufgeführt; Änderungen werden gemäß Ziffer 7.2 mitgeteilt.

Nr.	Unternehmen	Anschrift	Aufgabenbereich	Garantie (Drittland)
1	Google Ireland Ltd. (Reg.-Nr. 368047) – Vertex AI Model Garden	Gordon House, Barrow Street, Dublin 4, D04 E5W5, Irland	LLM-Inferenz „EU“ (EU-Flagge)-Modelle (Gemini, Claude); Anthropic als Unterauftragsverarbeiter von Google	Google Cloud CDPA, EU-Region (kein Drittlandtransfer)
2	OpenAI OpCo, LLC (EWR/Schweiz: OpenAI Ireland Ltd.)	OpCo: 1455 3rd Street, San Francisco, CA 94158, USA · Ireland: 1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland	LLM-Inferenz (Public-Modelle), Audio-Transkription (whisper-1)	DPA + EU-SCCs (2021/914)
3	Mistral AI SAS (R.C.S. Paris 952 418 325)	15 rue des Halles, 75001 Paris, Frankreich	LLM-Inferenz (Public-Modell)	DPA, Training-Opt-out + Zero Data Retention; kein Drittlandtransfer
4	Hetzner Online GmbH (HRB 6089 Ansbach)	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Cloud-Hosting (Infrastruktur, inkl. self-hosted KI-Modelle)	DPA (kein Drittlandtransfer)

Nr.	Unternehmen	Anschrift	Aufgabenbereich	Garantie (Drittland)
5	relyon AG (HRB 766138 Stuttgart)	Eisenbahnstraße 50, 72072 Tübingen, Deutschland	Betrieb der nicht-GPU-lastigen Infrastruktur (Applikations-, Datenbank-, Datei- und Vektor-Speicher, Audit-Log) auf eigener Hardware als Colocation im Hetzner-Rechenzentrum	DPA (kein Drittlandtransfer)
6	weber.digital GmbH (HRB 411104)	Zollernstraße 49, 72336 Balingen, Germany	LLM inference (Public Models)	DPA (no third-country transfer)
7	Scaleway S.A.S. (R.C.S. Paris 433 115 904)	8 rue de la Ville l'Évêque, 75008 Paris, Frankreich	Cloud-Hosting (Infrastruktur, einschließlich Anwendung, Datenbank-, Vektor- und Dateispeicher)	DPA (kein Drittlandtransfer)

Hinweis: Anbieter und Datentransfers, die nicht zur Erbringung der Kernleistung gegenüber dem Auftraggeber eingesetzt werden – insbesondere Zahlungs- und E-Mail-Dienstleister sowie vom Auftraggeber selbst angebundene Connector-Zielsysteme (z. B. Microsoft, Google, GitHub, ClickUp, weclapp) – sind nicht Gegenstand dieses Auftrags. Connector-Zielsysteme liegen im Verantwortungsbereich des Auftraggebers und werden ausschließlich auf dessen Veranlassung und auf Basis seiner eigenen Vertragsbeziehungen angebunden.

Anlage 2 – Technische und organisatorische Maßnahmen

Nachfolgend die von der oneAI GmbH umgesetzten und gewährleisteten technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Die OneAI-Plattform wird auf Servern im ISO-27001-zertifizierten Rechenzentrum der Hetzner Online GmbH (Deutschland) betrieben, ergänzt durch eine zusätzliche, ebenfalls ISO-27001-zertifizierte Ausweich- bzw. Sekundärkapazität bei Scaleway S.A.S. (Frankreich, siehe Anlage 1); die nicht-GPU-lastige Infrastruktur wird durch den Infrastruktur-Unterauftragsverarbeiter relyon AG bereitgestellt (siehe Anlage 1). Die nachstehenden Maßnahmen gelten für den gesamten Betrieb der OneAI-Plattform.

1. Vertraulichkeit

1.1 Zutrittskontrolle

1. Die Mitarbeitenden der oneAI GmbH sind im Umgang mit und zur Vertraulichkeit von sensiblen Daten geschult.
2. Die Büro- und Betriebsräume der oneAI GmbH sind mit einem elektronischen Schließsystem gesichert; elektronische Schlüssel werden nur an berechtigte Personen ausgegeben, die Ausgabe wird protokolliert.

3. Geschäftsräume sind verschlossen und können nur durch berechtigte Personen mit einem Schlüssel betreten werden.
4. Die Server der OneAI-Plattform stehen im ISO-27001-zertifizierten Rechenzentrum der Hetzner Online GmbH (Deutschland). Die Rechenzentrumsflächen sind rund um die Uhr durch Personal des Rechenzentrumsbetreibers besetzt sowie alarm- und videoüberwacht.
5. Besucher von Rechenzentrumsflächen werden am Eingang abgeholt und in eine Besucherliste eingetragen; der Zutritt ist nur mit gültigen Ausweispapieren möglich.
6. Wichtige Dokumente werden in verschließbaren Schränken aufbewahrt; die Schlüssel erhalten nur berechtigte Personen.

1.2 Zugangskontrolle

1. Passwordless-First: Authentifizierung über WebAuthn/Passkeys (FIDO2); keine passwortbasierte Standardanmeldung.
2. Single Sign-On über Microsoft Entra ID (OAuth 2.0) und Google Sign-In; administrative Zugänge rollenbasiert, zusätzlich geschützt durch Conditional-Access-Richtlinien und verpflichtende Multi-Faktor-Authentifizierung (MFA).
3. Alle Mitarbeitenden erhalten ein personalisiertes Benutzerkonto; Passwörter werden nicht geteilt. Soweit Passwörter genutzt werden, gilt eine Komplexitätsrichtlinie mit mindestens 15 Zeichen (Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen).
4. Automatisierte Benutzerbereitstellung und -deaktivierung über Enterprise SCIM 2.0.
5. Das Netzwerk wird durch eine regelbasierte, regelmäßig überprüfte Firewall geschützt; Spamfilter und Antiviren-/Malwareschutz mit mehrmals täglich aktualisierten Signaturen.
6. Mobile Geräte enthalten keine unverschlüsselten personenbezogenen Daten; Einsatz eines Mobile Device Management (MDM).
7. Session-Management: 24-Stunden-Ablauf, Session-Token SHA-256-gehasht; API-Keys mit optionalem Ablaufdatum, verschlüsselt gespeichert.
8. Externe Dienstleister werden nur mit abgeschlossenem Auftragsverarbeitungsvertrag eingesetzt; ihr Zugriff wird auf das erforderliche Maß beschränkt.

1.3 Zugriffskontrolle

1. Für alle Systeme und Ablagen besteht ein Berechtigungskonzept mit Benutzerrollen (RBAC) auf Organisations- und Space-Ebene (Lesen/Schreiben/Admin).
2. Strikte Mandantentrennung auf Datenbankebene; jede Operation wird authentifiziert und automatisch dem jeweiligen Mandanten zugeordnet.
3. Benutzerkonten ausgeschiedener Mitarbeitender werden unmittelbar nach Beendigung des Arbeitsverhältnisses gesperrt und nach einer Übergangszeit gelöscht.
4. Zugriffe auf Anwendungen mit personenbezogenen Daten werden protokolliert; die Protokolle werden 14 Tage aufbewahrt.
5. Nicht mehr benötigte oder zur Wiederverwendung vorgesehene Datenträger werden manuell zerstört oder durch mehrfaches Überschreiben sicher gelöscht.
6. Der Zugriff auf vom Auftraggeber bereitgestellte virtuelle Maschinen im Rahmen des optionalen Fernzugriffs (vgl. Ziffer 1.1) ist ausschließlich autorisiertem Personal vorbehalten. Gemeinsam genutzte Zugangsdaten (Shared Credentials) werden hierfür nicht eingesetzt; jede zugreifende Person authentifiziert sich über einen persönlichen SSH-Schlüssel oder ein individuelles Benutzerkonto.

1.4 Trennung

1. Die Daten unterschiedlicher Mandanten werden logisch sowie netzseitig über in der Sicherheitsarchitektur hinterlegte VLANs voneinander getrennt; die Netzsegmente werden über eine Firewall getrennt.
2. Produktiv-Systeme sind von Test- und Entwicklungsumgebungen getrennt.

1.5 Pseudonymisierung & Verschlüsselung

1. Alle personenbezogenen Daten werden bei der Übertragung durch geeignete Maßnahmen (TLS 1.2+/HTTPS, VPN) verschlüsselt.
2. Ruhende Provider-API-Keys werden mit XChaCha20-Poly1305 (Cure53-auditierte Bibliothek) verschlüsselt; gespeicherte Kennwörter und Zugangsdaten werden verschlüsselt in einem Passwort-Safe gehalten.
3. Backups werden separat verschlüsselt; zentrales Secrets-Management, keine hartkodierten Credentials.

1.6 Zugangsdaten zu Drittsystemen des Auftraggebers

Stellt der Auftraggeber dem Auftragsverarbeiter im Rahmen der Nutzung bestimmter Konnektoren (z. B. zur Anbindung von SMB-Netzwerkfreigaben) Zugangsdaten zu eigenen Drittsystemen bereit, gilt ergänzend Folgendes:

1. Die Zugangsdaten werden verschlüsselt in der Datenbank des Auftragsverarbeiters gespeichert. Die zur Entschlüsselung erforderlichen Schlüssel werden von der Infrastruktur des Auftragsverarbeiters selbst vorgehalten, da die vereinbarte, auch nutzerunabhängige Verarbeitung (z. B. Hintergrundindexierung) eine Entschlüsselung durch den Auftragsverarbeiter technisch voraussetzt; eine Architektur, bei der ausschließlich der Auftraggeber zur Entschlüsselung in der Lage ist, ist mit dieser Funktionalität nicht vereinbar.
2. Der Zugriff auf die eigene Infrastruktur des Auftragsverarbeiters sowie auf die Entschlüsselungsschlüssel ist auf einen eng begrenzten, namentlich bestimmten Kreis autorisierten Fachpersonals beschränkt, das durch die üblichen arbeitsvertraglichen Vertraulichkeitsverpflichtungen gebunden ist. Da sich Drittsysteme des Auftraggebers (z. B. der SMB-Server) außerhalb der eigenen Infrastruktur des Auftragsverarbeiters befinden und von diesem weder betrieben noch administriert werden, erfolgt eine lückenlose, manipulationssichere Protokollierung der dort vorgenommenen Handlungen konsequent auf Ebene dieses Drittsystems selbst – dort, wo sie technisch zuverlässig umgesetzt werden kann. Dem Auftraggeber wird empfohlen, eine entsprechende, unabhängige Protokollierung auf Ebene seiner eigenen Infrastruktur vorzusehen.
3. Dem Auftraggeber wird empfohlen, dem Auftragsverarbeiter ausschließlich Zugangsdaten mit dem für den vorgesehenen Zweck erforderlichen Mindestumfang an Berechtigungen bereitzustellen (z. B. lesenden Zugriff, beschränkt auf die benötigten Freigaben bzw. Verzeichnisse) und eine Protokollierung von Zugriffen auf die Freigabe auf Ebene des eigenen Drittsystems vorzusehen.

2. Integrität

2.1 Eingabekontrolle

1. Eingegebene, veränderte oder gelöschte Daten können über Journal- bzw. Änderungsprotokolle sowie das Dual Audit Log (Provider- und Deployer-Log, Hash-Chain-unveränderlich) nachträglich überprüft werden.
2. Schutz vor SQL-Injection durch parametrisierte Abfragen; SSRF-Schutz über einen dedizierten Outbound-Proxy; Schema-Validierung auf allen API-Endpunkten; Webhook-Verifizierung über HMAC-SHA256.

Der Zugriff auf vom Auftraggeber im Rahmen des optionalen Fernzugriffs (vgl. Ziffer 1.1) bereitgestellte virtuelle Maschinen ist auf einen eng begrenzten, namentlich bestimmten Kreis autorisierten Fachpersonals beschränkt, das durch die üblichen arbeitsvertraglichen Vertraulichkeitsverpflichtungen gebunden ist. Da sich die virtuelle Maschine außerhalb der eigenen Infrastruktur des Auftragsverarbeiters befindet und von diesem weder betrieben noch administriert wird, erfolgt eine lückenlose, manipulationssichere Protokollierung sämtlicher Zugriffe und Handlungen konsequent auf Ebene der vom Auftraggeber selbst betriebenen Netzwerk- bzw. Systemumgebung – dort, wo sie technisch zuverlässig umgesetzt werden kann. Dem Auftraggeber wird empfohlen, eine entsprechende, unabhängige Protokollierung in seiner eigenen Infrastruktur vorzusehen.

2.2 Weitergabekontrolle

1. Es werden ohne Weisung des Auftraggebers keine Daten an Dritte weitergegeben; es findet kein Training auf Kundendaten statt.
2. Der Zugriff von mobilen Arbeitsplätzen oder aus dem Home-Office auf interne Systeme erfolgt ausschließlich über verschlüsselte Verbindungen (SSL/VPN).
3. Der Fernzugriff auf vom Auftraggeber bereitgestellte virtuelle Maschinen zum Zweck der Installation des Relay-Docker-Containers (vgl. Ziffer 1.1) erfolgt ausschließlich über verschlüsselte Standardprotokolle (SSH oder RDP).

3. Verfügbarkeit und Belastbarkeit, Wiederherstellbarkeit

1. Die Rechenzentren sind klimatisiert und verfügen über eine CO2-Feuerlöschanlage.
2. Die Serverinfrastrukturen sind durch eine unterbrechungsfreie Stromversorgung (USV) gegen Stromausfall abgesichert.
3. Die Datenspeicher sind durch redundante RAID-Systeme gegen Ausfall gesichert.
4. Relevante Serversysteme sind als virtuelle Maschinen in einem Cluster gegen den Ausfall von Serverhardware abgesichert.
5. Alle Systeme werden mindestens täglich gesichert (Anwendungsserver als Gesamtsystem und zusätzlich auf Anwendungsebene zur granularen Wiederherstellung).
6. Alle Sicherungen werden verschlüsselt an zwei räumlich getrennten Orten gespeichert.
7. Alle Systeme werden durch einen aktuellen Viren-/Malwarescanner geschützt; die Signaturen werden mehrmals täglich aktualisiert.
8. Die Code-Ausführung erfolgt in isolierten Sandboxes; das Monitoring ist self-hosted, ohne externe Telemetrie.
9. Für betriebskritische IT-Infrastrukturen besteht ein Desaster-Recovery-Konzept; es werden regelmäßige Wiederherstellungstests durchgeführt**.**

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. Verzeichnis von Verarbeitungstätigkeiten geführt und gepflegt; Datenschutzbeauftragter: Henrik Simmack (dpo@oneai.eu); allgemeiner Datenschutz-Kontakt: privacy@oneai.eu; Datenschutz-Managementsystem etabliert.
2. Incident-Response-Management vorhanden; Mitarbeitende auf Vertraulichkeit verpflichtet und datenschutzrechtlich geschult.

5. Auftragskontrolle

1. Auswahl von Unterauftragsverarbeitern unter besonderer Berücksichtigung von Datenschutz und Datensicherheit.
2. Keine Verarbeitung durch Unterauftragsverarbeiter ohne Abschluss eines AVV/DPA (vgl. Anlage 1).

Hinweis zur Rechtsverbindlichkeit: Diese Vereinbarung ist in deutscher Sprache abgefasst und allein rechtsverbindlich. Etwaige Übersetzungen dienen ausschließlich Informationszwecken.

Data Processing Agreement (Courtesy English Translation)

This is a non-binding courtesy translation. Pursuant to the final clause of the German version, the German text is drafted in German and is solely legally binding; any translation serves information purposes only.

Data Processing Agreement

pursuant to Art. 28 GDPR

Version: 2.2 · As of: 6 November 2026

This Data Processing Agreement applies between oneAI GmbH, Eisenbahnstraße 50, 72072 Tübingen, Germany (hereinafter "Processor") and the respective Customer who accepts oneAI GmbH's Terms of Use (EULA) and General Terms and Conditions (GTC) (hereinafter "Controller"). Controller and Processor are hereinafter individually also referred to as a "Party" and jointly as the "Parties". This Agreement automatically becomes part of the contractual relationship between oneAI GmbH and each Customer upon acceptance of the Terms of Use, without the need for separate signature.

Preamble

To specify the rights and obligations arising from the data processing relationship under the statutory requirements of Art. 28 GDPR, the Parties conclude the following Agreement. This Agreement supplements the Terms of Use (EULA) and General Terms and Conditions (GTC) of oneAI GmbH existing between the Parties, which together form the contractual basis for the use of the oneAI SaaS platform (hereinafter jointly the "Main Agreement").

1 Subject Matter and Duration of the Engagement

1.1 Subject Matter of the Engagement

The subject matter of the engagement is the performance of the following tasks:

The Processor provides the Controller with the provisioning and operation of the OneAI SaaS platform (hub.oneai.eu) on the basis of the Main Agreement. This includes in particular AI-assisted text and chat processing, RAG-based document search, management of Spaces and uploaded content, and audit logging. For the individual services, reference is made to the service description of the Main Agreement.

The processing of personal data is carried out in accordance with the model operation mode selected by the Controller:

Standard models (self-hosted) and Private Models – processing exclusively within the infrastructure of the Processor or the Controller;

“EU Models” (EU-flag models) – processing via Google Vertex AI Model Garden in the EU region;

Public Models – external model providers to be actively selected by the Controller; the guarantees set out in Annex 1 additionally apply in this respect.

At the Controller's express request, or where expressly agreed in the Main Agreement or the relevant individual order – in particular where installation is not carried out by an implementation partner engaged by the Controller – the Processor additionally provides the following optional service: the Controller provides the Processor with a ready-to-use, isolated virtual machine within its own network. The Processor connects to this VM solely for the purpose of installing and configuring a Relay Docker container, which enables the Controller's local SMB shares to be connected to the oneAI cloud platform. The Processor does not create or operate the virtual machine itself; provisioning, operation and security of the VM are the Controller's responsibility. In the course of this activity, the Processor has no access to the SMB share itself, as it does not hold the credentials required for this; access is limited to the network level of the provided VM for the purpose of container installation and configuration. No third-country transfer is involved. Following successful installation and configuration, the access granted to the Processor to the virtual machine is terminated; any renewed access (e.g. for updates or maintenance) shall only take place following renewed authorisation by the Controller.

1.2 Duration of the Engagement

The duration of this engagement corresponds to the term of the underlying Main Agreement. The Controller may terminate this Agreement at any time without notice if the Processor commits a serious breach of this Agreement or applicable data protection provisions, fails to carry out an instruction of the Controller, refuses to provide required information, or denies the Controller access in the context of audits. Following termination, the Processor may no longer process the Controller's personal data.

1.3 Remuneration

All services of the Processor in connection with the fulfilment of its obligations under this Agreement are covered by the remuneration under the underlying Main Agreement.

2 Details of the Subject Matter of the Engagement

2.1 Nature, Purpose and Permissibility of the Processing

The nature and purpose of the processing of personal data by the Processor arise from the Main Agreement and the associated service description. The Controller alone is responsible for assessing the permissibility of the processing.

2.2 Categories of Personal Data

The subject matter of the processing is all personal data that the Controller or its authorised users enter, upload or otherwise have processed in the course of using the Platform. Depending on use, this may in particular include: name and contact data, communication content, document content, IT access and authorisation management data, IT usage metadata, and other content entered by the Controller or its users. The determination of the categories of data actually processed is the sole responsibility of the Controller as controller, in the context of its own usage decisions. Note: When using Public Models, the Controller is obliged not to submit special categories of personal data under Art. 9 GDPR (e.g. health data) in prompts without an appropriate legal basis (cf. Main Agreement/Terms of Use). Where the Controller provides the Processor with access credentials to its own third-party systems in connection with certain connectors (e.g. SMB network shares), the special provisions in Annex 2, Clause 1.6 apply in addition.

2.3 Categories of Data Subjects

The circle of data subjects is determined by the Controller's own use of the Platform and may in particular include: employees of the Controller, customers and business partners of the Controller, applicants, and other natural persons whose personal data the Controller or its authorised users enter in the course of using the Platform. The determination of the categories of data subjects actually affected is the sole responsibility of the Controller as controller.

3 Technical and Organisational Measures

3.1 The Processor takes appropriate technical and organisational measures for the adequate protection of personal data, as required by Art. 28(3) sentence 2(c) GDPR in conjunction with Art. 32(1) GDPR, in order to ensure the security of the processing. To this end, the Processor ensures:

the ongoing confidentiality, integrity, availability and resilience of the systems and services in connection with the processing;

the ability to rapidly restore the availability of and access to personal data in the event of a physical or technical incident.

3.2 The Parties agree on the measures set out in detail in Annex 2 (“Technical and Organisational Measures”) to this Agreement. These apply to the entire operation of the OneAI platform; insofar as parts of the infrastructure are provided by a sub-processor (see Annex 1), its measures are included in the protection level described.

3.3 The measures are subject to technical progress. The Processor is permitted to implement alternative, adequate measures in line with the state of the art, provided the security level of the defined measures is not undercut. Material changes must be documented and communicated to the Controller in text form.

4 Third-Country Transfer

4.1 When using self-hosted standard models, “EU Models” (EU-flag models) (Google Vertex AI Model Garden, EU region) and Private Models, processing takes place exclusively within the European Union or a contracting state of the EEA Agreement; no third-country transfer occurs in this respect.

4.2 A transfer to a third country is only permitted under the following conditions:

an adequacy decision under Art. 45 GDPR exists for the country concerned;

the Processor provides appropriate safeguards under Art. 46 or 47 GDPR (in particular EU Standard Contractual Clauses under Implementing Decision (EU) 2021/914);

the transfer is necessary for the establishment, exercise or defence of legal claims in connection with specific administrative, judicial or regulatory proceedings; or

the transfer is necessary to protect the vital interests of the data subject or another natural person.

4.3 A transfer to a Public Model located outside the EU/EEA (e.g. OpenAI, USA) occurs exclusively as a result of the deliberate selection of a Public Model not marked as “EU” (EU flag) by the Controller or its users. Standard models (self-hosted), “EU” (EU flag) models and Private Models do not trigger any third-country transfer. By selecting such a Public Model, the

Controller gives the Processor the documented instruction under Art. 28(3) sentence 2(a) GDPR to transfer the relevant data to the selected provider; the Controller, as controller, alone decides whether and where the transfer takes place. If no such selection is made, no third-country transfer occurs. The Controller may further use the Platform's administration functions to technically control which models are available to its users, and in particular may deactivate (technically exclude) Public Models not marked as “EU” (EU flag) and Private Models organisation-wide. If the Controller makes use of this, a third-country transfer via model selection is technically excluded.

4.4 The transfer associated with such a selection is based on the guarantees set out in Annex 1 (EU Standard Contractual Clauses under Implementing Decision (EU) 2021/914 in conjunction with the respective providers' Data Processing Addenda). Every transfer must comply with all contractual obligations under this Agreement, in particular the purpose limitation. The assessment of the permissibility of the transfer in the specific individual case – in particular with regard to the content entered – is the responsibility of the Controller as controller, where applicable in the context of its data protection impact assessment (Art. 35 GDPR).

5 Rectification, Erasure and Restriction of Data

5.1 The Processor may only rectify, erase or restrict the processing of data processed under the engagement in accordance with the Controller's instructions (Art. 28(3) sentence 2(a) GDPR).

5.2 If a data subject approaches the Processor directly with a request for immediate rectification or erasure of their personal data, the Processor shall forward the request to the Controller without undue delay.

5.3 Insofar as covered by the scope of services, the Processor shall ensure, in accordance with the Controller's documented instructions, the rights to erasure, to be forgotten, to rectification, to data portability and to information without undue delay.

6 Audits and Other Obligations of the Processor

In addition to the obligations under this Agreement, the Processor shall comply with the statutory obligations under Art. 28 to 33 GDPR; in particular:

a) The Processor's data protection officer is Mr Henrik Simmack, Hinter Gärten 8, 72459 Albstadt, Germany, e-mail: dpo@oneai.eu. For general data protection enquiries, the Processor can additionally be reached at: privacy@oneai.eu. Any change in the person or contact details of the data protection officer will be notified to the Controller without undue delay in text form.

b) The Processor and any person subordinate to it who has access to the Controller's personal data may only process such data in accordance with the Controller's instructions under Clause 10 of this Agreement, unless they are obliged to process it under Union or Member State law (Art. 28(3) sentence 2(a), Art. 29 GDPR).

c) The Processor shall only deploy persons who are bound to confidentiality and have been made familiar with the relevant data protection provisions (Art. 28(3) sentence 2(b) GDPR). This obligation continues to apply after termination of this Agreement and/or the Main Agreement.

d) The Processor shall cooperate with the supervisory authority in the performance of its tasks.

e) The Processor shall inform the Controller without undue delay of any audit actions and measures of the supervisory authority insofar as they relate to this engagement.

f) The Processor shall support the Controller to the best of its ability in connection with supervisory authority audits, administrative or criminal proceedings, claims for damages by data subjects or third parties, and other claims in connection with the processing.

g) The Processor shall regularly review its internal processes and the technical and organisational measures to ensure that processing within its area of responsibility complies with applicable data protection law and that the rights of data subjects are safeguarded.

h) The Processor shall demonstrate the technical and organisational measures taken to the Controller within the scope of its audit rights under Clause 8.

7 Sub-Processing Relationships

7.1 Sub-processing relationships within the meaning of this Agreement are services directly related to the performance of the principal service. This does not include ancillary services used by the Processor, e.g. telecommunications, postal/transport or disposal services. However, the Processor remains obliged to ensure data protection and data security for the Controller's data by appropriate and lawful contractual arrangements and control measures, even for such ancillary services.

7.2 The Processor is entitled to engage the sub-processors named in Annex 1 to process the Controller's personal data. The engagement of further or other sub-processors shall be communicated to the Controller in text form. If the Controller does not object in text form within 30 days of receipt of this notification, the change is deemed approved. An objection is only valid and relevant if the Controller demonstrates, in text form within this period, objectively and comprehensibly, that and for which specific reasons the engagement of the new or changed sub-processor reduces the level of protection or security owed under this Agreement, the GDPR, or Regulation (EU) 2024/1689 (EU AI Act), or violates mandatory requirements of these provisions. Unsubstantiated objections, as well as objections based exclusively on economic, competitive, strategic or other considerations not grounded in data protection or security law, are invalid. If, following a valid objection, no amicable solution is reached within a further period of 14 days, the Controller shall have a right of extraordinary termination with respect to the part of the service affected by the sub-engagement.

7.3 If the Processor performs the agreed service with the involvement of sub-processors outside the EU/EEA, it shall ensure that the data protection permissibility is guaranteed – in particular through the guarantees under Clause 4. The sub-processor shall be subject to the same data protection obligations as set out in this Agreement, with sufficient guarantees of appropriate technical and organisational measures (Art. 28(4) sentence 1 GDPR).

8 Controller's Audit Rights

8.1 The Controller has the right, in consultation with the Processor, to carry out audits or have them carried out by an auditor bound to confidentiality. The Controller has the right to satisfy itself of compliance with the technical and organisational measures by means of random checks, generally once a year or on a specific occasion (Art. 28(3) sentence 2(h) GDPR).

8.2 The Processor shall ensure that the Controller can satisfy itself of compliance with the obligations. It is obliged, upon request, to provide the Controller with the necessary information and in particular to demonstrate the implementation of the technical and organisational measures (Art. 28(3) sentence 2(h) GDPR).

8.3 Evidence of such measures may be provided by current certificates, reports or report extracts from independent bodies (e.g. auditors, data protection auditors, quality auditors), suitable certification (e.g. IT security or data protection audit), or other suitable measures.

9 Support of the Controller, Notification of Breaches by the Processor

The Processor shall support the Controller in complying with the obligations set out in Art. 32 to 36 GDPR regarding the security of personal data, breach notification obligations, data protection impact assessments and prior consultations. This includes in particular:

a) ensuring an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing and the likelihood and severity of potential infringements, and that enable the immediate detection of relevant breach events;

b) the obligation to document and notify the Controller without undue delay of breaches of the protection of personal data (Art. 33(2) GDPR), and to take appropriate measures, in coordination with the Controller, to secure the data and mitigate possible adverse effects;

c) supporting the Controller (Art. 28(3) sentence 2(e) GDPR) with its notification obligation to the supervisory authority or the data subject;

d) supporting the Controller with its information obligation towards the data subject and providing all relevant information upon request.

10 Controller's Right to Issue Instructions, Instruction-Bound Processing

10.1 The Controller has a comprehensive right to issue instructions to the Processor regarding the nature, scope and method of data processing.

10.2 Data may only be processed within the scope of this Agreement and in accordance with the Controller's instructions. The Processor is prohibited from using the data for other purposes or disclosing it to third parties without the Controller's knowledge. Copies or duplicates are not made without the Controller's knowledge; excluded from this are backup copies insofar as they are necessary to ensure proper processing.

10.3 Instructions from the Controller shall be documented by the Processor. Verbal instructions shall be confirmed without undue delay in text or written form.

10.4 Changes to the subject matter and procedure of the processing shall be agreed jointly and documented. Processed personal data shall only be forwarded to third parties or the data subject with the Controller's prior consent in text form.

10.5 If the Processor is of the opinion that an instruction violates data protection provisions, it shall notify the Controller without undue delay. The Processor is entitled to suspend implementation of the instruction concerned until it is confirmed or amended by the Controller (Art. 28(3) sentence 3 GDPR).

10.6 No training on customer data. The Processor never uses the Controller's personal data to train its own or third-party AI models. For self-hosted standard models this is technically enforced; for Public Models this is contractually secured via the respective providers' Data Processing Addenda (no-training clauses, and for Mistral additionally through an activated training opt-out).

11 Liability

11.1 The liability of the Parties is governed by statutory provisions, in particular Art. 82 GDPR. The Processor is only liable for damage caused by the processing if it has failed to comply with the obligations under the GDPR specifically addressed to processors, or has acted outside of or contrary to the Controller's lawful instructions (Art. 82(2) sentence 2 GDPR).

11.2 In their internal relationship, the Parties bear the damage in proportion to their respective share of responsibility and fault (Art. 82(5) GDPR). Insofar as the Controller, as controller, issues instructions, enters content into the Platform, or selects models or Public Model providers, it bears the resulting data protection responsibility.

11.3 A Party is released from liability if it proves that it is not in any way responsible for the event giving rise to the damage (Art. 82(3) GDPR).

11.4 Any limitations and caps on liability under the Main Agreement also apply to claims arising from or in connection with this Agreement, insofar as legally permissible. They do not apply in cases of intent and gross negligence, injury to life, body or health, direct statutory claims of data subjects, or sanctions under Art. 83 GDPR.

12 Deletion of Data and Return of Data Carriers

12.1 Copies or duplicates of the data are not made without the Controller's knowledge. Excepted are necessary backup copies to ensure proper data processing and data required to comply with statutory retention obligations.

12.2 Upon completion of the contractually agreed work or at the Controller's request – at the latest upon termination of the Main Agreement – the Processor shall, at the Controller's choice, return or delete all documents in its possession and all processing or usage results created in connection with the engagement (Art. 28(3) sentence 2(g) GDPR). This also applies to test data and discarded material. The deletion log shall be presented upon request.

12.3 Documentation serving as evidence of proper, contract-compliant data processing shall be retained by the Processor beyond the end of the contract in accordance with the applicable retention periods. It may hand these over to the Controller at the end of the contract for its own exoneration.

13 Miscellaneous, Amendment of this Agreement

13.1 Should individual provisions of this Agreement be or become invalid or unenforceable, this shall not affect the validity of the remaining provisions. The invalid or unenforceable provision shall be replaced by the valid and enforceable provision that comes closest to the economic purpose of the original provision. The same applies to any gaps in the Agreement.

13.2 This Agreement is governed by German law. The exclusive place of jurisdiction for disputes arising from or in connection with this Agreement is, to the extent legally permissible, Tübingen.

13.3 Changes to this Agreement will be announced to the Controller by e-mail or via the Platform at least six (6) weeks before the intended effective date. The Controller's consent is deemed given if it does not object in writing before the intended date; the Controller will be separately notified of this legal consequence in the change notification. A material change to the subject matter of the contract (principal obligations) by way of unilateral amendment is excluded. This does not affect the Parties' obligation to adapt this Agreement insofar as this becomes necessary due to a change in applicable data protection laws or binding requirements

of the European Commission or the competent supervisory authorities. The engagement or replacement of sub-processors is governed exclusively by the provision in Clause 7.2; the preceding paragraphs of this Clause 13.3 do not apply to this.

Annex 1 – List of Sub-Processors

List of sub-processors engaged by the Processor with the Controller's consent (with verified business addresses). The list is set out below; changes will be communicated in accordance with Clause 7.2.

Note: Providers and data transfers not used to provide the core service to the Controller – in particular payment and e-mail service providers, as well as connector target systems connected by the Controller itself (e.g. Microsoft, Google, GitHub, ClickUp, weclapp) – are not the subject of this engagement. Connector target systems fall within the Controller's area of responsibility and are connected solely at its instigation and on the basis of its own contractual relationships.

No.	Provider	Address	Purpose	Guarantee (Third Country)
1	Google Ireland Ltd. (Reg. No. 368047) – Vertex AI Model Garden	Gordon House, Barrow Street, Dublin 4, D04 E5W5, Ireland	LLM inference “EU” (EU-flag) models (Gemini, Claude); Anthropic as sub-processor of Google	Google Cloud CDPA, EU region (no third-country transfer)
2	OpenAI OpCo, LLC (EEA/Switzerland: OpenAI Ireland Ltd.)	OpCo: 1455 3rd Street, San Francisco, CA 94158, USA · Ireland: 1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	LLM inference (Public Models), audio transcription (whisper-1)	DPA + EU SCCs (2021/914)
3	Mistral AI SAS (R.C.S. Paris 952 418 325)	15 rue des Halles, 75001 Paris, France	LLM inference (Public Model)	DPA, training opt-out + zero data retention; no third-country transfer
4	Hetzner Online GmbH (HRB 6089 Ansbach)	Industriestr. 25, 91710 Gunzenhausen, Germany	Cloud hosting (infrastructure, incl. self-hosted AI models)	DPA (no third-country transfer)

5	relyon AG (HRB 766138 Stuttgart)	Eisenbahnstraße 50, 72072 Tübingen, Germany	Operation of the non-GPU-intensive infrastructure (application, database, file and vector storage, audit log) on its own hardware as colocation in the Hetzner data centre	DPA (no third-country transfer)
6	weber.digital GmbH (HRB 411104)	Zollernstraße 49, 72336 Balingen, Germany	LLM inference (Public Models)	DPA (no third-country transfer)
7	Scaleway S.A.S. (R.C.S. Paris 433 115 904)	8 rue de la Ville l'Évêque, 75008 Paris, France	Cloud hosting (infrastructure, including application, database, vector and file storage)	DPA (no third-country transfer)

Annex 2 – Technical and Organisational Measures

The following technical and organisational measures implemented and guaranteed by oneAI GmbH pursuant to Art. 32 GDPR are set out below. The OneAI platform is operated on servers in the ISO 27001-certified data centre of Hetzner Online GmbH (Germany), supplemented by an additional, likewise ISO 27001-certified secondary/backup capacity with Scaleway S.A.S. (France, see Annex 1); the non-GPU-intensive infrastructure is provided by the infrastructure sub-processor relyon AG (see Annex 1). The measures set out below apply to the entire operation of the OneAI platform.

1. CONFIDENTIALITY

1.1 Physical Access Control

oneAI GmbH employees are trained in handling and maintaining the confidentiality of sensitive data.

oneAI GmbH's office and operational premises are secured with an electronic locking system; electronic keys are issued only to authorised persons, and issuance is logged.

Business premises are locked and may only be entered by authorised persons with a key.

The OneAI platform's servers are located in the ISO 27001-certified data centre of Hetzner Online GmbH (Germany). The data centre premises are staffed around the clock by the data centre operator's personnel and are alarm- and video-monitored.

Visitors to data centre premises are collected at the entrance and entered in a visitor list; access is only possible with valid identification documents.

Important documents are stored in lockable cabinets; only authorised persons receive keys.

1.2 Access Control (Authentication)

Passwordless-first: authentication via WebAuthn/passkeys (FIDO2); no standard password-based login.

Single sign-on via Microsoft Entra ID (OAuth 2.0) and Google Sign-In; administrative access is role-based, additionally protected by conditional access policies and mandatory multi-factor authentication (MFA).

All employees receive a personalised user account; passwords are not shared. Where passwords are used, a complexity policy applies requiring at least 15 characters (upper/lower case, numbers, special characters).

Automated user provisioning and deprovisioning via Enterprise SCIM 2.0.

The network is protected by a rule-based, regularly reviewed firewall; spam filters and anti-virus/malware protection with signatures updated several times daily.

Mobile devices contain no unencrypted personal data; a Mobile Device Management (MDM) system is in use.

Session management: 24-hour expiry, session tokens SHA-256-hashed; API keys with an optional expiry date, stored encrypted.

External service providers are only engaged with a concluded data processing agreement; their access is limited to the required extent.

1.3 Access Control (Authorisation)

A role-based permission concept (RBAC) exists for all systems and storage at organisation and space level (read/write/admin).

Strict tenant separation at database level; every operation is authenticated and assigned to its tenant.

User accounts of departed employees are blocked immediately upon termination of employment and deleted after a transitional period.

Access to applications containing personal data is logged; logs are retained for 14 days.

Data carriers no longer required or intended for reuse are manually destroyed or securely erased by repeated overwriting.

Access to virtual machines provided by the Controller in connection with the optional remote access service (cf. Clause 1.1) is restricted to authorised personnel only. Shared credentials are not used for this purpose; each accessing person authenticates using a personal SSH key or an individual user account.

1.4 Separation

Data of different tenants is separated logically and at the network level via VLANs defined in the security architecture; network segments are separated by a firewall.

Production systems are separated from test and development environments.

1.5 Pseudonymisation & Encryption

All personal data is encrypted during transmission by appropriate measures (TLS 1.2+/HTTPS, VPN).

Provider API keys at rest are encrypted with XChaCha20-Poly1305 (Cure53-audited library); stored passwords and credentials are held encrypted in a password safe.

Backups are separately encrypted; central secrets management, no hard-coded credentials.

1.6 Access Credentials to the Controller's Third-Party Systems (e.g. SMB Network Shares)

Where the Controller provides the Processor with access credentials to its own third-party systems in connection with the use of certain connectors (e.g. to connect SMB network shares), the following applies in addition: the credentials are stored encrypted in the Processor's database. The keys required for decryption are held by the Processor's own infrastructure, since the agreed processing — including processing independent of the user being online (e.g. background indexing) — technically requires decryption by the Processor; an architecture in which only the Controller is able to decrypt is not compatible with this functionality.

Access to the Processor's own infrastructure and to the decryption keys is restricted to a narrowly defined, named group of authorised specialist personnel, who are bound by the standard confidentiality obligations contained in their employment agreements. As the Controller's third-party systems (e.g. the SMB server) lie outside the Processor's own infrastructure and are neither operated nor administered by the Processor, complete, tamper-resistant logging of actions taken there is consistently carried out at the level of that third-party system itself – where it can be implemented reliably. The Controller is recommended to implement corresponding, independent logging within its own infrastructure.

The Controller is advised to provide the Processor only with credentials limited to the minimum scope of permissions required for the intended purpose (e.g. read-only access, restricted to the necessary shares or directories) and to maintain logging of access to the share at the level of its own third-party system.

2. INTEGRITY

2.1 Input Control

Entered, modified or deleted data can be subsequently verified via journal/change logs and the Dual Audit Log (Provider and Deployer log, immutable hash chain).

Protection against SQL injection via parameterised queries; SSRF protection through a dedicated outbound proxy; schema validation on all API endpoints; webhook verification via HMAC-SHA256.

Access to virtual machines provided by the Controller in connection with the optional remote access service (cf. Clause 1.1) is restricted to a narrowly defined, named group of authorised specialist personnel, who are bound by the standard confidentiality obligations contained in their employment agreements. As the virtual machine lies outside the Processor's own infrastructure and is neither operated nor administered by the Processor, complete, tamper-resistant logging of all access to and actions performed on that machine is consistently carried out at the level of the Controller's own network or system environment – where it can be

implemented reliably. The Controller is recommended to implement corresponding, independent logging within its own infrastructure.

2.2 Transfer Control

No data is disclosed to third parties without the Controller's instruction; no training takes place on customer data.

Access from mobile workplaces or home offices to internal systems is exclusively via encrypted connections (SSL/VPN).

Remote access to virtual machines provided by the Controller for the purpose of installing the Relay Docker container (cf. Clause 1.1) is carried out exclusively via encrypted standard protocols (SSH or RDP).

3. AVAILABILITY, RESILIENCE AND RECOVERABILITY

Data centres are air-conditioned and equipped with a CO2 fire suppression system.

Server infrastructures are protected against power outages by an uninterruptible power supply (UPS).

Data storage is protected against failure by redundant RAID systems.

Relevant server systems are secured as virtual machines in a cluster against server hardware failure.

All systems are backed up at least daily (application servers as a whole system and additionally at the application level for granular restoration).

All backups are stored encrypted at two geographically separate locations.

All systems are protected by up-to-date virus/malware scanners; signatures are updated several times daily.

Code execution takes place in isolated sandboxes; monitoring is self-hosted, with no external telemetry.

A disaster recovery concept exists for business-critical IT infrastructure; regular recovery tests are carried out.

4. PROCEDURE FOR REGULAR REVIEW, ASSESSMENT AND EVALUATION

Record of processing activities maintained and kept up to date; data protection officer: Henrik Simmack (dpo@oneai.eu); general data protection contact: privacy@oneai.eu; data protection management system established.

Incident response management in place; employees bound to confidentiality and trained in data protection law.

5. SUB-PROCESSOR CONTROL

Selection of sub-processors with particular regard to data protection and data security.

No processing by sub-processors without conclusion of a DPA (cf. Annex 1).

Note on legal validity: This Agreement is drafted in German and is solely legally binding. Any translations serve information purposes only.