

JOACHIM DREISTEIN MEDIENENTWICKLUNG, DÜSSELDORF

dAI Pro Managed Vertragspaket

Vertrag, Anlagen und Auftragsverarbeitung

29.09.2026

Angaben in eckigen Klammern werden je Kunde ausgefüllt.

Dieses Paket enthält:

- Vertrag dAI Pro Managed
- Anlage 1 · Leistungsbeschreibung
- Anlage 2 · Service Level
- Anlage 3 · Auftragsverarbeitung
- Anhang B · TOM
- Anlage 4 · Auftragsblatt Managed (Vorlage)

Nicht enthalten ist Anlage 5, die Allgemeinen Geschäftsbedingungen des Anbieters (Stand Juni 2026). Sie steht als eigene PDF auf www.dreistein.de/dai-pro/vertrag bereit.

Inhalt

Vertrag über Bereitstellung und Betrieb einer dAI Pro-Instanz („dAI Pro Managed“)	4
Präambel	4
§ 1 Vertragsgegenstand	4
§ 2 Pakete, Grenzen, Überschreitung	5
§ 3 Einrichtung	5
§ 4 Sprachmodelle und Dienste Dritter	6
§ 5 Bereitstellung, Betrieb, Updates	6
§ 6 Pflichten des Kunden	7
§ 7 Nutzungsrechte, Eigentum an Daten	9
§ 8 Zugriff des Anbieters auf die Instanz (Fernwartung)	9
§ 9 Datensicherung, Herausgabe, Löschung	10
§ 10 Vergütung	10
§ 11 Laufzeit und Kündigung	11
§ 12 Datenschutz	11
§ 13 Besondere Bestimmungen für KI-Ausgaben, Gewährleistung, Haftung	12
§ 14 Referenznennung	13
§ 15 Vertragsübernahme, Rechtsnachfolge, Schlussbestimmungen	13
Anlage 1 — Leistungsbeschreibung dAI Pro	15
1. Das Produkt	15
2. Begriffe	15
3. Pakete und Zählweise	16
4. Funktionen	17
5. Sprachmodelle und Dienste Dritter	21
6. Einrichtungspakete	22
7. Preise (Stand 8. September 2026, netto zuzüglich Umsatzsteuer)	22
8. Nicht Gegenstand der Leistung	23
Anlage 2 — Service Level und Betrieb („dAI Pro Managed“)	24
1. Verfügbarkeit	24
2. Wartung und Updates	25
3. Support und Störungsbeseitigung	25
4. Datensicherung	26
5. Überwachung, Protokolle, Löschrufen	26
6. Technischer Betrieb	26
7. Exit	28

Anlage 3 — Vereinbarung zur Auftragsverarbeitung (Art. 28 DSGVO) für „dAI Pro Managed“ sowie für Support und Fernwartung bei Selbstbetrieb (§ 1 Abs. 4)	29
Parteien	29
§ 1 Gegenstand, Dauer, Verhältnis zum Hauptvertrag	29
§ 2 Rollen und Abgrenzung	29
§ 3 Pflichten des Auftragnehmers	30
§ 4 Pflichten des Auftraggebers	31
§ 5 Weisungsberechtigte Personen	32
§ 6 Subunternehmer	32
§ 7 Kontrollrechte	33
§ 8 Löschung und Rückgabe	33
§ 9 Haftung	33
§ 10 Schlussbestimmungen	34
Anhang A — Verarbeitung im Einzelnen	34
Anhang B — Technische und organisatorische Maßnahmen	37
Anhang C — Subunternehmer	37
Anhang D — Fernwartung und Support bei Selbstbetrieb (Verträge „dAI Pro-Web“ und „dAI Pro-TYPO3“)	40
Anhang E — Verpflichtung nach § 203 Abs. 4 StGB (nur bei Auftraggebern, die Berufsgeheimnisträger sind)	41
Technische und organisatorische Maßnahmen (Art. 32 DSGVO) — dAI Pro Managed	42
1. Vertraulichkeit	42
2. Integrität	44
3. Verfügbarkeit und Belastbarkeit	45
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung	45
Anlage 4 — Auftragsblatt zum Vertrag „dAI Pro Managed“	47
1. Parteien und Ansprechpartner	47
2. Instanz und Nutzung	47
3. Paket und Vergütung	48
4. Sprachmodelle und Sprachdienste	48
5. Datenschutz und Inhalte	49
6. Betrieb	49
7. Unterschriften	50

Vertrag über Bereitstellung und Betrieb einer dAI Pro-Instanz („dAI Pro Managed“)

zwischen

Joachim Dreistein Medienentwicklung, Inhaber Joachim Dreistein, Bolkerstraße 14, 40213 Düsseldorf, E-Mail info@dreistein.de, nachfolgend „Anbieter“

und

[KUNDE, Rechtsform], [Anschrift], vertreten durch [Name, Funktion], nachfolgend „Kunde“

Präambel

Der Anbieter hat die Software **dAI Pro** entwickelt. Sie macht die Inhalte des Kunden (Website, Dokumente, Datenbanken, Ticketsysteme und weitere Datenquellen) durch einen KI-Assistenten befragbar, der ausschließlich aus diesen Inhalten und mit Quellenangabe antwortet, und stellt Werkzeuge zur Pflege und Prüfung dieser Wissensbasis bereit (Agenten, Qualitätsprüfung, Eingang). Der Anbieter betreibt die Software für den Kunden als eigene, technisch getrennte Instanz auf Servern des Anbieters in der Europäischen Union. Der Kunde bringt den Zugang zum Sprachmodell seiner Wahl selbst ein.

§ 1 Vertragsgegenstand

1. Der Anbieter stellt dem Kunden für die Vertragslaufzeit eine eigene Instanz der Software dAI Pro („Instanz“) zur Nutzung über das Internet bereit und betreibt sie (Software as a Service). Die Instanz ist unter der Adresse `[kundenname].dreistein.de` [alternativ: unter der vom Kunden bereitgestellten Domain [...], für die der Kunde die erforderlichen DNS-Einträge setzt] erreichbar.
2. Der Funktionsumfang der Software ergibt sich aus **Anlage 1 (Leistungsbeschreibung)**. Der Kunde wählt dort ein Paket; das gewählte Paket und die zugehörigen Grenzen (Datensätze, Datenquellen, Agenten) sind in **Anlage 4 (Auftragsblatt)** festgehalten.
3. Betrieb, Verfügbarkeit, Wartung, Datensicherung und Support richten sich nach **Anlage 2 (Service Level und Betrieb)**.
4. Die Verarbeitung personenbezogener Daten im Auftrag des Kunden regelt die **Vereinbarung zur Auftragsverarbeitung (Anlage 3)** mit ihren Anhängen.
5. Die Einrichtung der Instanz (Anbindung der Datenquellen, erste Indexierung, Einbau des Chats in die Website des Kunden, Übergabe) ist eine einmalige Leistung nach § 3.
6. Individuelle Erweiterungen der Software für den Kunden (Kunden-Extras), Schulungen über das gewählte Einrichtungspaket (Anlage 1 Abschnitt 6) hinaus und weitere Beratungsleistungen sind nicht Gegenstand dieses Vertrags und werden gesondert beauftragt (AGB Abschnitte II und V).
7. Das Dokument „Rechtshinweise und Textbausteine“ des Anbieters ist ein Informationsdokument und kein Vertragsbestandteil.

§ 2 Pakete, Grenzen, Überschreitung

1. Das gewählte Paket bestimmt (a) die erlaubten Agenten-Typen, (b) die erlaubte Anzahl der Datenquellen und (c) die maximale Anzahl der Datensätze der Instanz („Paketmaximum“). Was als Datensatz und als Datenquelle zählt, definiert Anlage 1 Abschnitt 3; die Zahl ist für den Kunden jederzeit in der Oberfläche der Instanz ablesbar.
2. Überschreitet die Instanz das Paketmaximum, zeigt die Software dem Kunden auf jeder Seite einen Hinweis; der Anbieter erhält eine Benachrichtigung. Bis zur Karenzgrenze, das ist das Paketmaximum zuzüglich 10 %, bleibt die Instanz uneingeschränkt nutzbar. Die konkrete Karenzgrenze wird im Auftragsblatt beziffert.
3. Ab der Karenzgrenze legt die Software keine neuen Datensätze mehr an; bestehende Datensätze bleiben nutzbar und aktualisierbar, der Chat und alle übrigen Funktionen laufen weiter. Die Software zeigt dem Kunden die Sperre deutlich an.
4. Der Kunde entscheidet nach dem Hinweis, ob er Datensätze entfernt oder in ein höheres Paket wechselt. Ein automatischer Paketwechsel oder eine stillschweigende Nachberechnung findet nicht statt. Erklärt der Kunde in Textform den Wechsel in ein höheres Paket, hebt der Anbieter die Grenzen unverzüglich an; die höhere Vergütung ist ab dem auf den Zugang der Erklärung folgenden Monat geschuldet. Ein Wechsel in ein niedrigeres Paket ist zum Ende der jeweiligen Laufzeit nach § 11 möglich und setzt voraus, dass die Instanz die Grenzen des niedrigeren Pakets einhält.
5. Die erlaubte Anzahl der Datenquellen und die erlaubten Agenten-Typen setzt die Software unmittelbar durch: Weitere Datenquellen lassen sich nicht anlegen, nicht erlaubte Agenten-Typen stehen nicht zur Auswahl und werden nicht ausgeführt.
6. Für Bestände oberhalb der höchsten Paketstufe (Anlage 1) unterbreitet der Anbieter auf Anfrage ein individuelles Angebot.

§ 3 Einrichtung

1. Der Anbieter richtet die Instanz nach dem in Anlage 4 gewählten Einrichtungspaket ein. Die Leistungsinhalte der Einrichtungspakete beschreibt Anlage 1 Abschnitt 6.
2. Die Einrichtung ist eine Werkleistung nach AGB Abschnitt II. Sie ist abnahmereif, wenn die vereinbarten Datenquellen indexiert sind, der Chat in die Website des Kunden eingebaut oder Einbettungs-Code und Anleitung an den Kunden übergeben sind und der Anbieter die Übergabe in Textform erklärt hat. Die Abnahme richtet sich nach AGB § 16 Abs. 2 (Abnahmefiktion bei Produktivnahme oder nach 14 Tagen).
3. Der Kunde stellt für die Einrichtung rechtzeitig bereit: die zu indexierenden Quellen mit Zugangsdaten, soweit erforderlich; den API-Schlüssel des von ihm gewählten Sprachmodell-Anbieters (§ 4); einen fachlich zuständigen Ansprechpartner; Zugang zur Website oder Weisung an seine Agentur für den Einbau des Chats (AGB § 3).
4. Leistungen über das gewählte Einrichtungspaket hinaus (Inhaltsaufbereitung, zusätzliche Datenquellen, Schulungen, Anpassungen) vergütet der Kunde nach Aufwand zu dem im Auftragsblatt genannten Stundensatz (AGB § 7).

§ 4 Sprachmodelle und Dienste Dritter

1. Die Software arbeitet mit Sprachmodellen, Einbettungsmodellen und Sprachdiensten Dritter (Anlage 1 Abschnitt 5). Im Regelfall wählt der Kunde den Anbieter, schließt den Nutzungsvertrag und eine gegebenenfalls erforderliche Datenschutzvereinbarung selbst, hinterlegt seinen eigenen API-Schlüssel und trägt die dort anfallenden Nutzungsentgelte. Optional kann der Anbieter für die Ersteinrichtung ein einmaliges Startkontingent über sein Mistral-AI-Konto bis zu einem Gegenwert von 10,00 € bereitstellen, wenn dies im Auftragsblatt ausgewählt ist. Das Startkontingent ist eine unentgeltliche einmalige Zusatzleistung, endet mit Verbrauch des Kontingents und begründet keinen Anspruch auf weitere Nutzung über den Zugang des Anbieters. Es wird ausschließlich über einen Mistral-Dienst bzw. -Plan erbracht, für den die Verarbeitung für diesen Einsatz nach den bei Aktivierung geltenden Vertrags- und Datenschutzunterlagen in der Europäischen Union erfolgt; die konkrete Verarbeitungsregion wird vor Aktivierung dokumentiert. Für diese Nutzung ist Mistral AI Unterauftragsverarbeiter des Anbieters; die Verarbeitung erfolgt nur bei bestehender Auftragsverarbeitungsvereinbarung nach Anlage 3 und nach Maßgabe von deren § 6 und Anhang C. Spätestens nach Verbrauch des Startkontingents hinterlegt der Kunde seinen eigenen API-Schlüssel, sofern nicht ausdrücklich eine gesonderte dauerhafte Nutzung über einen Zugang des Anbieters vereinbart wird.
2. Der Kunde ist dafür verantwortlich, dass die Nutzung des gewählten Anbieters mit seinen datenschutzrechtlichen Pflichten vereinbar ist, insbesondere bei Anbietern mit Sitz oder Unterauftragnehmern außerhalb der EU (Anlage 3 § 4 Abs. 2). Die Software zeigt für jede Sammlung an, in welcher Region die beteiligten Dienste verarbeiten (Verarbeitungsregion, Anlage 1 Abschnitt 4.9).
3. Der Anbieter hat keinen Einfluss auf Verfügbarkeit, Antwortqualität, Preise und Bedingungen der Dienste Dritter. Störungen dieser Dienste sind keine Störungen der Instanz im Sinne der Anlage 2. Stellt ein Dritter einen Dienst ein oder ändert ihn so, dass die Anbindung angepasst werden muss, nimmt der Anbieter die Anpassung im Rahmen der Updates (§ 5 Abs. 3) vor; ein Anspruch auf die dauerhafte Verfügbarkeit eines bestimmten Modells besteht nicht.
4. Der Kunde kann das Sprachmodell jederzeit in der Instanz wechseln. Für Modelle mit eigenem Einbettungsmodell ist einmalig ein Füll-Lauf der Einbettungen erforderlich (Anlage 1 Abschnitt 4.10).

§ 5 Bereitstellung, Betrieb, Updates

1. Der Anbieter betreibt die Instanz auf von ihm angemieteten Servern in der Europäischen Union (Anlage 3, Anhang C). Ein Wechsel des Rechenzentrumsbetreibers oder des Rechenzentrumsstandorts innerhalb der EU ist zulässig; Anlage 3 § 6 gilt.
2. Die Instanz ist technisch von anderen Instanzen getrennt: eigene Datenbank mit eigener Datenbankrolle, eigener Dateispeicher, eigene Konfiguration, eigene Hintergrunddienste. Der Programmcode wird von allen Instanzen des Anbieters gemeinsam genutzt (Anlage 2 Abschnitt 6).
3. Der Anbieter hält die Software aktuell und spielt Fehlerbehebungen, Sicherheitsupdates und Weiterentwicklungen in die Instanz ein. Ein Anspruch auf bestimmte neue Funktionen besteht nicht. Änderungen, die den Kunden zu Anpassungen an seiner Einbindung zwingen, kündigt der Anbieter mindestens vier Wochen vorher in Textform an und beschreibt die nötigen Schritte; bei zwingenden Sicherheits- oder Rechtsänderungen darf die Frist angemessen verkürzt werden.

4. Der Anbieter darf die Software aus sachlichen technischen, sicherheitsbezogenen, regulatorischen oder produktbezogenen Gründen ändern, soweit der vereinbarte Leistungszweck nicht wesentlich beeinträchtigt wird und die Änderung für den Kunden zumutbar ist. Wesentliche Änderungen der Kernfunktionen nach Anlage 1 Abschnitten 4.1 bis 4.3 kündigt der Anbieter mindestens vier Wochen vor ihrem Wirksamwerden in Textform an; bei zwingenden Sicherheits- oder Rechtsänderungen darf die Frist angemessen verkürzt werden. Entfällt eine solche Kernfunktion ohne gleichwertigen Ersatz oder führt eine Änderung zu einer nicht nur unerheblichen nachteiligen Veränderung des vereinbarten Leistungsumfangs, kann der Kunde bis zum Wirksamwerden der Änderung mit Wirkung zu diesem Zeitpunkt kündigen. Zwingende Sicherheits- oder Gesetzesänderungen bleiben zulässig; gesetzliche Mängelrechte bleiben unberührt.

§ 6 Pflichten des Kunden

1. **Inhalte und Rechte.** Der Kunde bestimmt, welche Inhalte die Instanz indexiert. Er stellt sicher, dass er zur Nutzung dieser Inhalte und zur Weitergabe an das von ihm gewählte Sprachmodell berechtigt ist (Urheber-, Marken-, Persönlichkeits- und Datenschutzrecht) und dass die Inhalte nicht rechtswidrig sind. Für Inhalte Dritter (z. B. verlinkte Fremdseiten) gilt dies entsprechend.
2. Der Kunde führt der Instanz besondere Kategorien personenbezogener Daten (Art. 9 DSGVO), Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO) oder einem Berufsgeheimnis (§ 203 StGB) unterliegende Daten nur zu, wenn dies in Anlage 4 ausdrücklich vereinbart ist und die erforderliche Rechtsgrundlage und Schutzmaßnahmen bestehen. Bei Quellen, die solche Daten typischerweise oder unvermeidbar enthalten können, trifft der Kunde risikoadäquate Auswahl-, Filter- und Hinweismechanismen; eine lückenlose manuelle Vorprüfung jedes einzelnen Datensatzes ist nicht geschuldet. Der Anbieter kann ergänzende Maßnahmen verlangen oder eine Anbindung ablehnen, wenn die vereinbarten Schutzmaßnahmen nicht ausreichen.
3. **Transparenz und Datenschutzhinweise.** Der Kunde informiert die Nutzer seiner Website und seine Beschäftigten über die Verarbeitung durch die Instanz (Art. 13, 14 DSGVO). Er belässt die vom Anbieter nach Art. 50 Abs. 1 der Verordnung (EU) 2024/1689 vorgesehenen sichtbaren Hinweise, dass ein KI-System antwortet. Soweit die jeweils bereitgestellte Produktversion maschinenlesbare Kennzeichnungen nach Art. 50 Abs. 2 enthält, darf der Kunde diese nicht entfernen oder technisch unterdrücken. Seine eigenen Pflichten nach Art. 50 Abs. 4 erfüllt er, soweit er Ausgaben veröffentlicht oder synthetische Stimmen realer Personen einsetzt. Der Anbieter stellt Textbausteine zur Verfügung (§ 1 Abs. 7); deren rechtliche Prüfung obliegt dem Kunden.
4. **Einwilligungen.** Setzt die Website des Kunden eine Einwilligungslösung (Cookie-Banner) voraus, konfiguriert der Kunde die Einbindung des Chats entsprechend (Anlage 1 Abschnitt 4.11). Das Chat-Widget setzt keine Cookies.
5. **Erlaubte Websites.** Für jede produktiv öffentlich in eine Website eingebundene Sammlung muss mindestens eine erlaubte Website/Origin in einer Freigabeliste hinterlegt sein. Der Kunde pflegt diese Liste und trägt die aus den von ihm freigegebenen Einbindungen entstehenden Kosten. Die Freigabeliste steuert browserbasierte Einbindungen, bei denen der Browser einen Origin-Header mitsendet; eine leere Liste sperrt solche browserbasierten öffentlichen Einbindungen. Serverseitige Aufrufe sowie API-/MCP-Aufrufe ohne Origin-Header werden von der Origin-Liste nicht gesteuert; ihre Absicherung richtet sich nach den für die jeweilige Schnittstelle vorgesehenen Zugangsschutz- und Aktivierungsmechanismen.

6. **Zugangsdaten.** Der Kunde hält Zugangsdaten zur Instanz, API-Schlüssel und den Signaturschlüssel für angemeldete Besucher (Anlage 1 Abschnitt 4.3) vertraulich, vergibt Benutzerkonten nur an berechtigte Personen mit den erforderlichen Rechten und meldet einen Missbrauch unverzüglich (AGB § 19 Abs. 2).

7. Zulässige Nutzung und Inhalte.

- a. Der Kunde nutzt die Instanz nur für eigene Geschäftszwecke und die eigenen Websites, Marken und Zielgruppen, die in Anlage 4 benannt sind. Eine Nutzung für Dritte (Weitervermietung, Betrieb für Kunden des Kunden) bedarf einer gesonderten Vereinbarung.
- b. Der Kunde darf keine Inhalte einstellen, indexieren, verarbeiten lassen oder über die Instanz verbreiten, deren Besitz, Bereitstellung, Verbreitung oder konkrete Verwendung nach anwendbarem Recht rechtswidrig ist oder Rechte Dritter verletzt. Dies gilt insbesondere für strafbare Inhalte wie Darstellungen sexuellen Missbrauchs von Kindern, rechtswidrige terroristische Propaganda oder Rekrutierung, strafbare Volksverhetzung, rechtswidrige Kennzeichen oder Propagandamittel verfassungswidriger oder terroristischer Organisationen sowie konkrete Drohungen oder Anleitungen zu schweren Straftaten. Gesetzlich zulässige Nutzung zu Zwecken der staatsbürgerlichen Aufklärung, Berichterstattung, Wissenschaft, Forschung, Lehre, Kunst, Dokumentation oder Prävention bleibt unberührt. Radikale, polemische, kontroverse, politische oder religiöse Auffassungen sind nicht allein wegen ihrer inhaltlichen Richtung unzulässig, solange ihre konkrete Speicherung, Verarbeitung und Ausgabe rechtmäßig ist.
- c. Rechtmäßige, aber besonders sensible Inhalte, insbesondere explizite Sexualdarstellungen, drastische Gewaltdarstellungen oder extremistisches Quellenmaterial, teilt der Kunde dem Anbieter vor produktiver Aktivierung mit, wenn hierdurch besondere technische, jugendschutz-, sicherheits- oder compliancebezogene Maßnahmen erforderlich werden können.
- d. Der Anbieter ist nicht zu einer allgemeinen Vorabkontrolle oder fortlaufenden Überwachung der Kundendaten verpflichtet. Erlangt er jedoch konkrete Kenntnis von offensichtlich rechtswidrigen Inhalten oder einer Nutzung, die eine erhebliche Gefahr für Personen oder die Sicherheit der Systeme begründet, darf und, soweit gesetzlich erforderlich, muss er im erforderlichen und verhältnismäßigen Umfang einzelne Inhalte sperren, die betroffene Funktion oder bei schwerwiegenden Fällen die Instanz vorläufig deaktivieren. Er informiert den Kunden unverzüglich über Grund und Umfang, soweit gesetzliche Vorgaben, behördliche Anordnungen oder der Schutz gefährdeter Personen dem nicht entgegenstehen. Beruht eine Sperre auf einem vom Kunden zu vertretenden Verstoß gegen diesen Abschnitt, bleibt die vereinbarte Vergütung geschuldet, soweit der Anbieter leistungsbereit bleibt und die Sperre zur Abwehr des Verstoßes erforderlich und verhältnismäßig ist; ersparte Aufwendungen sind anzurechnen. Bei einer nur teilweisen Sperre bleibt die Vergütung im Übrigen unberührt. Erweist sich die Sperre als nicht berechtigt oder ist ihr Anlass vom Kunden nicht zu vertreten, wird die Vergütung für Dauer und Umfang der Beeinträchtigung angemessen gutgeschrieben. Gesetzliche Minderungs-, Schadensersatz-, Kündigungs-, Melde-, Auskunfts-, Sicherungs- und Entfernungspflichten sowie sonstige gesetzliche Rechte bleiben unberührt.
- e. AGB § 19 Abs. 3 gilt; der Kunde unterlässt außerdem Versuche, die Wissensregel des Assistenten zu umgehen, das System automatisiert zu überlasten oder Sicherheitsmechanismen auszuhebeln.

8. **Prüfung der Ausgaben.** Der Kunde ist sich bewusst, dass Antworten des Assistenten maschinell erzeugt werden und trotz der Bindung an die Wissensbasis unvollständig, missverständlich oder in Einzelfällen unzutreffend sein können. Er setzt den Assistenten nicht für Aussagen ein, deren Fehlerhaftigkeit zu erheblichen Schäden führen kann (insbesondere verbindliche Rechts-, Steuer-, Medizin- oder Sicherheitsauskünfte), ohne geeignete organisatorische Vorkehrungen (Freigabe von Frage-Antwort-Paaren, Prüfung durch Fachpersonal, Golden Set). § 13 bleibt unberührt.

§ 7 Nutzungsrechte, Eigentum an Daten

1. Der Kunde erhält für die Vertragslaufzeit das einfache, nicht übertragbare, nicht unterlizenzierbare Recht, die Software in der Instanz für eigene Zwecke nach diesem Vertrag zu nutzen. Eine Überlassung des Programmcodes findet nicht statt. Alle Rechte an der Software, an Weiterentwicklungen und an vom Anbieter erstellten Prompts, Konfigurationen und Methoden bleiben beim Anbieter (AGB § 24 gilt entsprechend).
2. Die vom Kunden eingebrachten Inhalte, die daraus erzeugte Wissensbasis, die Gesprächsprotokolle und alle übrigen Daten der Instanz („Kundendaten“) bleiben Daten des Kunden. Der Anbieter nutzt sie ausschließlich zur Vertragserfüllung und verwendet sie nicht zum Training von Modellen. Eine Nutzung durch die Sprachmodell-Anbieter richtet sich nach deren Bedingungen (§ 4 Abs. 1).
3. Der Anbieter darf technische Betriebsdaten ohne Inhalte nur dann für eigene Betriebs- und Produktverbesserungszwecke auswerten, wenn sie keinen Personenbezug aufweisen oder zuvor wirksam anonymisiert wurden (z. B. aggregierte Anzahl von Anfragen, Antwortzeiten, Fehlerquoten, Ressourcenverbrauch). Fragen, Antworten und Dokumentinhalte werden hierfür nicht ausgewertet. Soweit Rohdaten Personenbezug haben, verarbeitet der Anbieter sie ausschließlich nach Anlage 3 im Auftrag des Kunden und verwendet sie nicht für eigene Zwecke.
4. Für vom Anbieter im Auftrag des Kunden erstellte individuelle Erweiterungen (Kunden-Extras) gilt AGB § 17.

§ 8 Zugriff des Anbieters auf die Instanz (Fernwartung)

1. Der Anbieter greift auf die Oberfläche und die Daten der Instanz nur zu, soweit dies zur Einrichtung, Störungsbeseitigung, Sicherheitspflege, Datensicherung oder auf Anforderung des Kunden erforderlich ist.
2. Die Software setzt dies technisch um: Solange die Instanz keinen aktiven Benutzer des Kunden hat, kann sich der Anbieter mit seinem Anbieterkonto (in der Software als „Betreiber“ bezeichnet) anmelden. Danach ist die Anmeldung des Anbieterkontos nur möglich, wenn ein Administrator des Kunden die Fernwartung in der Oberfläche („Fernwartung“) für einen Zeitraum oder bis auf Widerruf freigegeben hat. Jede Anmeldung des Anbieterkontos an der Oberfläche wird in der Instanz protokolliert und ist für den Kunden einsehbar; ein Hinweis ist während der Sitzung auf jeder Seite sichtbar.
3. Unabhängig von Abs. 2 hat der Anbieter als Betreiber der Server technischen Zugriff auf Dateien und Datenbank der Instanz (Systemadministration). Er nutzt diesen Zugriff nur zu den Zwecken nach Abs. 1 und für automatisierte Abläufe (Updates, Prüfung der Paketgrenzen, Datensicherung, Löschung). Bei sicherheitsrelevanten Vorfällen darf der Anbieter ohne vorherige Freigabe eingreifen und informiert den Kunden unverzüglich.

4. Weisungen des Kunden im Rahmen der Auftragsverarbeitung bleiben unberührt (Anlage 3).

§ 9 Datensicherung, Herausgabe, Löschung

1. Der Anbieter sichert die Datenbank und den Dateispeicher der Instanz nach Anlage 2 Abschnitt 4. Abweichend von AGB § 19 Abs. 1 obliegt die Datensicherung der Instanz dem Anbieter; der Kunde bleibt für die Sicherung seiner Quellinhalte (Website, Dokumente, Drittsysteme) selbst verantwortlich.
2. Der Kunde kann jederzeit einen Export seiner Kundendaten verlangen: Datenbank-Dump der Instanz (alle Schemas), hochgeladene Dateien und Konfiguration ohne Geheimnisse des Anbieters, in einem gängigen maschinenlesbaren Format, übergeben über einen gesicherten Kanal. Der erste Export je Kalenderjahr sowie der Export bei Vertragsende sind in der Vergütung enthalten; weitere Exporte vergütet der Kunde nach Aufwand.
3. Mit Vertragsende sperrt der Anbieter die Instanz. Er bewahrt Kundendaten und Sicherungen für eine Nachlaufzeit von 30 Tagen nach Vertragsende auf, damit der Kunde den Export nach Abs. 2 abrufen kann, und löscht danach die Instanz vollständig (Datenbank, Datenbankrolle, Dateien, Konfiguration, Zertifikate, DNS-Eintrag und Sicherungen nach Maßgabe der Anlage 3 § 8 Abs. 2). Verlangt der Kunde in Textform die sofortige Löschung, entfällt die Nachlaufzeit. Über die Löschung erstellt der Anbieter auf Verlangen ein Löschartokoll ohne Inhalte der Wissensbasis. Gesetzliche Aufbewahrungspflichten des Anbieters für Vertrags- und Abrechnungsdaten bleiben unberührt.
4. Auf Wunsch des Kunden übergibt der Anbieter die Instanz gegen Vergütung nach Aufwand zum Selbstbetrieb; hierfür ist der Abschluss des Softwarelizenzvertrags „dAI Pro-Web“ erforderlich.

§ 10 Vergütung

1. Der Kunde zahlt die in Anlage 4 vereinbarte monatliche Vergütung für das gewählte Paket sowie die einmalige Vergütung für die Einrichtung. Die Preisliste des Anbieters zum Zeitpunkt des Vertragsschlusses ist in Anlage 1 Abschnitt 7 wiedergegeben.
2. Die laufende Vergütung ist ab Übergabe der Instanz (§ 3 Abs. 2) geschuldet. Ist die Instanz abnahmereif und verzögert sich die Übergabe ausschließlich wegen fehlender Mitwirkung des Kunden, beginnt die laufende Vergütung vier Wochen nach einer entsprechenden Bereitstellungs- und Mitwirkungsaufforderung des Anbieters. Die laufende Vergütung wird vierteljährlich im Voraus in Rechnung gestellt. Die Einrichtungsvergütung wird in voller Höhe mit Übergabe der Instanz (§ 3 Abs. 2) fällig und nach der Übergabe in Rechnung gestellt. Zahlungsziel und Verzugsfolgen: AGB § 8.
3. Nicht enthalten sind die Nutzungsentgelte des Sprachmodell-Anbieters (§ 4), Leistungen nach § 3 Abs. 4, Kunden-Extras (§ 1 Abs. 6) und zusätzliche Exporte (§ 9 Abs. 2).
4. Abweichend von AGB § 7 Abs. 5 gilt für die laufende Vergütung ausschließlich folgende Preisanpassungsregel: Der Anbieter kann die Vergütung erstmals zum Beginn einer Verlängerungsperiode und danach höchstens einmal innerhalb von zwölf Monaten anpassen, soweit sich die für die Leistungserbringung maßgeblichen Gesamtkosten nach Vertragsschluss verändern. Berücksichtigungsfähig sind insbesondere Kosten für Hosting und Infrastruktur, vom Anbieter zu tragende Software-, Lizenz- und Drittleistungsentgelte sowie neu eingeführte oder veränderte Steuern, Abgaben und zwingende Aufwendungen für Sicherheit oder regulatorische Anforderungen. Kostensteigerungen und Kostensenkungen sind nach denselben Maßstäben zu

berücksichtigen und gegeneinander zu verrechnen. Sinken die maßgeblichen Gesamtkosten, senkt der Anbieter die laufende Vergütung in entsprechendem Umfang zum nächstmöglichen Anpassungszeitpunkt; eine Preiserhöhung allein zur Ausweitung der Gewinnmarge ist ausgeschlossen. Der Anbieter teilt jede Änderung mindestens drei Monate vor ihrem Wirksamwerden in Textform mit und nennt die maßgeblichen Kostenfaktoren sowie deren Auswirkung auf den Gesamtpreis. Erhöht sich die laufende Vergütung um mehr als 5 % gegenüber der zuletzt geschuldeten Vergütung, kann der Kunde den Vertrag bis zum Wirksamwerden der Erhöhung mit Wirkung zu diesem Zeitpunkt kündigen. Eine Anpassung innerhalb der ersten zwölf Monate der laufenden Leistung ist ausgeschlossen.

5. Alle Preise verstehen sich netto zuzüglich Umsatzsteuer.

§ 11 Laufzeit und Kündigung

1. Der Vertrag beginnt mit Unterzeichnung. Die Mindestlaufzeit der laufenden Bereitstellung beträgt zwölf Monate und beginnt mit der Übergabe der Instanz (§ 3 Abs. 2); bei einer ausschließlich vom Kunden verursachten Verzögerung gilt der Beginn nach Maßgabe des § 10 Abs. 2 vier Wochen nach der dort genannten Bereitstellungs- und Mitwirkungsaufforderung. Der Vertrag verlängert sich jeweils um zwölf Monate, wenn er nicht mit einer Frist von drei Monaten zum Ende der jeweiligen Laufzeit in Textform gekündigt wird. Diese Regelung geht AGB § 20 Abs. 1 vor.
2. Ist der Kunde mit unbestrittenen oder rechtskräftig festgestellten Entgelten in Höhe von mindestens zwei monatlichen Vergütungen länger als 30 Tage in Verzug, darf der Anbieter die Instanz nach Ankündigung in Textform mit einer Frist von sieben Tagen sperren. Die Sperre ist unzulässig, soweit der Kunde die Forderung vor der Ankündigung nachvollziehbar und nicht offensichtlich unbegründet bestritten hat. Die Vergütung bleibt während der Sperre geschuldet, soweit der Anbieter leistungsbereit bleibt. Nach vollständiger Zahlung hebt der Anbieter die Sperre unverzüglich auf.
3. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt für den Anbieter insbesondere vor, wenn der Kunde trotz einer Sperrandrohung nach Abs. 2 und angemessener Nachfrist die dort genannten unbestrittenen oder rechtskräftig festgestellten Rückstände nicht ausgleicht, trotz Abmahnung rechtswidrige Inhalte indexiert oder die Instanz vertragswidrig für Dritte nutzt (§ 6). Für den Kunden kann ein wichtiger Grund insbesondere vorliegen, wenn die zugesagte Verfügbarkeit wiederholt erheblich unterschritten wird und der Anbieter trotz Anzeige und angemessener Frist keine Abhilfe schafft. Das Kündigungsrecht bei Widerspruch gegen einen neuen Unterauftragsverarbeiter richtet sich nach Anlage 3 § 6 Abs. 2. Im Voraus gezahlte laufende Vergütung für die Zeit nach Wirksamwerden einer vom Kunden berechtigt erklärten außerordentlichen Kündigung oder einer vom Anbieter zu vertretenden Beendigung wird anteilig erstattet; bei einer vom Anbieter wegen eines vom Kunden zu vertretenden wichtigen Grundes erklärten Kündigung erfolgt keine Erstattung.
4. Für die Beendigung gilt § 9 Abs. 3.

§ 12 Datenschutz

1. Der Kunde ist Verantwortlicher für die in seiner Instanz verarbeiteten personenbezogenen Daten (Inhalte der Wissensbasis, Daten der Website-Besucher, Daten seiner Beschäftigten und Kunden im Eingang und in angebundenen Systemen). Der Anbieter verarbeitet diese Daten als Auftragsverarbeiter nach Anlage 3.

2. Der Anbieter verarbeitet die Vertrags-, Kontakt- und Abrechnungsdaten des Kunden sowie die Stammdaten und Zählwerte der Instanz (Name, Domain, Paket, Grenzen, Nutzungsstand) als Verantwortlicher (AGB § 11 Abs. 3). Das Protokoll der Anmeldungen des Anbieterkontos liegt in der Instanz und unterliegt der Anlage 3.
3. Nutzt der Kunde einen eigenen Account/API-Schlüssel eines Sprachmodell- oder Sprachdienstanbieters (§ 4 Abs. 1), bestimmt sich dessen datenschutzrechtliche Rolle nach dem jeweils geltenden Vertrag, der DPA und der tatsächlichen Verarbeitung. Soweit der Drittanbieter personenbezogene Daten ausschließlich auf Weisung des Kunden verarbeitet, schließt der Kunde die erforderliche Vereinbarung nach Art. 28 DSGVO unmittelbar mit ihm. Der Anbieter übermittelt Daten an diesen Dienst ausschließlich in technischer Ausführung der dokumentierten Weisung des Kunden. Eigene Verarbeitungszwecke des Drittanbieters bleiben vom Kunden gesondert zu bewerten.

§ 13 Besondere Bestimmungen für KI-Ausgaben, Gewährleistung, Haftung

1. Der Anbieter schuldet den Betrieb der Software nach Anlage 1 und Anlage 2, nicht ein bestimmtes inhaltliches Ergebnis einzelner Antworten. Die Software ist so gestaltet, dass Antworten nur aus der Wissensbasis erzeugt und mit Quellen belegt werden; die inhaltliche Richtigkeit, Vollständigkeit und Aktualität einer Antwort hängt von den Inhalten des Kunden, der Fragestellung und dem vom Kunden gewählten Sprachmodell ab und wird nicht gewährleistet.
2. Mängel der Software behebt der Anbieter im Rahmen der Updates (§ 5 Abs. 3) und der Störungsbeseitigung (Anlage 2). Die Gewährleistung für die mietvertraglich überlassene Software richtet sich nach den gesetzlichen Vorschriften. Ausgeschlossen ist lediglich die verschuldensunabhängige Schadensersatzhaftung nach § 536a Abs. 1 Alternative 1 BGB für bereits bei Vertragsschluss vorhandene Mängel; dies gilt nicht bei einer übernommenen Garantie oder arglistigem Verschweigen. Sonstige Mängelrechte und die Haftung für zu vertretende Pflichtverletzungen bleiben unberührt.
3. Der Anbieter haftet nicht, soweit ein Schaden ausschließlich auf unrichtigen, unvollständigen oder veralteten Inhalten des Kunden, auf einer vom Kunden zu vertretenden Verletzung des § 6 Abs. 8 oder auf dem Verhalten eines vom Kunden gewählten Drittanbieters beruht und keine vom Anbieter zu vertretende Pflichtverletzung mitursächlich war. Im Übrigen gilt AGB § 12; AGB § 12 Abs. 5 gilt nicht für Daten der Instanz, deren Sicherung nach § 9 Abs. 1 dem Anbieter obliegt.
4. Der Kunde stellt den Anbieter von berechtigten Ansprüchen Dritter frei, die auf vom Kunden bereitgestellten Inhalten, einer vom Kunden zu vertretenden Verletzung des § 6 oder der vertragswidrigen Nutzung der Instanz für Dritte beruhen, einschließlich angemessener Kosten der Rechtsverteidigung. Der Anbieter informiert den Kunden unverzüglich über geltend gemachte Ansprüche und ermöglicht ihm, soweit zumutbar, an der Rechtsverteidigung mitzuwirken; Anerkenntnisse oder Vergleiche zulasten des Kunden bedürfen dessen vorheriger Zustimmung, die nicht unbillig verweigert werden darf.
5. Rollen und Zweckbestimmung nach der Verordnung (EU) 2024/1689 (KI-Verordnung): Der Anbieter ist Anbieter des KI-Systems dAI Pro (Art. 3 Nr. 3) und, soweit dAI Pro ein KI-Modell mit allgemeinem Verwendungszweck integriert, nachgelagerter Anbieter (Art. 3 Nr. 68); der Kunde ist Betreiber (Art. 3 Nr. 4). Zweckbestimmung ist die Beantwortung von Fragen aus den vom Kunden bereitgestellten Inhalten sowie die Unterstützung der Inhaltspflege und des Kundensupports. dAI Pro ist nicht für Entscheidungen über natürliche Personen bestimmt, insbesondere nicht für die in Anhang III genannten Hochrisiko-Zwecke; ein solcher Einsatz ist nicht Vertragsgegenstand und

bedarf einer gesonderten schriftlichen Vereinbarung, die der Anbieter ablehnen kann. Ein Rollenwechsel des Kunden zum Anbieter tritt nicht allein wegen jeder zweckwidrigen Nutzung ein, sondern nur, wenn die gesetzlichen Voraussetzungen des Art. 25 KI-Verordnung erfüllt sind, insbesondere bei einer relevanten wesentlichen Änderung oder einer Zweckänderung, durch die das System zum Hochrisiko-System wird. Anbieter und Kunde treffen jeweils die sie betreffenden Maßnahmen zur Unterstützung der KI-Kompetenz nach Art. 4 und erfüllen ihre Transparenzpflichten nach Art. 50.

§ 14 Referenznennung

Es gilt AGB § 9 Abs. 3. Eine erteilte Zustimmung zur Referenznennung kann der Kunde jederzeit mit Wirkung für die Zukunft in Textform widerrufen.

§ 15 Vertragsübernahme, Rechtsnachfolge, Schlussbestimmungen

1. Es gelten die AGB des Anbieters in der bei Vertragsschluss gültigen Fassung (Anlage 5). In Fragen des Datenschutzes geht Anlage 3 (Auftragsverarbeitung) allen übrigen Vertragsbestandteilen vor. Im Übrigen gilt bei Widersprüchen folgende Rangfolge:
 - a. Anlage 4 (Auftragsblatt), (2) dieser Vertrag, (3) Anlagen 1 und 2, (4) AGB.
2. Änderungen und Ergänzungen bedürfen der Textform (AGB § 15 Abs. 3). Für Anlage 4 genügt ein von beiden Parteien in Textform bestätigtes aktualisiertes Auftragsblatt.
3. Der Anbieter darf diesen Vertrag mit allen Rechten und Pflichten auf einen Rechtsnachfolger seines Unternehmens oder auf eine von Joachim Dreistein beherrschte Gesellschaft übertragen, wenn der Übernehmer sämtliche Verpflichtungen aus diesem Vertrag einschließlich Datenschutz-, Sicherheits- und Herausgabepflichten übernimmt. Der Anbieter kündigt die Übertragung mindestens vier Wochen vorher in Textform an. Beeinträchtigt die Übertragung berechnete Interessen des Kunden wesentlich, kann der Kunde innerhalb von vier Wochen nach Zugang der Ankündigung zum Zeitpunkt der Übertragung kündigen. Der Kunde darf den Vertrag mit Zustimmung des Anbieters in Textform auf ein mit ihm verbundenes Unternehmen übertragen; die Zustimmung darf nicht unbillig verweigert werden.
4. Anwendbares Recht und Gerichtsstand: AGB § 15 Abs. 1 und 2.
5. Abweichend von AGB § 2 Abs. 2 benennt der Anbieter keinen Stellvertreter; eine personelle Vertretung wird nicht geschuldet. Ist der Anbieter dauerhaft an der Leistungserbringung gehindert und besteht keine Rechtsnachfolge, kann der Kunde den Vertrag aus wichtigem Grund kündigen. Soweit der Anbieter die Datenherausgabe noch selbst bewirken kann, hat der Kunde Anspruch auf Export seiner Daten nach § 9 Abs. 2. Eine Fortführung, Schlüsselherausgabe oder Leistung durch eine Ersatz- oder Vertrauensperson wird mangels bestellter Vertretung nicht zugesagt. Bereits bestehende gesetzliche Rechte des Kunden bleiben unberührt.
6. Sollten einzelne Bestimmungen unwirksam sein, bleibt der Vertrag im Übrigen wirksam (AGB § 15 Abs. 4).

Anlagen:

- Anlage 1: Leistungsbeschreibung dAI Pro (Pakete, Zählweise, Funktionen, Einrichtung, Preise)
- Anlage 2: Service Level und Betrieb

- Anlage 3: Vereinbarung zur Auftragsverarbeitung mit Anhängen A (Verarbeitung), B (technische und organisatorische Maßnahmen), C (Subunternehmer), D (Fernwartung bei Selbstbetrieb, hier ohne Anwendung) und E (Verpflichtung nach § 203 StGB, nur bei Berufsgeheimnisträgern)
- Anlage 4: Auftragsblatt (gesondertes, von beiden Parteien unterzeichnetes Dokument)
- Anlage 5: Allgemeine Geschäftsbedingungen des Anbieters, Stand Juni 2026 (als gesondertes Dokument mit diesem Vertrag übergeben)

Unterzeichnung: Dieser Vertrag einschließlich seiner Anlagen wird durch das von beiden Parteien unterschriebene Auftragsblatt (Anlage 4 Abschnitt 7) geschlossen. Eine gesonderte Unterschrift unter diesen Vertrag ist nicht erforderlich.

Anlage 1 — Leistungsbeschreibung dAI Pro

1. Das Produkt

dAI Pro ist eine Software, die die vorhandenen Inhalte eines Unternehmens (Website, Dokumente, Datenbanken, Wissens- und Ticketsysteme) in eine durchsuchbare Wissensbasis überführt und darauf einen KI-Assistenten betreibt. Der Assistent ist so gestaltet, dass er Fragen von Website-Besuchern im Chat oder in einer Suche **ausschließlich aus dieser Wissensbasis und mit Quellenangabe** beantwortet, fehlende Informationen benennt und, wenn eingerichtet, den Weg zu einem Menschen anbietet (zur Beschaffenheit der einzelnen Antwort: Vertrag § 13 Abs. 1). Zweckbestimmung im Sinne der KI-Verordnung ist die Beantwortung von Fragen aus den Inhalten des Kunden sowie die Unterstützung der Inhaltspflege und des Kundensupports; die Software ist nicht dazu bestimmt, Entscheidungen über natürliche Personen zu treffen oder vorzubereiten.

dAI Pro gibt es in zwei Ausführungen mit demselben Funktionskern:

Ausführung	Beschreibung	Vertragsform
dAI Pro-Web	Eigenständige Webanwendung (PHP/Symfony, PostgreSQL mit pgvector). Betrieb als gehostete Instanz durch den Anbieter („dAI Pro Managed“) oder im Selbstbetrieb beim Kunden.	Vertrag „dAI Pro Managed“ bzw. Softwarelizenzvertrag „dAI Pro-Web“
dAI Pro-TYPO3	Erweiterung für TYPO3 12.4, 13.4 und 14 mit denselben Modulen im TYPO3-Backend (Abweichungen: Abschnitt 4.13).	nur individuelle Vereinbarung auf Anfrage; kein standardisierter Listenpreis

2. Begriffe

Begriff	Bedeutung
Instanz	Eine Installation von dAI Pro mit eigener Datenbank, eigenem Dateispeicher und eigenen Benutzerkonten. Bei „dAI Pro Managed“ betreibt der Anbieter je Kunde eine Instanz.
Sammlung	Eine abgeschlossene Wissensbasis innerhalb der Instanz mit eigenen Einstellungen, Datenquellen und eigenem Suchindex (technisch ein eigenes Datenbankschema). Eine Instanz kann mehrere Sammlungen haben, etwa je Website, Marke oder Zielgruppe.
Datenquelle	Woher das Wissen einer Sammlung kommt (Abschnitt 4.2).
Dokument / Datensatz	Ein indexierter Inhalt: eine Webseite, eine Datei, eine Tabellenzeile, eine aus einer Datei extrahierte Abbildung, jeweils je Sprachfassung. Erscheint als Zeile in der Dokumentliste der Sammlung.
Index	Die durchsuchbare Form der Dokumente (Volltext- und Vektorindex).

Begriff	Bedeutung
Assistent	Ein Profil innerhalb einer Sammlung mit eigenem Auftreten, eigenen Frage-Antwort-Paaren und eingegrenztem Wissen.
Agent	Ein Auftrag nach Zeitplan, der die Wissensbasis pflegt oder prüft (Abschnitt 4.5).
Sprachmodell	Das KI-Modell eines Drittanbieters, das Antworten formuliert, Texte versteht oder Einbettungen erzeugt (Abschnitt 5).
Arbeitstag	Montag bis Freitag mit Ausnahme der gesetzlichen Feiertage in Nordrhein-Westfalen.

3. Pakete und Zählweise

3.1 PAKETE

Paket	Agenten	Datenquellen	Funktionsumfang
Grundpaket	vier Agenten-Typen nach Wahl des Kunden (aus den neun Typen in 4.5)	bis zu vier Datenquellen beliebigen Typs	alle Funktionen nach Abschnitt 4
Voller Funktionsumfang	alle neun Agenten-Typen	Anzahl unbeschränkt	alle Funktionen nach Abschnitt 4

Beide Pakete gibt es in zwei Staffeln nach Größe der Wissensbasis: **bis 6.000 Datensätze** und **6.001 bis 20.000 Datensätze**. Für größere Bestände erstellt der Anbieter ein individuelles Angebot.

3.2 WAS ALS DATENSATZ ZÄHLT

Gezählt werden die **Zeilen der Dokumentliste über alle Sammlungen der Instanz**. Es zählt alles, was die Software als eigenes Dokument führt: jede Webseite, jede Datei, jede Tabellenzeile aus CSV, Excel oder Datenbank, jede aus einer Datei extrahierte Abbildung und jede Sprachfassung. Beispiele: Ein Datenblatt mit zwölf Zeichnungen ergibt dreizehn Datensätze. Eine Website mit 100 Seiten in zwei Sprachen, deren Seiten 20 PDF-Dateien und 80 Bilder verlinken, ergibt 300 Datensätze, wenn PDF-Dateien und Bilder nur in einer Sprachfassung vorliegen. Deaktivierte Dokumente zählen mit; gelöschte zählen nicht. Die Zahl ist in der Oberfläche der Instanz jederzeit ablesbar.

3.3 WAS ALS DATENQUELLE ZÄHLT

Jeder in der Instanz angelegte Eintrag vom Typ Datenquelle zählt, unabhängig von seinem Typ. **Eine Website ist eine Datenquelle**, auch wenn ihre Liste mehrere Domains, Sitemaps oder Einzelseiten enthält. Legt der Kunde je Domain eine eigene Datenquelle an, zählt jede gesondert. Gelöschte Datenquellen zählen nicht.

3.4 GRENZEN UND ÜBERSCHREITUNG

Die Grenzen des gewählten Pakets sind in der Instanz hinterlegt und werden von der Software durchgesetzt (Vertrag § 2):

- **Agenten:** Nicht erlaubte Typen stehen nicht zur Auswahl; bestehende Agenten eines nicht erlaubten Typs sind gekennzeichnet und laufen nicht.

- **Datenquellen:** Ab der erlaubten Anzahl entfällt das Anlegen weiterer Quellen.
- **Datensätze:** Über dem Paketmaximum zeigt die Instanz dem Kunden auf jeder Seite einen Hinweis (für einen Tag ausblendbar); der Anbieter erhält einmalig eine Benachrichtigung. Ab der Karenzgrenze (Vertrag § 2 Abs. 2) entstehen keine neuen Datensätze mehr; bestehende bleiben nutzbar und aktualisierbar, Chat und alle übrigen Funktionen laufen weiter. Die Instanz zeigt die Sperre auf jeder Seite.
- Hinweis und Sperre wirken unmittelbar; der Zählwert für Anzeige und Benachrichtigung wird alle 15 Minuten festgestellt. Der Kunde sieht den Stand in der Oberfläche.

4. Funktionen

4.1 CHAT UND SUCHE FÜR BESUCHER

- Chat-Widget als Blase oder fest eingebettet, auf beliebigen Websites über einen Einbettungs-Code, mit Freigabeliste erlaubter Websites (Abschnitt 4.8).
- Antworten mit Quellen und Fundstellen-Ankern (Textstelle auf der Webseite, Seite im PDF); Bilder aus der Wissensbasis in der Antwort.
- Suche als zweiter Kanal: Trefferliste über den Index mit Zusammenfassung.
- Einstiegsfragen, Folgefragen-Vorschläge, Antwort-Feedback (Daumen), „Einfache Sprache“ auf Wunsch des Besuchers.
- Mehrsprachig: sieben Oberflächensprachen (Deutsch, Englisch, Niederländisch, Französisch, Italienisch, Polnisch, Ukrainisch); Gesprächssprache wird erkannt; mehrsprachige Wissensbasis je Sprachfassung.
- Gesprächsverlauf bleibt beim Seitenwechsel im Sitzungsspeicher des Browsers erhalten (endet mit dem Schließen des Tabs; „Neues Gespräch“ löscht ihn). Das Chat-Widget setzt keine Cookies.
- Zwei Antwortverfahren, die die Software je Frage selbst wählt: Suche im Index (RAG) oder Mitgabe des gesamten Bestands kleiner Sammlungen (CAG) mit Zwischenspeicher beim Sprachmodell-Anbieter. Der an das Sprachmodell übergebene Gesprächsverlauf ist auf die letzten Gesprächszüge begrenzt.
- Antwort-Cache je Sammlung (identische Fragen werden aus dem Cache beantwortet, ohne Zuordnung zum Fragenden; vom Kunden löscherbar).
- Widget entwickelt nach den Anforderungen der WCAG 2.2 Stufe AA (Tastatur, Screenreader, Fokus, Kontraste der Standardfarben, Zoom, reduzierte Bewegung, Sprachkennzeichnung); ein externer Konformitätsnachweis ist nicht Vertragsgegenstand.
- KI-Kennzeichnung: Die Kennzeichnung nach Art. 50 Abs. 1 (Hinweis, dass ein KI-System antwortet) erfolgt in Begrüßung und Hilfetext. Antworten im Chat-Widget tragen ein sichtbares Kennzeichen („KI-generiert“) und eine maschinenlesbare Markierung; erzeugte Dokumente tragen die Kennzeichnung in den Dokumenteigenschaften. Die maschinenlesbare Kennzeichnung nach Art. 50 Abs. 2 für Antworten über API und MCP, Audioausgaben und KI-Suchzusammenfassungen ist umgesetzt und dokumentiert.

4.2 DATENQUELLEN

Siebzehn Typen (in der TYPO3-Ausführung achtzehn, Abschnitt 4.13), in jeder Sammlung beliebig kombinierbar (im Grundpaket bis zu vier Datenquellen):

Typ	Inhalt
Webseiten-Indexierung	Websites über Sitemaps, Domains (Crawl mit Tiefe und Seitenlimit) oder Einzelseiten; wahlweise HTTP oder gerenderter Abruf (Headless-Browser); verlinkte Dateien und Bilder werden mitgenommen; robots.txt wird beachtet
Dateien	Hochgeladene Dateien (PDF, Office, Text, Bilder); Texterkennung für gescannte PDFs und Abbildungen, sofern der gewählte Sprachmodell-Anbieter sie anbietet (Abschnitt 5)
Internetlinks	Einzelne Adressen von Webseiten oder Dateien
Manuelle Eingabe	Direkt eingegebene Texte und Frage-Antwort-Paare
Supportdatenbank	Vom Kunden aus dem Eingang ins Wissen übernommene Antworten
CSV / Excel	Tabellen; jede Zeile ein Dokument
Ordner	Dateien in einem Verzeichnis auf dem Server der Instanz
Datenbank	Abfragen gegen eine vom Kunden benannte Datenbank
Confluence, Notion	Seiten aus diesen Wissenssystemen
Zendesk	Hilfartikel oder Tickets, nach Wahl des Kunden
Freshdesk	Artikel der Wissensdatenbank
Nextcloud, SharePoint, Google Drive	Dateien aus diesen Speichern
E-Mail	Postfach über IMAP (z. B. Support-Postfach)

Für alle Typen: Sprachfassungen je Dokument, Kopplung verlinkter Dateien und Bilder, Einzelaktivierung und -deaktivierung von Dokumenten, Kopieren in andere Sammlungen, Indexierungs-Anweisungen je Quelle, wahlweise Übersetzung fehlender Sprachfassungen durch das Sprachmodell.

4.3 ASSISTENTEN UND AKTIONEN

- Mehrere Assistenten je Sammlung mit eigenem Auftreten, Frage-Antwort-Paaren, eingegrenztem Wissen und eigenem Sprachmodell.
- Redaktions-Copilot für die Erstellung und Prüfung von Inhalten aus der Wissensbasis.
- Mensch-Übergabe: Formular im Chat, Übergabe des Gesprächsverlaufs mit Zusammenfassung per E-Mail an vom Kunden benannte Adressen, optional mit Kopie an den Besucher, Geschäftszeiten-Hinweis, optionaler Bot-Schutz (Cloudflare Turnstile, vom Anbieter je Instanz mit Schlüsseln aus dem Cloudflare-Konto des Kunden eingerichtet).
- Aktionen aus dem Chat: Rückruf, Termin, Ticket oder Webhook an Systeme des Kunden (Zammad, Freshdesk, Zendesk, Jira, HubSpot, eigene Endpunkte), jeweils erst nach Bestätigung durch den Besucher; Werkzeuge mit Funktionsaufrufen und Übergabe an Spezial-Assistenten.
- Angemeldete Besucher: Übernahme einer vom Kunden signierten Identität (Token) für persönliche Antworten über Werkzeuge; die Identität wird im Protokoll nur pseudonymisiert geführt.

- Datei- und Foto-Upload durch Besucher: Die Datei wird nur für die Dauer der Anfrage ausgewertet und nicht gespeichert.

4.4 SPRACH-CHAT

Spracheingabe und Vorlesen der Antwort über einen eigenen Sprachdienst der Instanz. Der Audio-Anbieter ist je Sammlung getrennt vom Chat-Modell wählbar; Audio-Funktionen bieten Mistral AI und OpenAI, die Spracherkennung kann alternativ Gladia übernehmen; ob Gladia eingesetzt wird, entscheidet der Kunde je Sammlung (Anbieterbedingungen zu Unterauftragnehmern und Speicherdauer sind vom Kunden zu prüfen), der Anbieter setzt Gladia in seinen eigenen Diensten seit 18.09.2026 nicht ein. Anthropic, Google Gemini und OpenAI-kompatible Endpunkte bieten keine Audio-Funktionen. Eigene Stimmen, Sprechtempo, Fachvokabular.

4.5 AGENTEN (NEUN TYPEN)

Agent (technischer Typ)	Aufgabe
Frische-Wächter (<code>freshness</code>)	Prüft die Quellen auf Änderungen, indexiert Geändertes nach, entfernt Verschwundenes
Inhalts-Wächter (<code>content_sanity</code>)	Findet Widersprüche, veraltete und unklare Inhalte
Content-Gap-Radar (<code>gap_radar</code>)	Wertet unbeantwortete Fragen aus dem Protokoll aus und schlägt fehlende Inhalte vor
FAQ-Generator (<code>faq_generator</code>)	Erzeugt Frage-Antwort-Vorschläge aus der Wissensbasis
Ticket-Assistent (<code>ticket_assistant</code>)	Beantwortet Fragen aus dem Ticketsystem des Kunden als Entwurf
Eingang (<code>support_inbox</code>)	Liest Vorgänge aus Ticketsystem oder Postfach, erstellt Antwortentwürfe als interne Notiz; Freigabe durch Mitarbeiter; freigegebene Antworten übernimmt der Bearbeiter auf Klick in die Supportdatenbank
Freier Prompt (<code>custom_prompt</code>)	Regelmäßiger Bericht oder Prüfung nach eigener Anweisung
Qualitätsprüfung (<code>quality_audit</code>)	Bewertet Gespräche nach Lösungsquote, Ursachen und Kosten
Golden Set (<code>golden_set</code>)	Regressionstest: feste Fragen mit Soll-Antworten, Prüfung nach jeder Änderung

Agenten laufen nach Zeitplan im Hintergrund, schreiben Berichte und können per E-Mail benachrichtigen. Ihre Ergebnisse werden nicht ohne ausdrückliche Einstellung des Kunden zu Inhalten der Wissensbasis.

4.6 QUALITÄTS-COCKPIT, VERBRAUCH UND KOSTEN

- Protokoll je Antwort mit Verfahren, Fundstellen, Gesprächsausgang (beantwortet, keine Information, Rückfrage, Übergabe) und Kosten in Euro.
- Verbrauchsseite je Sammlung: Aufrufe, Token, Seiten (OCR), Kosten nach Zweck und Modell, Monatsansicht, Export als CSV und Excel; Preise je Modell pflegbar, Umrechnung mit dem Referenzkurs der Europäischen Zentralbank.

- Golden-Set-Vorschläge aus der Qualitätsprüfung.

4.7 VERWALTUNG

- Benutzer, Gruppen und Rechte je Sammlung; Rollen im Eingang; Backend-Sprache je Person; Konten gelten auch für die REST-API.
- REST-API mit Token-Anmeldung für Sammlungen, Datenquellen, Dokumente, Jobs, Agenten, Chat und Suche; Endpunkt für KI-Agenten (Model Context Protocol, standardmäßig aus, gedrosselt).
- Handbuch mit 31 Kapiteln, in der Oberfläche als Hilfe-Dialoge verlinkt.

4.8 EINBETTUNG

Ein-Zeilen-Einbettung des Chats oder der Suche, Gestaltung je Sammlung (Farben, Schrift, Position, Texte), Freigabeliste erlaubter Websites; bei produktiv öffentlichen browserbasierten Einbindungen muss mindestens eine erlaubte Origin hinterlegt sein, eine leere Liste sperrt diese Browser-Einbindung. Serverseitige sowie API-/MCP-Aufrufe ohne Origin-Header werden nicht über diese Liste gesteuert. Anbindung an Einwilligungslösungen (Abschnitt 4.11).

4.9 VERARBEITUNGSREGION (SOVERÄNITÄT)

Je Sammlung wählbar: keine Einschränkung, nur EU, nur Deutschland. Die Software prüft die beteiligten Dienste (Chat, Einbettungen, Sprache) gegen die hinterlegte Region und zeigt Besuchern ein Attest mit der Kette der Anbieter; ein maschinenlesbarer Nachweis steht für Datenschutzbeauftragte bereit. Das Attest lautet „KI-Verarbeitung durch Dienste mit Verarbeitungsregion EU/Deutschland laut Anbieterangabe“ und nennt die Quelle der Anbieterangabe; es wirkt als Kennzeichnung gegenüber Besuchern, nicht als technische Sperre. Die tatsächliche Verarbeitungsregion hängt vom konkret gebuchten Dienst, Account und dessen Konfiguration ab und ist vor Aktivierung anhand der aktuellen Anbieterunterlagen zu dokumentieren. Die Region eines OpenAI-kompatiblen Endpunkts oder einer Regionseinstellung des Anbieters trägt der Kunde selbst ein; die Software prüft diese Angabe nicht.

4.10 SPRACHMODELL-WECHSEL OHNE NEUINDEXIERUNG

Je Sammlung können mehrere Sprachmodell-Konfigurationen parallel hinterlegt werden; für jede Konfiguration mit eigenem Einbettungsmodell wird nach einem einmaligen Füll-Lauf ein eigener Einbettungssatz vorgehalten. Danach ist der Wechsel des antwortenden Modells sofort wirksam; Modelle ohne eigenes Einbettungsmodell (z. B. Anthropic) nutzen den Hauptindex der Sammlung.

4.11 EINWILLIGUNG

Soll der Chat erst nach einer Einwilligung laden, bindet sich die Einbettung an die Consent-Lösung der Website des Kunden (Cookiebot, Usercentrics, eigenes Ereignis oder ein von der Consent-Lösung gesetztes Cookie). Bis zur Einwilligung werden keine Chat- oder Einstellungsdaten übertragen; lediglich das Einbettungs-Skript wird vom Server der Instanz geladen.

4.12 DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN (ART. 25 DSGVO)

Löschfrist des Chat-Protokolls 90 Tage; IP-Adressen nur als Prüfwert; keine Cookies im Chat-Widget; Uploads und Sprachaufnahmen ohne Speicherung; Übergabe, Upload und Endpunkt für KI-Agenten nur nach Aktivierung durch den Kunden; Freigabeliste erlaubter Websites; Verarbeitungsregion mit Attest; Geheimnisse werden nie wieder angezeigt.

4.13 ABWEICHUNGEN DER TYPO3-AUSFÜHRUNG

- Die Oberfläche ist ein Backend-Modul in TYPO3 mit denselben Bereichen; Benutzer und Gruppen sind die Backend-Benutzer und -Gruppen von TYPO3.
- Zusätzlicher Datenquellen-Typ „TYPO3-Seiten“ (liest Seiten, Inhalte, Bilder und Dateien der TYPO3-Instanz direkt).
- Frontend-Logins von TYPO3 gelten ohne weiteren Schritt als angemeldete Besucher (4.3); Formulare des TYPO3-Formular-Frameworks können in den Eingang münden.
- Hintergrundprozesse laufen über den TYPO3-Scheduler oder dieselben Konsolenbefehle; Konnektoren werden über die Dienste-Konfiguration von TYPO3 erweitert.
- REST-API, Endpunkt für KI-Agenten und Attest stehen unter dem Pfad der Erweiterung bereit.

5. Sprachmodelle und Dienste Dritter

Die Software unterstützt folgende Anbieter; der Kunde wählt je Sammlung und hinterlegt seinen eigenen API-Schlüssel (Vertrag § 4):

Anbieter	Sitz	Verarbeitungsregion (Anzeige)	Leistungen
Mistral AI SAS	Paris, Frankreich	EU (bei entsprechend gebuchtem/konfiguriertem Dienst)	Chat, Einbettungen, Texterkennung (OCR), Sprache (Eingabe und Ausgabe)
OpenAI	USA	EU oder Welt, abhängig vom konkret gebuchten Dienst/Projekt	Chat, Einbettungen, Sprache
Anthropic	USA	Welt bzw. nach konkret gebuchtem Dienst	Chat
Google (Gemini)	USA	EU oder Welt, abhängig von Produkt/Projekt/Region	Chat, Einbettungen
Gladia SAS	Paris, Frankreich	EU oder Welt, abhängig vom gebuchten Tarif und dessen Unterauftragnehmern	nur Spracherkennung
OpenAI-kompatible Endpunkte	je nach Anbieter	nach tatsächlich gewähltem Anbieter/Endpunkt	Chat, Einbettungen; Vorlagen für IONOS AI Model Hub (DE), STACKIT (DE), Mittwald (DE), OVHcloud (FR), Scaleway (FR), eigene Server (Ollama, vLLM)

Verfügbarkeit, Modellstände, Preise, Datenschutzbedingungen, Unterauftragnehmer, Speicherfristen und tatsächlich verfügbare Verarbeitungsregionen bestimmt der jeweilige Drittanbieter. Der Kunde prüft vor Aktivierung eines Dienstes dessen aktuelle Vertrags- und Datenschutzunterlagen (gebuchter Dienst, Account oder Projekt, Auftragsverarbeitungsvertrag, Unterauftragnehmer) und hält das Ergebnis fest; die Tabelle ist Orientierung, keine Zusage des Anbieters. Eine vom Kunden eingetragene Regionseinstellung ist keine Garantie des Anbieters.

6. Einrichtungspakete

Paket	Leistungen
Einrichtung	Instanz aufsetzen, bis zu vier Datenquellen anbinden, erste Indexierung, Sprachmodell-Konfiguration mit dem Schlüssel des Kunden, Chat gestalten und in die Website einbauen (oder Einbettungs-Code und Anleitung an die Agentur des Kunden), Übergabe mit Einweisung (eine Stunde per Videokonferenz). Gesamtaufwand: bis zu 8 Arbeitsstunden.
Einrichtung mit Begleitung	Zusätzlich: Feinschliff der Anweisungen (Prompts) und der Begrüßung, Aufbau eines Golden Sets mit bis zu 20 Fragen, Schulung der Redaktion (bis zu zwei Stunden) sowie ein vierwöchiger Begleitzeitraum für Auswertung des Protokolls und Nachjustierung. Sämtliche Tätigkeiten innerhalb des Begleitzeitraums werden auf das Gesamtbudget angerechnet. Gesamtaufwand einschließlich Einrichtung: bis zu 16 Arbeitsstunden.
Einrichtung mit umfassender Begleitung	Zusätzlich: Aufbereitung der Inhalte für die Wissensbasis im vereinbarten Umfang, Mehrsprachigkeit, Einrichtung der Agenten, Anbindung von Übergabe und Aktionen sowie ein dreimonatiger Begleitzeitraum. Sämtliche Tätigkeiten innerhalb des Begleitzeitraums werden auf das Gesamtbudget angerechnet. Gesamtaufwand einschließlich der vorhergehenden Leistungen: bis zu 32 Arbeitsstunden. Komplexe Datenmigrationen, individuelle Programmierung und Drittanbieterprojekte sind nicht enthalten.

Die Einrichtungspakete enthalten folgende Höchstkontingente: „Einrichtung“ bis 8 Arbeitsstunden insgesamt; „Einrichtung mit Begleitung“ bis 16 Arbeitsstunden insgesamt; „Einrichtung mit umfassender Begleitung“ bis 32 Arbeitsstunden insgesamt. Nicht verbrauchte Stunden verfallen mit Abschluss des jeweiligen Einrichtungspakets; Mehrleistungen werden nur nach vorheriger Abstimmung nach Aufwand abgerechnet.

7. Preise (Stand 8. September 2026, netto zuzüglich Umsatzsteuer)

Paket	bis 6.000 Datensätze	6.001 bis 20.000 Datensätze	darüber
Grundpaket	149 € / Monat	249 € / Monat	auf Anfrage
Voller Funktionsumfang	249 € / Monat	399 € / Monat	auf Anfrage

Einrichtung	einmalig
Einrichtung	990 €
Einrichtung mit Begleitung	1.900 €
Einrichtung mit umfassender Begleitung	3.900 €

Zuzüglich der Nutzungsentgelte des vom Kunden gewählten Sprachmodell-Anbieters, die der Kunde direkt an diesen zahlt. Zusätzliche Leistungen nach Aufwand zu dem im Auftragsblatt genannten Stundensatz.

8. Nicht Gegenstand der Leistung

- Erstellung, Korrektur oder Pflege der Inhalte des Kunden (außer im Rahmen der Einrichtungspakete).
- Betrieb, Pflege und Sicherung der Website des Kunden und seiner Drittsysteme.
- Verträge, Kosten und Datenschutzvereinbarungen mit Sprachmodell-Anbietern.
- Rechtliche Prüfung der Datenschutzerklärung und der KI-Kennzeichnung des Kunden.
- Individuelle Erweiterungen (Kunden-Extras), Konnektoren für weitere Systeme, Schulungen über das gewählte Einrichtungspaket hinaus.
- Ein bestimmtes inhaltliches Ergebnis einzelner Antworten (Vertrag § 13 Abs. 1).

Anlage 2 — Service Level und Betrieb („dAI Pro Managed“)

1. Verfügbarkeit

1. Der Anbieter schuldet eine Verfügbarkeit der Instanz von 99,0 % im Monatsmittel, gemessen durch die vereinbarte externe Verfügbarkeitsüberwachung am öffentlich erreichbaren Prüfpunkt der Instanz. Der Prüfpunkt prüft bei jedem Aufruf die Datenbank, den Suchindex, die Auslieferung der Anmeldeseite, das Vorhandensein einer Sprachmodell-Konfiguration und das Ergebnis des letzten Chat-Selbsttests, den die Instanz alle 30 Minuten mit einer echten Chat-Anfrage und einer Suche ausführt; als verfügbar gilt jede Minute, in der der Prüfpunkt mit HTTP 200 und dem Status „ok“ antwortet. Ein Chat-Selbsttest ist aktuell, wenn sein Ergebnis nicht älter als 60 Minuten ist. Fehlt ein aktueller Selbsttest oder liegt der letzte erfolgreiche Selbsttest länger als 60 Minuten zurück, darf der Prüfpunkt nicht allein deshalb als „ok“ gewertet werden. Ausfälle, die ausschließlich auf nach Abs. 2 ausgenommenen Diensten Dritter beruhen, bleiben bei der SLA-Berechnung unberücksichtigt; soweit der Prüfpunkt einen solchen Drittanbietersausfall dennoch als „nicht ok“ meldet, dokumentiert der Anbieter die Ursache und bereinigt die Monatsauswertung anhand der Monitoring- und Providerdaten. Diese Sonderregel geht AGB § 18 Abs. 2 vor.
2. Verfügbar ist die Instanz, wenn Anmeldung, Chat und Suche über das Internet erreichbar sind und Anfragen beantwortet werden. Nicht als Nichtverfügbarkeit gelten: angekündigte Wartungsfenster (Abschnitt 2 Abs. 1) und dringende Sicherheitsupdates (Abschnitt 2 Abs. 3), Störungen der Dienste Dritter (Sprachmodell-Anbieter, Website des Kunden, Drittsysteme der Datenquellen) — Ausfälle des Sprachmodell-Anbieters erkennt der Chat-Selbsttest der Instanz selbst und weist sie im Prüfpunkt gesondert aus (Feld `dependency`, Zustand `provider_error`); der Plattformstatus bleibt in diesem Fall „ok“, sodass die externe Messung nach Abs. 1 solche Ausfälle nicht als Nichtverfügbarkeit zählt; als Störung des Anbieters gelten Netz- und Zeitüberschreitungsfehler zum Anbieter, dessen Antworten mit HTTP-Status 5xx, 408, 425 oder 429 sowie unlesbare oder abgebrochene Antworten, nicht dagegen Fehler, die auf Schlüssel, Guthaben oder Konfiguration des Modellzugangs beruhen —, Ausfälle von Netzen außerhalb des Rechenzentrums, höhere Gewalt (AGB § 5 Abs. 2) sowie Beeinträchtigungen, die der Kunde zu vertreten hat (z. B. Überlastung durch eine zu weit gefasste Freigabeliste erlaubter Websites, fehlerhafte Einbindung).
3. Der Sprach-Chat (WebSocket-Dienst) und die Hintergrundverarbeitung (Indexierung, Agenten) sind Teil des Betriebs, aber nicht der Verfügbarkeitsmessung; Störungen dort werden als Störungen nach Abschnitt 3 behandelt.
4. Unterschreitet die gemessene Verfügbarkeit den Wert nach Abs. 1, erhält der Kunde auf Verlangen eine Servicegutschrift von 5 % der auf den betroffenen Monat entfallenden Netto-Grundvergütung je angefangenem Prozentpunkt der Unterschreitung, höchstens 50 %. Der Kunde macht die Gutschrift innerhalb von drei Monaten nach Monatsende in Textform geltend. Gesetzliche Mängel-, Minderungs-, Schadensersatz- und Kündigungsrechte bleiben unberührt; eine Servicegutschrift wird auf Ansprüche wegen derselben Nichtverfügbarkeit angerechnet.

2. Wartung und Updates

1. Planbare Wartungsarbeiten führt der Anbieter außerhalb der Geschäftszeiten des Kunden durch, im Zeitfenster **22:00 bis 06:00 Uhr** oder am Wochenende, und kündigt Arbeiten mit erwarteter Unterbrechung von mehr als 15 Minuten mindestens **48 Stunden** vorher per E-Mail an den technischen Ansprechpartner des Kunden an.
2. Updates der Software (Fehlerbehebungen, Sicherheitsupdates, neue Funktionen) spielt der Anbieter laufend ein. Ein Update wechselt den gemeinsam genutzten Programmstand (Abschnitt 6) und dauert für die Instanz in der Regel wenige Sekunden ohne Unterbrechung des Chats; erforderliche Datenbankmigrationen laufen automatisch.
3. Sicherheitsupdates mit dringendem Handlungsbedarf darf der Anbieter ohne Vorankündigung einspielen; er informiert den Kunden anschließend.
4. Für Änderungen, die eine Anpassung der Einbindung auf der Website des Kunden erfordern, gilt Vertrag § 5 Abs. 3.

3. Support und Störungsbeseitigung

Support-Kanal	E-Mail an daipro@dreistein.de (zentrale Supportadresse); Telefon +49 211 97 53 39 97 für Störungen der Klasse 1
Servicezeiten	Arbeitstage (Anlage 1 Abschnitt 2) von 9:00 bis 17:00 Uhr
Berechtigte Personen	die im Auftragsblatt benannten Ansprechpartner des Kunden und ihre Stellvertreter

Klasse	Definition	Reaktionszeit (innerhalb der Servicezeiten)	Ziel für Behebung oder Umgehung
1 — betriebsverhindernd	Instanz nicht erreichbar, Chat antwortet nicht, Datenverlust droht	4 Stunden	1 Arbeitstag
2 — betriebsbehindernd	Wesentliche Funktion gestört, Betrieb mit Einschränkung möglich (z. B. Indexierung steht, Sprach-Chat aus)	1 Arbeitstag	3 Arbeitstage
3 — sonstige	Fehler ohne wesentliche Einschränkung, Fragen zur Bedienung	2 Arbeitstage	nächstes reguläres Update

Reaktionszeit ist die Zeit bis zur qualifizierten Rückmeldung mit Einschätzung und nächsten Schritten. Behebungsziele sind Zielwerte, keine Garantie. Support umfasst Störungen und Bedienungsfragen zur Software, nicht die Betreuung der Website, Inhalte oder Drittsysteme des Kunden. Beratungsleistungen, die über Störungsbeseitigung und Bedienungsfragen zur Software hinausgehen, sind nicht in der laufenden Vergütung enthalten und werden nur nach vorheriger Abstimmung nach Aufwand vergütet. Eine personelle Vertretung oder durchgehende Erreichbarkeit des Inhabers wird nicht zugesagt. Planbare Abwesenheiten werden, soweit sie voraussichtlich die Reaktionszeiten wesentlich berühren, vorab angekündigt; zwingende gesetzliche Mängel-, Kündigungs- und Schadensersatzrechte bleiben unberührt.

4. Datensicherung

1. Der Anbieter sichert täglich die Datenbank der Instanz und den Dateispeicher und bewahrt tägliche Sicherungen 14 Tage auf; wöchentliche Sicherungen werden acht Wochen aufbewahrt. Die Sicherungen werden vor der Übertragung verschlüsselt und logisch getrennt vom Produktivsystem bei einem anderen Anbieter gespeichert (Anlage 3, Anhang C).
2. Vor Updates mit strukturverändernden Datenbankmigrationen und vor geplanten manuellen Eingriffen des Anbieters in die Daten der Instanz wird eine zusätzliche Sicherung erzeugt.
3. Für eine Wiederherstellung aus Sicherung gilt ein Zielwert von einem Arbeitstag ab qualifizierter Störungsaufnahme, soweit die Sicherung technisch lesbar ist und Umfang/Fehlerbild keine außergewöhnlichen Maßnahmen erfordern; dies ist kein garantierter Wiederherstellungszeitpunkt. Eine Wiederherstellung wegen eines vom Kunden zu vertretenden Datenverlusts kann nach Aufwand vergütet werden.
4. Sicherungen enthalten Kundendaten und unterliegen der Auftragsverarbeitung. Instanzbezogene Sicherungen werden mit Ablauf der Nachlauffrist nach Vertrag § 9 Abs. 3 gezielt gelöscht; Sicherungsgenerationen, aus denen einzelne Instanzen technisch nicht gezielt entfernt werden können, spätestens mit Ablauf ihrer dokumentierten Aufbewahrungsfrist.

5. Überwachung, Protokolle, Löschfristen

1. Der Anbieter überwacht Erreichbarkeit, Speicherplatz und Hintergrunddienste und stellt den Zählwert der Paketgrenzen alle 15 Minuten fest. Der Chat-Selbsttest nach Abschnitt 1 Abs. 1 verursacht je Lauf eine kurze Modellanfrage über den Modellzugang der Instanz (rund 48 am Tag). Der Anbieter berechnet diese Prüfaufrufe nicht gesondert. Bei Verwendung eines Modellzugangs des Kunden können jedoch Nutzungsentgelte des jeweiligen Modellanbieters entstehen (bei üblichen Modellen im Cent-Bereich je Tag); die Aufrufe werden in der Verbrauchsübersicht als „Selbsttest (Verfügbarkeitsprüfung)“ ausgewiesen und bei einem vereinbarten Startkontingent (Vertrag § 4 Abs. 1) nicht auf dessen Gegenwert angerechnet. Ist das Startkontingent verbraucht, setzt der Selbsttest aus, bis der Kunde seinen eigenen Modellzugang hinterlegt hat.
2. Die Instanz protokolliert Chat- und Suchanfragen mit Frage, Antwort, gefundenen Textstellen und technischen Werten. Die IP-Adresse wird nur als schlüsselbasierter HMAC-SHA-256-Prüfwert mit einem je Instanz eigenen Geheimnis gespeichert. Die Protokolle werden standardmäßig nach 90 Tagen gelöscht; ein täglicher Aufräumlauf setzt die Frist unabhängig von neuen Einträgen durch. Auf dokumentierte Weisung des Kunden stellt der Anbieter eine andere Frist ein.
3. Anmeldungen des Anbieters an der Oberfläche der Instanz werden in der Instanz protokolliert. Webserver-Zugriffsprotokolle mit IP-Adressen im Klartext werden automatisch nach 14 Tagen gelöscht und nicht mit dem Chat-Protokoll zusammengeführt.
4. Kostenlose Demo-Umgebungen des Anbieters sind nicht Teil dieses Vertrags.

6. Technischer Betrieb

Merkmal	Ausgestaltung
Rechenzentrum	IONOS SE, Rechenzentrum Niederlauterbach (Frankreich), Region „Europa“; ein Wechsel innerhalb der EU bleibt nach Vertrag § 3 Abs. 1 vorbehalten

Merkmal	Ausgestaltung
Sicherungsspeicher	Hetzner Online GmbH, Storage Box im Rechenzentrum Falkenstein (Deutschland); Sicherungen vor der Übertragung verschlüsselt
Verfügbarkeitsmessung	updown.io (Paris, Frankreich): Abruf des Prüfpunkts <code>/api/v1/health</code> jeder Instanz (Datenbank, Suchindex, Anmeldeseite, Sprachmodell-Konfiguration, letzter Chat-Selbsttest) im Minutentakt aus Roubaix, Frankfurt und Helsinki, Ausfall aus zwei Standorten bestätigt, E-Mail an info@dreistein.de , Wochenbericht und Monatswerte je Instanz (Statistikseite „Uptime SLAs“); übermittelt werden ausschließlich technische Endpunkt-Metadaten (Hostname der Instanz, Zeitpunkt, HTTP-Status, Antwortzeit), keine Kundeninhalte oder Auftragsdaten
Trennung	eigene Datenbank und Datenbankrolle je Instanz (kein Superuser, keine Rechte an den Daten anderer Instanzen), eigenes Datenbankschema je Sammlung, eigener Dateispeicher, eigene Konfiguration, eigene Hintergrunddienste und eigener Sprachdienst je Instanz
Programmstand	ein gemeinsamer, versionierter Programmstand für alle Instanzen (Release), je Instanz per Symlink eingebunden; kundenindividuelle Erweiterungen liegen getrennt in der Instanz und überstehen Updates
Verschlüsselung	TLS für alle Verbindungen (HTTPS, WSS); Zertifikate über Let's Encrypt mit automatischer Erneuerung; Sicherheits-Header des Webserver (HSTS, Content-Type-Schutz, Framing-Schutz, Referrer-Policy)
Zugang der Instanz	Benutzerkonten mit Passwort (nach Stand der Technik gehasht), Anmeldebremse (fünf Fehlversuche je 15 Minuten je IP-Adresse und je Benutzername), API-Token mit Ablauf nach acht Stunden
Skalierung	ein Server für mehrere Instanzen; bei anhaltender Auslastung über 70 % prüft der Anbieter die Verlagerung einzelner Instanzen auf weitere Server
Domain	<code>[kundenname].dreistein.de</code> mit DNS-Eintrag durch den Anbieter oder eigene Domain des Kunden (Kunde setzt einen A- oder CNAME-Eintrag auf die vom Anbieter benannte Adresse)
E-Mail-Versand der Instanz	Über den SMTP-Zugang des Kunden mit der Absenderadresse des Kunden. Der Kunde hinterlegt Server, Zugangsdaten und Absender in der Instanz (Einstellungen → E-Mail-Versand) und prüft die Verbindung dort mit einer Testnachricht. Ohne diesen Zugang versendet die Instanz keine E-Mails (Mensch-Übergabe, Agentenberichte, Hinweise zu Paketgrenzen, Support). Adressen und Mailserver des Anbieters werden für die Instanz nicht verwendet.

7. Exit

Bei Vertragsende: Export nach Vertrag § 9 Abs. 2, Aufbewahrung und anschließende vollständige Löschung mit Löschprotokoll nach Vertrag § 9 Abs. 3. Auf Wunsch Übergabe der Instanz zum Selbstbetrieb nach Aufwand (Vertrag § 9 Abs. 4).

Anlage 3 — Vereinbarung zur Auftragsverarbeitung (Art. 28 DSGVO) für „dAI Pro Managed“ sowie für Support und Fernwartung bei Selbstbetrieb (§ 1 Abs. 4)

Parteien

Verantwortlicher (Auftraggeber): [KUNDE], [Anschrift], vertreten durch [Name] — der „Kunde“ des Hauptvertrags.

Auftragsverarbeiter (Auftragnehmer): Joachim Dreistein Medienentwicklung, Inhaber Joachim Dreistein, Bolkerstraße 14, 40213 Düsseldorf, E-Mail info@dreistein.de — der „Anbieter“ des Hauptvertrags.

§ 1 Gegenstand, Dauer, Verhältnis zum Hauptvertrag

1. Der Auftragnehmer betreibt für den Auftraggeber eine Instanz der Software dAI Pro auf Servern des Auftragnehmers (Hauptvertrag „dAI Pro Managed“). Dabei verarbeitet er personenbezogene Daten im Auftrag des Auftraggebers. Diese Vereinbarung regelt die Rechte und Pflichten der Parteien nach Art. 28 DSGVO.
2. Die Verarbeitung im Einzelnen (Gegenstand, Art, Zweck, Datenkategorien, Betroffene, Speicherung) ist in **Anhang A** beschrieben.
3. Die Vereinbarung gilt für die Dauer des Hauptvertrags und darüber hinaus, bis die Daten nach § 8 gelöscht sind.
4. Für Support- und Fernwartungsleistungen zu Installationen, die der Auftraggeber selbst betreibt (Verträge „dAI Pro-Web“ und „dAI Pro-TYPO3“), gilt diese Vereinbarung mit folgenden Maßgaben: An die Stelle des Anhangs A tritt Anhang D (Fernwartung), an die Stelle des § 3 Abs. 3 und des Anhangs B treten die Maßnahmen nach Anhang D Abschnitt 3; Anhang C gilt nicht, soweit keine Systeme des Auftragnehmers beteiligt sind; § 8 Abs. 2 gilt mit der Maßgabe, dass der Auftragnehmer beim Auftraggeber keine Daten speichert und Arbeitskopien nach Abschluss des Vorgangs löscht. Verweise auf den Hauptvertrag gelten sinngemäß für den jeweils geschlossenen Vertrag; Ansprechpartner und Meldeadresse ergeben sich aus dessen Auftragsblatt.

§ 2 Rollen und Abgrenzung

1. Der Auftraggeber ist Verantwortlicher für alle in seiner Instanz verarbeiteten personenbezogenen Daten: Inhalte der Wissensbasis, Daten der Besucher seiner Websites (Fragen, Uploads, Sprache, Kontaktdaten aus Übergabe und Aktionen, Identitäten angemeldeter Besucher), Daten seiner Beschäftigten (Benutzerkonten, Eingang) und Daten seiner Kunden in Ticketsystemen und Postfächern, die er anbindet.
2. Der Auftragnehmer verarbeitet Vertrags-, Kontakt- und Abrechnungsdaten des Auftraggebers sowie die Stammdaten und Zählwerte der Instanz (Name, Domain, Paket, Grenzen, Nutzungsstand) in eigener Verantwortung (Hauptvertrag § 12 Abs. 2); diese Daten sind nicht

Gegenstand dieser Vereinbarung. Das Protokoll der Anmeldungen des Anbieterkontos (Anhang A, A14) liegt in der Instanz und ist Auftragsdatum; der Auftragnehmer darf eine Kopie ohne Inhalte als Nachweis nach § 7 führen.

3. Bei Drittanbietern für Sprachmodelle, Einbettungen und Sprachdienste, die der Auftraggeber über einen eigenen Account/API-Schlüssel auswählt, richtet sich die datenschutzrechtliche Rolle nach den jeweils geltenden Verträgen, Datenschutzbedingungen und der tatsächlichen Verarbeitung. Soweit der Drittanbieter personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers verarbeitet, besteht das Auftragsverhältnis unmittelbar zwischen Auftraggeber und Drittanbieter; der Auftragnehmer übermittelt Daten an diesen ausschließlich in technischer Ausführung der dokumentierten Weisung und legt die Datenflüsse in Anhang A offen. Soweit ein Drittanbieter Daten für eigene Zwecke verarbeitet, hat der Auftraggeber diese Rolle und Rechtsgrundlage gesondert zu bewerten. Stellt der Auftragnehmer ausnahmsweise einen eigenen Zugangsschlüssel bereit, ist der betreffende Drittanbieter Unterauftragsverarbeiter des Auftragnehmers und vor Einsatz nach § 6 in Anhang C aufzunehmen.

§ 3 Pflichten des Auftragnehmers

1. **Weisungsbindung.** Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO), auch hinsichtlich der Übermittlung an ein Drittland. Als Weisungen gelten der Hauptvertrag, diese Vereinbarung und die Konfiguration, die der Auftraggeber in der Oberfläche der Instanz vornimmt (insbesondere Wahl der Datenquellen, der Sprachmodell- und Audio-Anbieter und der aktivierten Funktionen; die Verarbeitungsregion ist eine Kennzeichnung gegenüber Besuchern, keine Sperre). Weitere Weisungen, etwa zur Löschfrist des Chat-Protokolls, erteilt der Auftraggeber in Textform. Hält der Auftragnehmer eine Weisung für datenschutzrechtlich unzulässig, informiert er den Auftraggeber unverzüglich und darf die Ausführung aussetzen, bis der Auftraggeber sie bestätigt. Ist der Auftragnehmer durch das Recht der Union oder eines Mitgliedstaats zu einer Verarbeitung verpflichtet, teilt er dem Auftraggeber diese rechtliche Anforderung vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
2. **Vertraulichkeit.** Der Auftragnehmer ist Einzelunternehmer; regulären Zugriff auf die Systeme hat ausschließlich der Inhaber. Externe Personen mit Zugriff auf Auftragsdaten werden nur nach § 6 eingeschaltet und vor Aufnahme der Tätigkeit auf Vertraulichkeit verpflichtet. Eine personelle Vertretung oder Notfallperson ist derzeit nicht bestellt und wird dem Auftraggeber nicht zugesagt.
3. **Sicherheit.** Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen des **Anhangs B** (Art. 32 DSGVO) und entwickelt sie mit dem Stand der Technik fort, ohne das Schutzniveau zu unterschreiten. Wesentliche Änderungen teilt er dem Auftraggeber mit.
4. **Unterstützung.** Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten Maßnahmen bei der Beantwortung von Anfragen Betroffener (Art. 12 bis 23 DSGVO) sowie bei den Pflichten aus Art. 32 bis 36 DSGVO (Art. 28 Abs. 3 lit. e und f DSGVO). Auskunfts-, Berichtigungs- und Löschbegehren zu Daten in der Instanz kann der Auftraggeber in der Regel selbst über die Oberfläche erfüllen (Dokumente, Protokolle, Benutzerkonten); darüber hinausgehende Unterstützung leistet der Auftragnehmer nach Aufwand, soweit sie nicht auf seinem Verschulden beruht. Wendet sich ein Betroffener direkt an den Auftragnehmer, leitet er das Begehren unverzüglich an den Auftraggeber weiter und antwortet dem Betroffenen nicht in der Sache. Für eine Datenschutz-Folgenabschätzung des Auftraggebers stellt der Auftragnehmer die

Beschreibungen nach Anhang A und B sowie die Datenflussbeschreibung zu den Sprachmodellen bereit.

5. Meldung von Verletzungen. Der Auftragnehmer meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten in seinem Verantwortungsbereich unverzüglich, in der Regel innerhalb von 24 Stunden und spätestens innerhalb von 48 Stunden nach Kenntnis, an den im Auftragsblatt benannten Ansprechpartner, zunächst mit den verfügbaren Angaben nach Art. 33 Abs. 3 DSGVO; fehlende Angaben reicht er nach. Kenntnis liegt vor, sobald der Auftragnehmer hinreichende Gewissheit über einen Sicherheitsvorfall mit Bezug zu personenbezogenen Daten hat.
6. **Verzeichnis und Nachweise.** Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt dem Auftraggeber die für den Nachweis der Pflichten aus Art. 28 DSGVO erforderlichen Informationen zur Verfügung (§ 7, Art. 28 Abs. 3 lit. h DSGVO).
7. Datenschutzkontakt des Auftragnehmers ist Joachim Dreistein, info@dreistein.de. Ein Datenschutzbeauftragter ist in diesem Vertrag nicht als bestellt bezeichnet. Der Auftragnehmer prüft die gesetzliche Benennungspflicht erneut, wenn sich Personalzahl oder Art, Umfang, Umstände oder Zwecke seiner eigenen Verarbeitungstätigkeiten so ändern, dass Art. 37 DSGVO oder § 38 BDSG einschlägig werden.
8. **Ort der Verarbeitung.** Die Verarbeitung erfolgt in Rechenzentren in der Europäischen Union (Anhang C). Fernzugriffe des Auftragnehmers erfolgen in der Regel aus Deutschland, im Übrigen aus dem Europäischen Wirtschaftsraum, nicht aus Drittländern. Übermittlungen in Drittländer finden nur auf Weisung des Auftraggebers durch die von ihm gewählten Dienste statt (§ 2 Abs. 3).
9. **Löschung nach Abschluss.** Nach Beendigung der Leistungen löscht der Auftragnehmer die Auftragsdaten oder gibt sie zurück (§ 8, Art. 28 Abs. 3 lit. g DSGVO).

§ 4 Pflichten des Auftraggebers

1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung und die Wahrung der Betroffenenrechte verantwortlich. Er informiert die Betroffenen (Website-Besucher, Beschäftigte mit Benutzerkonto, Kunden, Personen in den Inhalten) nach Art. 13 und 14 DSGVO; Textbausteine stellt der Auftragnehmer ohne Gewähr bereit.
2. Der Auftraggeber schließt mit den von ihm gewählten Anbietern von Sprachmodellen und Sprachdiensten die erforderlichen Vereinbarungen nach Art. 28 DSGVO und prüft bei Anbietern außerhalb der EU die Voraussetzungen der Art. 44 ff. DSGVO, einschließlich einer Transfer-Folgenabschätzung, soweit die Übermittlung auf Standardvertragsklauseln beruht. Die Region eines Anbieters trägt er, soweit die Software sie nicht vorgibt, in eigener Verantwortung ein.
3. Der Auftraggeber teilt im Auftragsblatt mit, ob Datenquellen besondere Kategorien personenbezogener Daten (Art. 9 DSGVO), Daten nach Art. 10 DSGVO oder Berufsgeheimnisse (§ 203 StGB) enthalten können. Er stellt die erforderliche Rechtsgrundlage sicher und trifft risikoadäquate Auswahl-, Filter- und Informationsmaßnahmen. Eine lückenlose manuelle Prüfung jedes Datensatzes ist nicht geschuldet, sofern Art und Risiko der Quelle keine weitergehende Kontrolle erfordern. Der Auftragnehmer kann ergänzende Schutzmaßnahmen verlangen oder eine Anbindung ablehnen. Für Berufsgeheimnisträger gilt zusätzlich Anhang E. Ein Startkontingent über einen Zugang des Auftragnehmers oder ein Drittlanddienst wird bei Berufsgeheimnissen oder besonderen Datenkategorien nur aktiviert, wenn dies im Auftragsblatt ausdrücklich freigegeben ist und die datenschutz- bzw. berufsrechtliche Einbindung des konkret eingesetzten

Dienstes dokumentiert wurde. Soweit § 203 StGB einschlägig ist, bleibt das Startkontingent für solche Daten deaktiviert, solange nicht dokumentiert ist, dass auch der konkret eingesetzte Unterauftragnehmer in berufsrechtlich zulässiger Weise eingebunden und in dem erforderlichen Umfang zur Geheimhaltung verpflichtet ist.

4. Der Auftraggeber prüft vor Inbetriebnahme, ob eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich ist (KI-gestützte Interaktion mit Betroffenen); der Auftragnehmer stellt hierfür die Unterlagen nach § 3 Abs. 4 bereit.
5. Der Auftraggeber benennt im Auftragsblatt die Personen, die Weisungen erteilen dürfen, und einen Ansprechpartner für Meldungen nach § 3 Abs. 5.
6. Bindet der Auftraggeber Systeme mit Beschäftigtendaten an, aktiviert er die betreffenden Funktionen erst, nachdem er die Betroffeneninformationen bereitgestellt, eine tragfähige Rechtsgrundlage nach DSGVO/BDSG bestimmt und bestehende Mitbestimmungsrechte beachtet hat, insbesondere § 87 Abs. 1 Nr. 6 und § 90 Abs. 1 Nr. 3 BetrVG. Eine Betriebsvereinbarung kann eine geeignete Grundlage sein, muss aber ihrerseits die Anforderungen der DSGVO und des Art. 88 DSGVO erfüllen.

§ 5 Weisungsberechtigte Personen

Weisungen erteilen die im Auftragsblatt benannten Personen des Auftraggebers. Beim Auftragnehmer nimmt Joachim Dreistein Weisungen entgegen. Änderungen sind in Textform mitzuteilen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

§ 6 Subunternehmer

1. Der Auftraggeber genehmigt allgemein die Einschaltung der in **Anhang C** genannten Subunternehmer (Art. 28 Abs. 2 Satz 2 DSGVO).
2. Beabsichtigte Änderungen der Unterauftragsverarbeiter teilt der Auftragnehmer mindestens vier Wochen vorher in Textform mit. Widerspricht der Auftraggeber innerhalb von zwei Wochen aus einem sachlichen datenschutzrechtlichen Grund, bemühen sich die Parteien um eine zumutbare Lösung. Gelingt dies nicht und ist der neue Unterauftragsverarbeiter für die weitere Leistung erforderlich, kann jede Partei den betroffenen Hauptvertrag mit einer Frist von einem Monat zum Monatsende kündigen.
3. Mit jedem Subunternehmer schließt der Auftragnehmer einen Vertrag, der diesem dieselben Datenschutzpflichten auferlegt wie diese Vereinbarung dem Auftragnehmer (Art. 28 Abs. 4 DSGVO). Kommt ein Subunternehmer seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten dieses Subunternehmers (Art. 28 Abs. 4 Satz 2 DSGVO); die wesentlichen datenschutzrechtlichen Inhalte des Subunternehmervertrags stellt er auf Anfrage zur Verfügung. Dienste, die der Auftragnehmer nur als Nebenleistung ohne Zugriff auf Auftragsdaten nutzt (Zertifikatsstelle, DNS-Verwaltung, Abruf des Referenzkurses der Europäischen Zentralbank, Überwachung der Sicherungsläufe mit bloßer Erfolgsmeldung ohne Inhaltsdaten, Verfügbarkeitsmessung des öffentlichen Endpunkts von außen mit Adresse, Antwortcode und Antwortzeit), sind keine Subunternehmer.
4. **Drittländer.** Subunternehmer des Auftragnehmers sitzen in der EU. Dienste mit Sitz oder Unterauftragnehmern in Drittländern werden nur eingesetzt, wenn der Auftraggeber sie selbst

wählt (§ 2 Abs. 3) oder ihrer Einschaltung nach Abs. 2 nicht widersprochen hat und geeignete Garantien nach Art. 44 ff. DSGVO vorliegen.

§ 7 Kontrollrechte

1. Der Auftragnehmer weist die Einhaltung seiner Pflichten durch geeignete Unterlagen nach: diese Vereinbarung mit Anhängen, das Verzeichnis nach Art. 30 Abs. 2 DSGVO, die Beschreibung der Maßnahmen nach Anhang B, Protokolle der Anmeldungen des Anbieterkontos, Löschprotokolle sowie auf Anfrage Berichte über sicherheitsrelevante Prüfungen.
2. Der Auftraggeber kann einmal je Kalenderjahr eine angemessene Dokumenten- oder Remote-Kontrolle sowie zusätzlich aus konkretem Anlass eine Kontrolle durchführen oder durch einen zur Vertraulichkeit verpflichteten sachkundigen Dritten durchführen lassen. Eine Vor-Ort-Inspektion ist zulässig, wenn eine Dokumenten-/Remote-Kontrolle zur Prüfung eines konkreten, erheblichen Datenschutzanlasses nicht ausreicht oder eine Aufsichtsbehörde sie verlangt. Reguläre Kontrollen sind grundsätzlich zwei Wochen vorher anzukündigen; Anlasskontrollen dürfen kurzfristiger erfolgen. Die Kontrolle wahrt Betriebs- und Geschäftsgeheimnisse sowie Daten anderer Kunden. Für die erste reguläre Dokumenten-/Remote-Kontrolle pro Kalenderjahr erhebt der Auftragnehmer kein zusätzliches Entgelt. Zusätzliche anlasslose Kontrollen sind nach Vereinbarung möglich und werden nach nachgewiesenem Zeitaufwand vergütet. Keine zusätzliche Kontrollvergütung fällt an, wenn die Kontrolle auf einer Datenschutzverletzung, behördlichen Anordnung, einem konkret begründeten Verdacht eines wesentlichen Verstoßes beruht oder einen wesentlichen Verstoß des Auftragnehmers bestätigt. Eigene Kosten des Auftraggebers/Auditors trägt der Auftraggeber.
3. Kontrollen der Aufsichtsbehörde beim Auftragnehmer, die den Auftraggeber betreffen, teilt der Auftragnehmer mit, soweit zulässig.

§ 8 Löschung und Rückgabe

1. Während der Laufzeit löscht der Auftraggeber Daten selbst über die Oberfläche der Instanz (Dokumente, Datenquellen, Sammlungen, Benutzerkonten, Protokolle). Die Software löscht Chat-Protokolle nach der eingestellten Frist (Standard 90 Tage, Anlage 2 Abschnitt 5) und verarbeitet hochgeladene Dateien und Sprachaufnahmen der Besucher nur für die Dauer der Anfrage, ohne sie zu speichern.
2. Nach Beendigung des Hauptvertrags stellt der Auftragnehmer die Daten der Instanz zur Rückgabe bereit (Hauptvertrag § 9 Abs. 2) und löscht sie nach Ablauf der Nachlauffrist des Hauptvertrags § 9 Abs. 3 vollständig. Instanzbezogene Sicherungen löscht er gezielt zum selben Zeitpunkt; soweit eine gezielte Löschung aus einer Sicherungsgeneration technisch nicht möglich ist, wird diese spätestens mit Ablauf ihrer dokumentierten Aufbewahrungsfrist, längstens acht Wochen nach Ablauf der Nachlauffrist, gelöscht und bis dahin nicht wiederhergestellt. Über die Löschung erstellt er ein Protokoll und übermittelt es dem Auftraggeber auf Verlangen. Der Auftraggeber kann statt der Rückgabe die sofortige Löschung verlangen.

§ 9 Haftung

Die Haftungsregelungen des Hauptvertrags gelten im Innenverhältnis der Parteien nur, soweit gesetzlich zulässig. Sie beschränken weder Ansprüche betroffener Personen nach Art. 82 DSGVO gegen die jeweils verantwortliche Partei noch den gesetzlichen Innenausgleich nach Art. 82 Abs. 5

DSGVO. Behördliche Geldbußen und Sanktionen trägt jede Partei grundsätzlich selbst, soweit sie auf ihrem eigenen Verantwortungsbereich beruhen; zwingende gesetzliche Rückgriffs- oder Ausgleichsansprüche bleiben unberührt.

§ 10 Schlussbestimmungen

1. Diese Vereinbarung geht in Fragen des Datenschutzes den übrigen Vereinbarungen der Parteien vor (Hauptvertrag § 15 Abs. 1).
2. Diese Vereinbarung und ihre Änderungen bedürfen der Schriftform; die elektronische Form einschließlich der Textform genügt (Art. 28 Abs. 9 DSGVO). Die Anhänge B und C darf der Auftragnehmer im Rahmen des § 3 Abs. 3 und des § 6 Abs. 2 fortschreiben; Anhang A wird ergänzt, wenn der Auftraggeber weitere Funktionen aktiviert, und die jeweils aktuelle Beschreibung stellt der Auftragnehmer bereit.
3. Es gilt deutsches Recht. Sollte eine Bestimmung unwirksam sein, bleibt die Vereinbarung im Übrigen wirksam; an die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung.

Unterzeichnung: Diese Vereinbarung einschließlich ihrer Anhänge wird mit dem Hauptvertrag geschlossen — durch das von beiden Parteien unterschriebene Auftragsblatt, soweit der Hauptvertrag eines vorsieht (dAI Pro Managed: Anlage 4 Abschnitt 7), sonst durch Unterzeichnung des Hauptvertrags; das wahrt die Form nach § 10 Abs. 2. Eine gesonderte Unterschrift unter diese Vereinbarung ist nicht erforderlich.

Anhang A — Verarbeitung im Einzelnen

Gegenstand: Betrieb einer dAI Pro-Instanz (Wissensbasis, KI-Assistent, Agenten, Support-Werkzeuge) für den Auftraggeber.

Zweck: Beantwortung von Fragen der Website-Besucher und Beschäftigten des Auftraggebers aus dessen Inhalten; Pflege und Qualitätsprüfung der Wissensbasis; Unterstützung des Kundensupports des Auftraggebers; Betrieb, Sicherung und Abrechnung.

Betroffene: Besucher der Websites des Auftraggebers; Personen, deren Daten in den angebundenen Inhalten vorkommen (Beschäftigte, Ansprechpartner, Autoren, Referenzkunden); Beschäftigte des Auftraggebers mit Benutzerkonto; Kunden und Interessenten des Auftraggebers, deren Vorgänge in angebundenen Ticketsystemen oder Postfächern liegen.

Nr.	Verarbeitung	Datenkategorien	Speicherung und Frist
A1	Wissensbasis: Auslesen der vom Auftraggeber angebundenen Quellen (Websites, Dateien, Tabellen, Datenbanken, Wissens- und Ticketsysteme, Postfächer), Zerlegung in Abschnitte, Einbettung, Volltextindex	alle in den Quellen enthaltenen Daten, z. B. Namen, Kontaktdaten, Inhalte von Tickets und E-Mails	Datenbank der Instanz (Schema je Sammlung) und Dateispeicher; bis zur Löschung durch den Auftraggeber oder Vertragsende

Nr.	Verarbeitung	Datenkategorien	Speicherung und Frist
A2	Chat und Suche: Übermittlung der Frage, des Gesprächsverlaufs der Sitzung, der gefundenen Abschnitte und bei Anhang oder Identität des Anhangstextes bzw. der Identitätsangaben an das vom Auftraggeber gewählte Sprachmodell; Antwort an den Besucher	Frage, Verlauf, gefundene Abschnitte, Antwort	transient; Verlauf nur im Browser des Besuchers (Sitzungsspeicher); Antwort-Cache je Sammlung: Frage und Antwort ohne Sitzungs- oder Absenderbezug, automatische Löschung nach 24 Stunden
A3	Chat-Protokoll: Fragen und Antworten mit technischen Werten	Frage, Antwort, Verfahren, gefundene Textstellen (Ablaufprotokoll), Anbieter und Modell, Sprache, Dauer, Token, Kosten, Ergebnis, Feedback, zufällige Gesprächskennung, Herkunft (Website), IP-Adresse nur als schlüsselbasierter Prüfwert (HMAC-SHA-256 mit Instanzgeheimnis), bei angemeldeten Besuchern ein ebenso gebildetes Pseudonym	Datenbank der Instanz; Löschung nach 90 Tagen (auf Weisung des Auftraggebers andere Frist) durch täglichen Aufräumlauf
A4	Datei- und Foto-Upload durch Besucher	Inhalt der Datei (Text, Bild), Dateiname, Typ, Größe	Datei nur für die Dauer der Anfrage; im Protokoll nur Name, Typ, Größe
A5	Sprach-Chat: Übermittlung der Sprachaufnahme an den vom Auftraggeber gewählten Spracherkennungsdienst, Rückgabe als Text; Vorlesen der Antwort	Sprachaufnahme, Transkript	Aufnahme nur streamend; keine Speicherung in der Instanz
A6	Mensch-Übergabe: Formular im Chat, Versand per E-Mail an vom Auftraggeber benannte Adressen, optional Kopie an den Besucher	Name, E-Mail-Adresse, Anliegen, vollständiger Gesprächsverlauf mit maschinell erzeugter Zusammenfassung	E-Mail-Versand über den vom Auftraggeber in der Instanz hinterlegten SMTP-Zugang (Mailserver des Auftraggebers, Anlage 2 Abschnitt 6); im Protokoll letzte Frage und Gesprächsverlauf ohne Kontaktdaten
A7	Aktionen aus dem Chat: Rückruf, Termin, Ticket, Webhook an Systeme des Auftraggebers nach Bestätigung des Besuchers	vom Besucher eingegebene Kontaktdaten und Anliegen	Übermittlung an das vom Auftraggeber konfigurierte System; in der Instanz Referenznummer, Kanal, Zeitpunkt, letzte Frage und Verlauf ohne Kontaktdaten

Nr.	Verarbeitung	Datenkategorien	Speicherung und Frist
A8	Angemeldete Besucher: Übernahme einer vom Auftraggeber signierten Identität für persönliche Antworten über Werkzeuge; Übermittlung von Kennung, Attributen und Werkzeugantworten zusammen mit der Frage an das gewählte Sprachmodell (A2)	Kennung, Name, Gruppen, vom Auftraggeber übergebene Attribute; Antworten der angebundenen Systeme	nur für die Dauer der Anfrage; im Protokoll ein Pseudonym (Hash der Kennung)
A9	Eingang und Ticket-Assistent: Lesen offener Vorgänge aus Ticketsystem oder Postfach, Übermittlung der Ticketinhalte an das gewählte Sprachmodell zur Entwurfserstellung, Antwortentwürfe als interne Notiz, Freigabe durch Beschäftigte, Übernahme freigegebener Antworten in die Supportdatenbank auf Klick	Inhalte der Tickets und E-Mails (Absender, Text, Anhänge), Bearbeiter, Entwürfe, Freigabeentscheidungen	Datenbank der Instanz; Vorgänge bis zur Löschung durch den Auftraggeber; übernommene Antworten als Dokumente (A1)
A10	Agenten: zeitgesteuerte Prüfungen der Wissensbasis und des Protokolls, Berichte per E-Mail	Daten aus A1 und A3; Berichte	Berichte in der Datenbank bis zur Löschung; E-Mails über den Mailserver des Auftragnehmers
A11	Benutzerkonten des Auftraggebers	Benutzername, Name, E-Mail, Passwort-Hash, Gruppen, Rolle im Eingang, Backend-Sprache; fehlgeschlagene Anmeldeversuche mit IP-Adresse (Anmeldebremse)	Datenbank der Instanz; bis zur Löschung durch den Auftraggeber; Anmeldeversuche 15 Minuten
A12	Verbrauchsprotokoll	Aufrufe, Token, Seiten, Kosten je Sammlung und Zweck; ohne Inhalte	Datenbank der Instanz; Vertragslaufzeit
A13	Datensicherung	Kopien der Datenbank und des Dateispeichers einschließlich Konfiguration	Sicherungsspeicher auf dem Server des Auftragnehmers (IONOS SE) und, vor der Übertragung verschlüsselt, bei der Hetzner Online GmbH (Anhang C); Fristen nach Anlage 2 Abschnitt 4 des Hauptvertrags; beim Entfernen einer Instanz erzeugte Sicherungen werden ebenfalls verschlüsselt und nach der Nachlaufzeit gelöscht
A14	Zugriff des Anbieterkontos (Fernwartung, Störungsbeseitigung)	Einsicht in Daten der Instanz im erforderlichen Umfang; Protokoll mit Benutzername, IP-Adresse, Grund und Zeitpunkt der Anmeldung	Zugriffsprotokoll in der Instanz; Zugriff auf die Oberfläche nur nach Freigabe (Hauptvertrag § 8)
A15	Endpunkt für KI-Agenten (MCP) , falls aktiviert	Frage des anfragenden Systems, Antwort, IP-Prüfwert	Protokoll wie A3

Nr.	Verarbeitung	Datenkategorien	Speicherung und Frist
A16	Server- und Anwendungsprotokolle (Webserver, Sprachdienst, Fehlerprotokolle)	IP-Adresse, Zeitpunkt, aufgerufene Adresse, Browserkennung, Fehlermeldungen ohne Chat-Inhalte	Server des Auftragnehmers; automatische Löschung nach 14 Tagen; keine Zusammenführung mit Chat-Protokollen
A17	E-Mail-Versand aus Übergabe, Agenten und Benachrichtigungen	Empfängeradressen, Inhalte der E-Mails (A6, A10)	Versand ausschließlich über den vom Auftraggeber in der Instanz hinterlegten SMTP-Zugang mit dessen Absenderadresse (Anlage 2 Abschnitt 6); Mailserver und Versandprotokolle liegen beim Auftraggeber; ohne hinterlegten Zugang findet kein Versand statt
A18	Konfigurationsprotokoll (Weisungsdokumentation)	Änderungen der Sammlungs-Konfiguration mit Zeitpunkt und Benutzer	Datenbank der Instanz (Tabelle <code>tx_aiconnect_config_log</code>), Ansicht „Änderungsprotokoll“ je Sammlung

Anhang B — Technische und organisatorische Maßnahmen

Die Maßnahmen nach Art. 32 DSGVO sind im Dokument „**Technische und organisatorische Maßnahmen dAI Pro Managed**“ (`anlage-tom-dai-pro.md`) in der bei Vertragsschluss gültigen Fassung beschrieben; es ist Bestandteil dieser Vereinbarung.

Anhang C — Subunternehmer

1. SUBUNTERNEHMER DES AUFTRAGNEHMERS

IONOS SE · Unternehmen	
Sitz	Elgendorfer Str. 57, 56410 Montabaur, Deutschland
Leistung	Server-Hosting (virtueller Server, VPS)
Datenbezug	alle Daten der Instanz (Speicherung und Betrieb)
Ort der Verarbeitung	Europäische Union — Rechenzentrum Niederlauterbach, Frankreich (Auskunft der IONOS SE vom 17.09.2026; Region „Europa“, Standortwechsel innerhalb der EU nach § 3 Abs. 8 vorbehalten). Unterauftragnehmer der IONOS SE für diese Leistungen laut deren Anhang 2 (Version 4.5, 04/2026): Arsys Internet S.L.U., Logroño, Spanien (Plattformbetrieb und Support VPS); 1&1 Mail & Media GmbH, Montabaur, und Open-Xchange GmbH, Olpe (E-Mail); Cloudflare ist laut IONOS-Auskunft für VPS ohne Bedeutung, Plesk wird nicht genutzt
Grundlage	Vertrag zur Auftragsverarbeitung mit IONOS SE (Version 1.3, Stand 03/2026, zugleich Ziffer 11.3 der IONOS-AGB), abgeschlossen am 17.09.2026

Mistral AI SAS · Unternehmen

Sitz	Paris, Frankreich
Leistung	Sprachmodell/Einbettungen[, Sprache] ausschließlich beim optionalen Startkontingent über den Anbieter-Account
Datenbezug	Fragen, gefundene Textstellen, Gesprächsverlauf im erforderlichen Umfang, ggf. Audio
Ort der Verarbeitung	Europäische Union; konkrete Verarbeitungsregion des verwendeten Mistral-Dienstes/Plans vor Aktivierung dokumentieren
Grundlage	AVV/DPA mit Mistral AI; gilt nur bei im Auftragsblatt gewähltem Startkontingent

Hetzner Online GmbH · Unternehmen

Sitz	Industriestr. 25, 91710 Gunzenhausen, Deutschland
Leistung	Speicherplatz für Sicherungskopien (Storage Box)
Datenbezug	verschlüsselte Sicherungen der Instanz (Datenbank, Dateien, Konfiguration); Verschlüsselung vor der Übertragung, Hetzner hat keinen Schlüssel
Ort der Verarbeitung	Deutschland (Rechenzentrum Falkenstein/Vogtl.); laut Hetzner-AVV Anlage 3 für EU-Standorte keine weiteren Subunternehmer
Grundlage	AV-Vertrag nach Art. 28 DSGVO vom 17.09.2026 (Hetzner-Fassung 1.2 vom 16.02.2026)

Regelmäßige Unterauftragsverarbeiter sind die IONOS SE (Hosting, E-Mail) und die Hetzner Online GmbH (verschlüsselte Sicherungen). Mistral AI SAS ist zusätzlich nur dann genehmigter Unterauftragsverarbeiter, wenn im Auftragsblatt das optionale Startkontingent über den Mistral-Zugang des Auftragnehmers gewählt ist. Jeder andere vom Auftragnehmer bereitgestellte Modell-/Sprachdienstzugang ist vor Einsatz nach § 6 als Unterauftragsverarbeiter in Anhang C aufzunehmen. Werden eine externe Überwachung mit Auftragsdatenzugriff oder ein Mail-Relay mit Auftragsdatenzugriff eingerichtet, nimmt der Auftragnehmer den betreffenden Anbieter vor Einsatz nach § 6 in Anhang C auf. Die Subunternehmerliste der IONOS SE (Anhang 2 zum IONOS-AVV, Version 4.5, Stand 04/2026) wurde am 17.09.2026 geprüft: Für die genutzten Leistungen (VPS, E-Mail) sind ausschließlich Unterauftragnehmer mit Sitz in der EU beteiligt; die Einträge mit Drittlandbezug betreffen nicht genutzte Produkte.

2. DIENSTE AUF WAHL UND IN VERANTWORTUNG DES AUFTRAGGEBERS (KEINE SUBUNTERNEHMER)

Dienst	Sitz	Wann beteiligt	Hinweis
Mistral AI SAS	Paris, Frankreich	wenn vom Auftraggeber mit eigenem Mistral-Account/API-Schlüssel gewählt; eigener Vertrag des Auftraggebers mit Mistral	Kein Unterauftragsverarbeiter des Auftragnehmers in dieser Konstellation; aktuelle DPA/Verarbeitungsregion/Aufbewahrung des Kundenaccounts prüfen.

Dienst	Sitz	Wann beteiligt	Hinweis
OpenAI (Vertragspartner OpenAI Ireland Ltd., Dublin; Verarbeitung durch OpenAI, L.L.C., USA, als dessen Unterauftragnehmer)	Irland / USA	wenn vom Auftraggeber mit eigenem Account/API-Schlüssel gewählt; eigener Vertrag des Auftraggebers mit diesem Dienst	Kein Unterauftragsverarbeiter des Auftragnehmers in dieser Konstellation; DPA und Drittlandmechanismus des konkreten Kundenaccounts prüfen.
Anthropic (Vertragspartner Anthropic Ireland Ltd., Dublin; Verarbeitung durch Anthropic, PBC, USA)	Irland / USA	wenn vom Auftraggeber mit eigenem Account/API-Schlüssel gewählt; eigener Vertrag des Auftraggebers mit diesem Dienst	Kein Unterauftragsverarbeiter des Auftragnehmers in dieser Konstellation; DPA, Unterauftragnehmer, Speicher-/Trainingsregeln und Verarbeitungsorte des Kundenaccounts prüfen.
Google (Vertragspartner Google Ireland Ltd. bzw. Google Cloud EMEA Ltd., Dublin; Verarbeitung durch Google LLC, USA)	Irland / USA	wenn vom Auftraggeber mit eigenem Account/API-Schlüssel gewählt; eigener Vertrag des Auftraggebers mit diesem Dienst	Kein Unterauftragsverarbeiter des Auftragnehmers in dieser Konstellation; DPA und tatsächliche Verarbeitungsregion des konkret gebuchten Google-Dienstes prüfen.
Gladia SAS	Paris, Frankreich	wenn vom Auftraggeber mit eigenem Account/API-Schlüssel gewählt; eigener Vertrag des Auftraggebers mit diesem Dienst	Kein Unterauftragsverarbeiter des Auftragnehmers in dieser Konstellation; DPA, Unterauftragnehmer und Speicherfristen des konkret gebuchten Plans prüfen.
OpenAI-kompatible Endpunkte (IONOS AI Model Hub, STACKIT, Mittwald, OVHcloud, Scaleway, eigene Server)	je nach Anbieter	wenn vom Auftraggeber mit eigenem Account/API-Schlüssel gewählt; eigener Vertrag des Auftraggebers mit diesem Dienst	Kein Unterauftragsverarbeiter des Auftragnehmers in dieser Konstellation; AVV/DPA und Verarbeitungsort des gewählten Endpunkts prüfen.
Cloudflare, Inc. (Turnstile)	San Francisco, USA / EU-Niederlassung	Bot-Schutz im Übergabe-Formular, nur wenn der Auftraggeber ihn wünscht; der Auftragnehmer hinterlegt die Schlüssel aus dem Cloudflare-Konto des Auftraggebers in der Instanz	IP-Adresse und technische Daten des Besuchers an Cloudflare; Drittlandmechanismus vor Aktivierung prüfen. Turnstile wird ausschließlich mit Schlüsseln aus einem Cloudflare-Konto des Auftraggebers aktiviert.

Dienst	Sitz	Wann beteiligt	Hinweis
Ticket-, Wissens- und Speichersysteme des Auftraggebers (Zammad, Freshdesk, Zendesk, Jira, HubSpot, Confluence, Notion, Nextcloud, SharePoint, Google Drive, IMAP-Postfächer)	je nach Anbieter	als Datenquelle oder Ziel von Aktionen, wenn angebunden	Verträge des Auftraggebers

Die nachfolgende Tabelle betrifft Dienste, die der Auftraggeber mit eigenem Account/API-Schlüssel auswählt. Sie sind in dieser Konstellation keine Unterauftragsverarbeiter des Auftragnehmers. Angaben zu Sitz, Unterauftragnehmern, Speicherfristen und Verarbeitungsregionen sind vom Auftraggeber vor Aktivierung anhand seiner aktuellen Vertragsunterlagen zu prüfen. Für Übermittlungen in die USA kann ein gültiger Angemessenheitsbeschluss (EU-US Data Privacy Framework) genutzt werden, soweit der relevante US-Rechtsträger gelistet ist; andernfalls sind geeignete Garantien nach Art. 46 DSGVO erforderlich.

Anhang D — Fernwartung und Support bei Selbstbetrieb (Verträge „dAI Pro-Web“ und „dAI Pro-TYPO3“)

1. VERARBEITUNG

Merkmal	Ausgestaltung
Gegenstand	Fehleranalyse, Störungsbeseitigung, Unterstützung bei Installation und Konfiguration auf Systemen des Auftraggebers
Zweck	Erfüllung der Support- und Pflegepflichten des jeweiligen Vertrags
Art der Verarbeitung	lesender Zugriff auf Oberfläche, Datenbank, Dateien und Protokolle der Installation; schreibender Zugriff nur zur Fehlerbehebung nach Weisung
Datenkategorien	alle in der Installation verarbeiteten Daten (Anhang A, A1 bis A12), soweit für den Vorgang erforderlich
Betroffene	wie Anhang A
Dauer	je Supportvorgang; Zugänge werden nach Abschluss deaktiviert oder vom Auftraggeber widerrufen
Speicherung beim Auftragnehmer	keine dauerhafte Speicherung; Arbeitskopien (Logauszüge, Datenbankauszüge) nur für die Dauer der Analyse, danach Löschung; keine Übernahme in Test- oder Demosysteme

2. WEISUNG UND ZUGANG

Der Auftraggeber erteilt den Zugang je Vorgang (Benutzerkonto mit erforderlichen Rechten, Fernwartungs-Freigabe in der Software, SSH- oder Datenbankzugang nur, soweit erforderlich) und kann ihn jederzeit widerrufen. Der Auftragnehmer dokumentiert Anlass, Zeitraum und Umfang jedes Zugriffs und stellt die Dokumentation auf Anfrage bereit.

3. MASSNAHMEN BEI FERNZUGRIFFEN

- Zugriff nur über verschlüsselte Verbindungen (HTTPS, SSH, VPN des Auftraggebers).
- Arbeitsplatzrechner des Auftragnehmers mit vollständiger Datenträgerverschlüsselung, Bildschirmsperre und aktuellem Betriebssystem.
- Keine Weitergabe von Zugangsdaten; Ablage von Zugangsdaten nur in einem Passwortmanager; Löschung nach Abschluss des Vorgangs, sofern der Auftraggeber keinen dauerhaften Supportzugang wünscht.
- Keine Speicherung von Auftragsdaten außerhalb der Analyse; Löschung von Arbeitskopien nach Abschluss; keine Übermittlung an Dritte.
- Zugriff ausschließlich durch den Inhaber (§ 3 Abs. 2).

Anhang E — Verpflichtung nach § 203 Abs. 4 StGB (nur bei Auftraggebern, die Berufsgeheimnisträger sind)

Musterverpflichtung für Berufsgeheimnisse (§ 203 StGB)

Der Auftragnehmer wird, soweit der Auftraggeber Berufsgeheimnisträger ist und der Auftragnehmer bestimmungsgemäß Kenntnis von geschützten Geheimnissen erlangen kann, als sonstige mitwirkende Person im Sinne des § 203 Abs. 3 Satz 2 StGB tätig. Er verpflichtet sich, die ihm im Rahmen der Tätigkeit bekannt werdenden fremden Geheimnisse nur im zur Vertragserfüllung erforderlichen Umfang zu verarbeiten und nicht unbefugt zu offenbaren. Der Auftragnehmer verpflichtet weitere Personen, die bestimmungsgemäß Kenntnis solcher Geheimnisse erlangen können, vor ihrem Einsatz in mindestens gleichem Umfang und weist dies dem Auftraggeber auf Verlangen nach. Die Verpflichtung gilt zeitlich unbeschränkt über das Vertragsende hinaus. Der Auftraggeber bleibt dafür verantwortlich, dass die Einbeziehung der mitwirkenden Person im konkreten Berufsrecht zulässig ist.

Ort, Datum: _____

Joachim Dreistein Medienentwicklung, Joachim Dreistein (Auftragnehmer)

Technische und organisatorische Maßnahmen (Art. 32 DSGVO) — dAI Pro Managed

1. Vertraulichkeit

1.1 ZUTRITTSKONTROLLE (PHYSISCH)

- Die Server stehen in Rechenzentren der IONOS SE in der Europäischen Union (Rechenzentrum Niederlauterbach, Frankreich); der Zutritt ist durch den Rechenzentrumsbetreiber geregelt (Zutrittskontrolle, Videoüberwachung, Sicherheitspersonal nach dessen Zertifizierungen; ISO/IEC-27001-Zertifikat der IONOS-Gruppe, TÜV NORD, gültig bis 18.04.2028).
- Beim Auftragnehmer werden keine Auftragsdaten auf lokalen Geräten dauerhaft gespeichert; Arbeitsplatzrechner sind vollverschlüsselt und mit Bildschirmsperre gesichert.

1.2 ZUGANGSKONTROLLE (SYSTEME)

- Serverzugang ausschließlich per SSH mit Schlüsselpaaren; Passwort-Anmeldung und interaktive Root-Anmeldung mit Passwort sind abgeschaltet.
- Fehlgeschlagene Anmeldeversuche werden durch fail2ban gesperrt; eine Firewall (UFW) lässt nur die benötigten Ports zu (SSH, HTTP, HTTPS sowie die Ports eines Konferenzdienstes des Auftragnehmers auf demselben Server, Abschnitt 1.4). Die Sprachdienste der Instanzen sind nur über den Webserver erreichbar und binden keinen öffentlichen Port.
- Datenbanken sind nur vom Anwendungsserver erreichbar (Bindung an localhost).
- Zugang zu den Systemen hat ausschließlich der Inhaber; es gibt keine geteilten Konten. Administrative Befehle für das Instanzsystem sind auf einzelne, geprüfte Skripte beschränkt (sudo-Regeln für den Webserver-Benutzer).
- Oberfläche der Instanz: persönliche Benutzerkonten mit Passwort (Hash nach dem jeweils aktuellen Standard der Anwendungsplattform), rollenbasierte Rechte und Anmeldebremse mit fünf Fehlversuchen je 15 Minuten je IP-Adresse und Benutzername; API-Token laufen nach acht Stunden ab. Für Administratoren, das Anbieterkonto und Redakteure ist die Zwei-Faktor-Anmeldung verpflichtend (Authenticator-App nach TOTP, Passkeys/WebAuthn oder Backup-Codes; Einrichtung wird nach der Anmeldung erzwungen, auch die API-Anmeldung verlangt den zweiten Faktor); in der TYPO3-Ausführung über die MFA-Funktionen von TYPO3 mit Pflicht für alle Backend-Benutzer.

1.3 ZUGRIFFSKONTROLLE (BERECHTIGUNGEN)

- Rechte in der Instanz über Gruppen: Sammlungen, Datenquellen, Werkzeuge, Agenten, LLM-Konfigurationen, Rollen im Eingang; Administratoren getrennt von Redakteuren; Konten für Integrationen mit minimalen Rechten.
- API-Schlüssel und Geheimnisse werden gespeichert, aber nie wieder angezeigt.
- **Zugriff des Anbieterkontos auf die Oberfläche** nur, solange die Instanz keinen aktiven Benutzer des Auftraggebers hat oder ein Administrator des Auftraggebers die Fernwartung für einen Zeitraum oder bis auf Widerruf freigegeben hat; die Sitzung endet mit Ablauf der Freigabe; jede Anmeldung an der Oberfläche wird in der Instanz protokolliert (Benutzername, IP-Adresse, Grund,

Zeitpunkt) und ist für den Auftraggeber einsehbar; ein Hinweisbanner ist während der Sitzung sichtbar.

- Systemzugriff des Auftragnehmers auf Dateien und Datenbank nur zu Betriebszwecken (Abschnitt 2.3).

1.4 TRENNUNGSKONTROLLE

- Je Kundeninstanz: eigene Datenbank mit eigener Datenbankrolle ohne Superuser-Rechte, eigener Dateispeicher, eigene Konfigurationsdatei, eigene Hintergrunddienste und eigener Sprachdienst auf eigenem Port; die Rolle einer Instanz hat keine Rechte an den Daten einer anderen Instanz. Die Trennung wird bei der Einrichtung jeder Instanz automatisch hergestellt und vom Auftragnehmer regelmäßig geprüft; konkrete Härtungsschritte auf Datenbankebene sind interne Maßnahmen des Auftragnehmers und keine gesondert zugesagten Einzelmaßnahmen.
- Innerhalb der Instanz: eigenes Datenbankschema je Sammlung; Zugriffsrechte je Sammlung über Gruppen.
- Kostenlose Demo-Umgebungen laufen in der Instanz des Auftragnehmers mit eigener Datenbank und eigenem Schema je Demo, getrennt von allen Kundeninstanzen; sie nutzen ausschließlich EU-Anbieter und werden nach sieben Tagen gelöscht.
- Der Server betreibt neben den Kundeninstanzen weitere Dienste des Auftragnehmers in getrennten Prozessen, Benutzern und Datenbanken. Kundeninstanzen sind durch eigene Datenbankrolle, Dateispeicher, Konfiguration und Dienste logisch getrennt. Lokale Test- und Entwicklungssysteme des Auftragnehmers werden ohne Auftragsdaten aus Kundeninstanzen betrieben. Ein ausschließlich für Kundeninstanzen reservierter Server ist keine zugesagte Mindestmaßnahme; eine spätere Trennung kann als zusätzliche Härtungsmaßnahme erfolgen, wenn Risiko, Auslastung oder Kundenanforderungen dies rechtfertigen.

1.5 PSEUDONYMISIERUNG UND DATENMINIMIERUNG

- IP-Adressen der Besucher werden im Chat-Protokoll nur als schlüsselbasierter Prüfwert (HMAC-SHA-256) gespeichert, dessen Schlüssel je Instanz getrennt in der Konfiguration liegt; angemeldete Besucher erscheinen nur als Pseudonym, das auf dieselbe Weise gebildet wird.
- Webserver-Protokolle mit IP-Adressen im Klartext werden nach 14 Tagen gelöscht und nicht mit Chat-Protokollen zusammengeführt.
- Hochgeladene Dateien der Besucher werden nur für die Dauer der Anfrage ausgewertet und nicht gespeichert; im Protokoll verbleiben Name, Typ und Größe.
- Sprachaufnahmen werden streamend an den gewählten Dienst übergeben und in der Instanz nicht gespeichert.
- Der Gesprächsverlauf liegt nur im Sitzungsspeicher des Browsers des Besuchers; das Chat-Widget setzt keine Cookies.
- Übergabe-E-Mails enthalten Kontaktdaten; das Protokoll der Instanz enthält davon nichts.
- Der an Sprachmodelle übergebene Gesprächsverlauf ist auf die letzten Gesprächszüge begrenzt.

1.6 VERSCHLÜSSELUNG

- Alle Verbindungen zur Instanz sind TLS-verschlüsselt (HTTPS, WSS); Zertifikate von Let's Encrypt mit automatischer Erneuerung. Sicherheits-Header des Webserver (HSTS, Content-Type-Schutz, Framing-Schutz, Referrer-Policy).

- Verbindungen der Instanz zu Sprachmodell-Anbietern, Datenquellen und Zielsystemen von Aktionen erfolgen über HTTPS; E-Mail-Versand über authentifizierte, verschlüsselte SMTP-Verbindung.
- Passwörter werden gehasht, Sitzungs- und Identitätstoken signiert (HMAC-SHA256).
- Konfigurationsdateien mit Geheimnissen sind nur für den Webserver-Benutzer lesbar (Dateimodus 640) und liegen außerhalb der Versionsverwaltung.
- Die Datenträger des Produktivservers werden vom Rechenzentrumsbetreiber (Anhang C) nach dessen zertifiziertem Sicherheitskonzept betrieben; eine Verschlüsselung der Datenträger im Ruhezustand ist nicht Bestandteil des gebuchten Servertarifs und wird nicht zugesagt. Der Schutz gespeicherter Daten beruht auf der Zugangs- und Zugriffskontrolle (Abschnitte 1.2 und 1.3), der physischen Sicherung des Rechenzentrums (Abschnitt 1.1) und den verschlüsselten Sicherungen. Sicherungsarchive werden vor der Übertragung mit einem asymmetrischen Verfahren (age, X25519) verschlüsselt; der private Schlüssel liegt ausschließlich außerhalb des Servers beim Auftragnehmer.

2. Integrität

2.1 WEITERGABEKONTROLLE

- Für produktiv öffentliche browserbasierte Einbindungen muss der Auftraggeber mindestens eine erlaubte Website/Origin hinterlegen. Browser-Aufrufe von Chat, Suche, Upload und Übergabe mit Origin-Header werden nur für freigegebene Websites zugelassen; eine leere Freigabeliste sperrt diese browserbasierte öffentliche Einbindung. Serverseitige Zugriffe sowie API-/MCP-Aufrufe ohne Origin-Header werden von der Origin-Liste nicht gesteuert und sind über die jeweils vorgesehenen Schnittstellen- und Aktivierungsmechanismen abzusichern.
- Übermittlungen an Sprachmodell-Anbieter enthalten nur die Frage, den Verlauf der Sitzung, die gefundenen Abschnitte und, falls vom Besucher oder Auftraggeber eingebracht, den Text eines Anhangs bzw. die Angaben einer Identität; die Verarbeitungsregion je Sammlung macht sichtbar, welche Dienste beteiligt sind.
- Exporte von Auftragsdaten werden nur an die benannten Ansprechpartner über einen gesicherten Kanal übergeben (verschlüsselter Download, kein unverschlüsselter E-Mail-Anhang).

2.2 EINGABEKONTROLLE (NACHVOLLZIEHBARKEIT)

- Anmeldungen des Anbieterkontos, Aufträge des Instanzsystems (Anlegen, Aktualisieren, Entfernen) und Löschungen werden mit Zeitpunkt, Handelnden und Protokoll festgehalten; Löschartokolle bleiben nach dem Entfernen einer Instanz erhalten.
- Aktionen aus dem Chat tragen Referenznummern; Agentenläufe werden mit Ergebnis protokolliert; Datenbankänderungen der Software werden je Instanz in einer Migrationstabelle verzeichnet.
- Der Programmcode ist versioniert; Änderungen werden als Releases mit Zeitstempel eingespielt und sind je Instanz nachvollziehbar.
- Änderungen der Konfiguration einer Sammlung (Anbieter, Funktionen, Fristen) werden mit Zeitpunkt und Benutzer protokolliert und sind für den Auftraggeber einsehbar (Weisungsdokumentation).

2.3 AUFTRAGSKONTROLLE

- Verarbeitung nur nach Hauptvertrag, Vereinbarung und Konfiguration des Auftraggebers; keine Nutzung von Auftragsdaten für andere Zwecke, kein Training von Modellen.
- Der Auftragnehmer greift auf Daten der Instanz nur für Betrieb, Störungsbeseitigung, Sicherheit, Datensicherung und auf Anforderung zu; Zugriffe auf die Oberfläche nur mit Freigabe (1.3).
- Subunternehmer nur nach Anhang C mit Vertrag nach Art. 28 DSGVO.
- Auftragsdaten werden nicht in KI-Werkzeuge des Auftragnehmers (Entwicklungs- oder Analyseassistenten) eingegeben.

3. Verfügbarkeit und Belastbarkeit

- **Datensicherung:** tägliche Sicherung von Datenbank, Dateispeicher und Konfiguration je Instanz mit den Fristen der Anlage 2; alle Generationen werden vor der Übertragung verschlüsselt und bei einem anderen Anbieter (Hetzner Online GmbH, Falkenstein, eigenes Konto) abgelegt; dort werden täglich serverseitige, vom Produktivserver aus nicht veränderbare Momentaufnahmen gehalten; der Zugang zum Konto des Sicherungsanbieters ist mit Zwei-Faktor-Anmeldung geschützt, die Übertragung erfolgt mit einem nur für die Sicherung bestimmten Unterkonto per SSH-Schlüssel; die Sicherungsläufe werden durch einen Totmannschalter überwacht.
- **Überwachung:** Prüfung der Erreichbarkeit, des Speicherplatzes und der Hintergrunddienste; die Hintergrundprozesse melden Lebenszeichen und sichern sich gegen Doppelstart ab.
- **Aktualisierungen:** Betriebssystem-Updates und Sicherheitsupdates werden regelmäßig eingespielt (dokumentierter Stand: Audit 04.07.2026); Software-Updates über das Release-Verfahren des Instanzsystems.
- **Schutz vor Überlastung:** Drosseln je Absender für Uploads, Übergabe und KI-Agenten-Endpunkt; Anmeldebremse; Begrenzung des an Sprachmodelle übergebenen Verlaufs; Kontingente je Paket.
- **Wiederherstellung:** Wiederherstellung einer Instanz aus Sicherung (Datenbank und Dateien) ist dokumentiert und wird mindestens halbjährlich getestet und protokolliert.
- **Ausfall des Inhabers:** Der Anbieter ist Einzelunternehmer und sagt keine personelle Vertretung zu. Die technischen Sicherungen, Exporte und Betriebsunterlagen sind so zu führen, dass eine geordnete Datenherausgabe im laufenden Betrieb möglich ist. Für einen dauerhaften persönlichen Ausfall besteht derzeit keine benannte Notfall-/Vertrauensperson; deshalb wird gegenüber Kunden keine Herausgabe oder Fortführung durch eine Ersatzperson zugesagt. RPO: höchstens 24 Stunden (tägliche Sicherung); Wiederherstellungsziel im normalen Betriebsfall: ein Arbeitstag, soweit technisch möglich.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- **Datenschutz-Management:** Verzeichnis der Verarbeitungstätigkeiten (Art. 30 Abs. 2 DSGVO); jährliche Überprüfung dieser Anlage; dokumentierte Löschkonzepte: Chat-Protokoll 90 Tage (täglicher Aufräumlauf), Webserver-Protokolle 14 Tage, Demo-Umgebungen 7 Tage, Instanzen nach der Nachlaufzeit des Hauptvertrags einschließlich Sicherungen.
- **Vorfallmanagement:** Meldung an den Auftraggeber innerhalb der in der Vereinbarung genannten Frist; Sicherung von Protokollen; Ursachenanalyse; Dokumentation.
- **Sicherheitsprüfungen:** Sicherheitsaudit des Servers (zuletzt 04.07.2026: Firewall, fail2ban, SSH-Härtung, Datenbankbindung, Geheimnisse, Sicherheits-Header, Betriebssystem-Updates);

automatisierte Tests des Programmcodes vor Releases; Prüfung sicherheitsrelevanter Änderungen im Code-Review.

- **Schlüsselverwaltung:** Rotation von Zugangsdaten bei Verdacht auf Kompromittierung und beim Ausscheiden von Personen; API-Schlüssel je Instanz getrennt.
- Datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO): Protokoll-Löschfrist 90 Tage; HMAC-basierter IP-Prüfwert mit Instanzgeheimnis; keine Cookies im Chat-Widget; transiente Uploads; Übergabe und Upload nur bei Aktivierung durch den Auftraggeber; KI-Agenten-Endpunkt standardmäßig aus; dokumentierte Verarbeitungsregion. Für produktive öffentliche browserbasierte Einbindungen ist eine Freigabeliste erlaubter Websites verpflichtend; eine leere Liste sperrt diese Browser-Einbindung. Serverseitige bzw. originlose API-/MCP-Aufrufe fallen nicht unter die Origin-Liste; ihr separater Zugangsschutz besteht aus Drossel je Quell-IP, IP-Liste je Sammlung, Aktivierungsschaltern und Token.

Anlage 4 — Auftragsblatt zum Vertrag „dAI Pro Managed“

Vorlage. Je Kunde ausfüllen; Angaben in eckigen Klammern ersetzen, nicht zutreffende Alternativen streichen. Das ausgefüllte Auftragsblatt wird von beiden Parteien unterzeichnet und ist Bestandteil des Vertrags (Vertrag § 1 Abs. 2 und § 15 Abs. 1 und 2). Die Auswahl zum Startkontingent muss mit Anlage 3 Anhang C übereinstimmen (Mistral AI SAS ist nur bei gewähltem Startkontingent Unterauftragsverarbeiter).

1. Parteien und Ansprechpartner

Angabe	Wert
Kunde	[Firma, Rechtsform, Anschrift, USt-IdNr.]
Vertretungsberechtigte Person des Kunden	[Name, Funktion]
Ansprechpartner Kunde, fachlich	[Name, E-Mail, Telefon]
Ansprechpartner Kunde, technisch	[Name, E-Mail, Telefon]
Stellvertretung	[Name, E-Mail, Telefon]
Weisungsberechtigte Personen (Anlage 3 § 5)	[Namen]
Ansprechpartner des Kunden für Datenschutzvorfälle (Anlage 3 § 3 Abs. 5)	[Name, E-Mail, Telefon]
Ansprechpartner Anbieter	Joachim Dreistein; Support: daipro@dreistein.de; Vertrags- und Datenschutzfragen: info@dreistein.de; Telefon +49 211 97 53 39 97; keine personelle Vertretung zugesagt

2. Instanz und Nutzung

Angabe	Wert
Instanzadresse	[kundenname].dreistein.de oder [eigene Domain]
Websites, Marken, Zielgruppen, für die die Instanz genutzt wird (Vertrag § 6 Abs. 7 lit. a)	[Liste]
Erlaubte Websites für die Einbindung (Freigabeliste, Vertrag § 6 Abs. 5)	[Liste der Origins, z. B. https://www.kunde.de]
Administratoren des Kunden (Benutzerkonten; Zwei-Faktor-Anmeldung verpflichtend)	[Namen, E-Mail-Adressen]
Anbieterkennzeichnung auf Anmeldeseite und Fernwartung	Firmenname: [Kunde]; Datenschutzhinweise für Nutzer der Instanz: [URL]

3. Paket und Vergütung

Angabe	Wert
Paket	[Grundpaket / Voller Funktionsumfang]
Staffel	[bis 6.000 / 6.001 bis 20.000 Datensätze]
Erlaubte Agenten (Grundpaket: vier nach Wahl)	[Liste der Typen]
Support-Funktionen (Eingang, Ticket-Assistent, Mensch-Übergabe)	[ja / nein]
Erlaubte Anzahl Datenquellen (Grundpaket: vier)	[Zahl]
Paketmaximum Datensätze / Karenzgrenze	[Paketmaximum] / [konkrete Karenzgrenze in Datensätzen]
Einrichtungspaket	[Einrichtung / mit Begleitung / mit umfassender Begleitung]
Monatliche Vergütung (netto)	[Betrag] €
Einmalige Vergütung Einrichtung (netto)	[Betrag] €
Stundensatz für Leistungen nach Aufwand (netto)	[Betrag] €
Abrechnung	vierteljährlich im Voraus
Fälligkeit der Einrichtungsvergütung	in voller Höhe mit Übergabe der Instanz (Vertrag § 3 Abs. 2); Rechnung nach der Übergabe
Zahlungsweise	[Rechnung per E-Mail, Überweisung / Rechnung per E-Mail, SEPA-Lastschrift (Mandat wird mit dem Vertrag erteilt)]
Vertragsbeginn	[Datum der Unterzeichnung / vereinbarter Vertragsbeginn]
Beginn Mindestlaufzeit / Mindestlaufzeit / Kündigungsfrist	[Übergabedatum; ersatzweise Beginn nach Vertrag § 10 Abs. 2] / 12 Monate / 3 Monate

Alle Beträge verstehen sich netto zuzüglich gesetzlicher Umsatzsteuer; das Angebot richtet sich ausschließlich an Unternehmer im Sinne des § 14 BGB, juristische Personen des öffentlichen Rechts und öffentlich-rechtliche Sondervermögen.

4. Sprachmodelle und Sprachdienste

Angabe	Wert
Sprachmodell-Anbieter (vom Kunden gewählt, eigener API-Schlüssel)	[Mistral AI / OpenAI / Anthropic / Google / OpenAI-kompatibler Endpunkt ...]
Verarbeitungsregion je Sammlung (Anlage 1 Abschnitt 5)	[EU / Deutschland / keine Vorgabe]

Angabe	Wert
Sprach-Chat	[nein / ja: Audio-Anbieter für Sprachausgabe und -erkennung: Mistral AI / OpenAI / Gladia (nur Spracherkennung; Anbieterbedingungen zu Unterauftragnehmern und Speicherdauer vom Kunden geprüft)]
Optionales Startkontingent Mistral über den Anbieter-Account (Vertrag § 4 Abs. 1)	[nein (Standard) / ja: einmalig bis 10,00 € Nutzungsgegenwert; danach eigener API-Schlüssel des Kunden] — bei „ja“ ist Mistral AI SAS nach Anlage 3 Anhang C Unterauftragsverarbeiter

5. Datenschutz und Inhalte

Angabe	Wert
Besondere Datenkategorien (Vertrag § 6 Abs. 2; Anlage 3 § 2 Abs. 3)	[nein / ja: Kategorien und vereinbarte Maßnahmen]
Berufsgeheimnis nach § 203 StGB (Anlage 3 Anhang E)	[nein / ja]
Hinweis im Upload-Dialog (Standardtext oder eigener Text je Sammlung)	[Standard / eigener Text: ...]
Chat-Protokoll: Löschfrist	[90 Tage (Standard) / ... Tage]
Rechtmäßig, aber besonders sensible Inhalte (Vertrag § 6 Abs. 7 lit. c)	[keine / Beschreibung]
Referenznennung (Vertrag § 14)	[ja / nein]

6. Betrieb

Angabe	Wert
E-Mail-Versand der Instanz	SMTP-Zugang des Kunden mit dessen Absenderadresse; der Kunde hinterlegt ihn in der Instanz unter Einstellungen → E-Mail-Versand und prüft ihn dort (Anlage 2 Abschnitt 6)
Datenschutzhinweise des Kunden für Nutzer der Instanz (Link)	[URL]
Fernwartungsfreigabe (Vertrag § 8)	wird vom Kunden in der Instanz erteilt: [1 Tag / 7 Tage / 30 Tage / bis auf Widerruf]
Anbindungen an Drittsysteme des Kunden (Ticketsystem, Postfach, Webhooks)	[keine / Liste mit Verantwortlichem beim Kunden]

7. Unterschriften

Mit ihrer Unterschrift schließen die Parteien den Vertrag „dAI Pro Managed“ einschließlich der Anlagen 1 bis 5 und die Vereinbarung zur Auftragsverarbeitung (Anlage 3) mit ihren Anhängen. Eine gesonderte Unterzeichnung des Vertrags und der Anlage 3 ist nicht erforderlich.

Anbieter	Kunde
Ort, Datum: _____	Ort, Datum: _____
Joachim Dreistein Medienentwicklung	[Kunde, vertretungsberechtigte Person]