Vertrag über Auftragsverarbeitung (AVV)

Data Processing Agreement (DPA)

gemäß / pursuant to Art. 28 DSGVO / GDPR

Stand / Version: *2026-10.11 ·* ***Status:*** *Bei Abweichungen zwischen den Sprachfassungen ist die deutsche Fassung maßgeblich. · In case of discrepancy between the language versions, the German version prevails.*

Vertragsparteien · Parties

DEUTSCH	ENGLISH
zwischen	**between**
Verantwortlicher – nachfolgend „Verantwortlicher“ –	Controller – hereinafter the “Controller” –
[Company name], [Company address]	**[Company name], [Company address]**
und	**and**
Auftragsverarbeiter – nachfolgend „Auftragsverarbeiter“ –	Processor – hereinafter the “Processor” –
HybridAI GmbH, Im Mediapark 5, 50670 Köln, Deutschland E-Mail (Datenschutz): privacy@hybridai.one	HybridAI GmbH, Im Mediapark 5, 50670 Cologne, Germany Email (data protection): privacy@hybridai.one

Gewählte Betriebsvariante · Selected operating variant

DEUTSCH	ENGLISH
Der Verantwortliche wählt für diese Verarbeitung eine der folgenden Betriebsvarianten. Die Auswahl bestimmt Datenflüsse und ergänzende Klauseln; nicht gewählte Varianten und die darauf bezogenen Regelungen (insb. § 7 sowie die Drittland-Einträge in Anlage 2) ruhen.	The Controller selects one of the following operating variants for this processing. The selection governs data flows and supplementary clauses; unselected variants and their related provisions (in particular § 7 and the third-country entries in Annex 2) remain dormant.
[ ] **Variante A – Lokaler Betrieb (On-Premise).** Betrieb des Modells auf Infrastruktur des Verantwortlichen; kein externer LLM-Dienst, keine Drittlandübermittlung.	[ ] **Variant A – Local operation (on-premise).** Model runs on the Controller’s infrastructure; no external LLM service, no third-country transfer.
[ ] **Variante B – EU-Stack.** Verarbeitung ausschließlich in EU/EWR (self-hosted bei HybridAI und/oder EU-Cloud-LLM, z. B. Mistral); keine Drittlandübermittlung.	[ ] **Variant B – EU stack.** Processing exclusively in the EU/EEA (self-hosted at HybridAI and/or EU cloud LLM, e.g. Mistral); no third-country transfer.
[X] Variante C – EU-Stack mit US-Modellen. Zusätzlich freigegeben sind LLM-Dienste mit Drittlandbezug (OpenAI, Anthropic); § 7, die Drittland-Einträge in Anlage 2 und die PII-Maskierung (§ 4 Abs. 2) greifen.	**[X] Variant C – EU stack with US models. Additionally enabled: LLM services involving a third country (OpenAI, Anthropic); § 7, the third-country entries in Annex 2 and PII masking (§ 4(2)) apply.**
In allen Varianten erbringt HybridAI die Leistung als „managed service“ – auch bei Betrieb in der IT des Verantwortlichen –; es liegt durchgehend Auftragsverarbeitung nach Art. 28 DSGVO vor.	*In all variants HybridAI provides the service as a managed service – including where it runs within the Controller’s IT – and processing on behalf under Art. 28 GDPR applies throughout.*

Optionale Zusatzvereinbarung: Verschwiegenheit nach § 203 StGB · Optional supplementary agreement: professional secrecy (Sec. 203 StGB)

DEUTSCH	ENGLISH
Für Verantwortliche, die Berufsgeheimnisträger im Sinne des § 203 Abs. 1 StGB sind (z. B. Heilberufe, Rechtsanwälte, Steuerberater, Wirtschaftsprüfer), kann ergänzend die Verpflichtung zur Verschwiegenheit gemäß § 203 StGB als **Anlage 4** vereinbart werden. [ ] **Vereinbart.** Anlage 4 ist Bestandteil dieses Vertrags. **[X] Nicht vereinbart. Anlage 4 ist nicht Bestandteil dieses Vertrags und in diesem Dokument nicht enthalten.** *Diese Zusatzvereinbarung ist optional und wird im Regelfall nicht getroffen; sie ist nur einschlägig, wenn geschützte Geheimnisse im Sinne des § 203 StGB verarbeitet werden.*	Controllers who are professionals bound to secrecy within the meaning of Sec. 203(1) of the German Criminal Code (StGB) (e.g. healthcare professions, attorneys-at-law, tax advisors, auditors) may additionally agree the confidentiality obligation pursuant to Sec. 203 StGB as **Annex 4**. [ ] **Agreed.** Annex 4 forms part of this Agreement. **[X] Not agreed. Annex 4 does not form part of this Agreement and is not included in this document.** *This supplementary agreement is optional and not concluded in the normal case; it is relevant only where protected secrets within the meaning of Sec. 203 StGB are processed.*

§ 1 Gegenstand, Art, Zweck und Dauer · § 1 Subject matter, nature, purpose and duration

DEUTSCH	ENGLISH
(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Gegenstand, Art und Zweck der Verarbeitung, die Kategorien personenbezogener Daten sowie die Kategorien betroffener Personen ergeben sich abschließend aus **Anlage 1**.	**(1)** The Processor processes personal data on behalf of the Controller. The subject matter, nature and purpose of the processing, the categories of personal data and the categories of data subjects are set out conclusively in **Annex 1**.
(2) Dieser Vertrag gilt für sämtliche Verarbeitungstätigkeiten, die der Auftragsverarbeiter für den Verantwortlichen im Zusammenhang mit seiner KI-Chatbot- bzw. LLM-Vermittlungsplattform erbringt.	**(2)** This Agreement applies to all processing activities the Processor performs for the Controller in connection with its AI chatbot / LLM mediation platform.
(3) Die Laufzeit dieses Vertrags entspricht der Laufzeit des zugrunde liegenden Hauptvertrags, unbeschadet fortbestehender Pflichten aus § 10 und § 3.	**(3)** The term of this Agreement corresponds to the term of the underlying main contract, without prejudice to surviving obligations under § 10 and § 3.
(4) Hauptvertrag im Sinne dieses Vertrages sind die Allgemeinen Geschäftsbedingungen der HybridAI GmbH nebst der jeweiligen Bestellung in ihrer bei Vertragsschluss geltenden Fassung.	**(4)** The main contract within the meaning of this Agreement consists of the General Terms and Conditions of HybridAI GmbH together with the respective order, in the version applicable at the time of conclusion of the contract.

§ 2 Weisungsrecht des Verantwortlichen · § 2 Controller's right to issue instructions

DEUTSCH	ENGLISH
(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich für die in Anlage 1 festgelegten Zwecke und nur auf Grundlage dokumentierter Weisungen des Verantwortlichen, einschließlich hinsichtlich Drittlandübermittlungen, es sei denn, er ist nach Unions- oder mitgliedstaatlichem Recht dazu verpflichtet. In diesem Fall teilt er dem Verantwortlichen diese Anforderung vor der Verarbeitung mit, sofern das Recht dies nicht aus wichtigem öffentlichem Interesse verbietet.	**(1)** The Processor processes personal data solely for the purposes set out in Annex 1 and only on documented instructions from the Controller, including regarding third-country transfers, unless required to do so by Union or Member State law. In such a case it informs the Controller of that requirement before processing, unless the law prohibits this on important grounds of public interest.
(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen verstößt.	**(2)** The Processor informs the Controller without undue delay if, in its opinion, an instruction infringes the GDPR or other data protection provisions.
(3) Eine Verarbeitung der überlassenen Daten für eigene Zwecke oder Zwecke Dritter ist unzulässig.	**(3)** Processing of the entrusted data for the Processor's own purposes or those of third parties is prohibited.

DEUTSCH	ENGLISH
(4) Keine Nutzung zu Trainings-/Fine-Tuning-Zwecken. Der Auftragsverarbeiter verwendet die im Auftrag verarbeiteten personenbezogenen Daten des Verantwortlichen **nicht** zum Training, zur Weiterentwicklung oder zum Fine-Tuning eigener oder fremder allgemeiner KI-/Sprachmodelle (Foundation Models). Er stellt vertraglich und technisch sicher, dass auch die in Anlage 2 genannten Unterauftragsverarbeiter (insbesondere LLM-Anbieter) die Daten nicht zu solchen Zwecken verwenden.	**(4) No use for training / fine-tuning.** The Processor shall **not** use the Controller's personal data processed on its behalf to train, further develop or fine-tune its own or third parties' general AI/language models (foundation models). It ensures by contractual and technical means that the sub-processors listed in Annex 2 (in particular LLM providers) likewise do not use the data for such purposes.

§ 3 Vertraulichkeit · § 3 Confidentiality

DEUTSCH	ENGLISH
(1) Der Auftragsverarbeiter gewährleistet, dass sich alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Vertragsende fort.	**(1)** The Processor ensures that all persons authorised to process the data have committed to confidentiality or are under an appropriate statutory confidentiality obligation. This obligation continues after termination.
(2) Der Zugang des Personals zu den Daten erfolgt nur, soweit dies zur Vertragserfüllung erforderlich ist (Need-to-know-Prinzip).	**(2)** Personnel are granted access to the data only to the extent necessary to perform this Agreement (need-to-know principle).
(3) Der Auftragsverarbeiter gestaltet seine innerbetriebliche Organisation datenschutzgerecht und weist die zugriffsberechtigten Personen entsprechend ein.	**(3)** The Processor organises its internal operations in a data-protection-compliant manner and instructs the authorised persons accordingly.

§ 4 Technische und organisatorische Maßnahmen · § 4 Technical and organisational measures

DEUTSCH	ENGLISH
(1) Der Auftragsverarbeiter trifft mindestens die in **Anlage 3** beschriebenen Maßnahmen nach Art. 32 DSGVO mit einem dem Risiko angemessenen Schutzniveau.	**(1)** The Processor implements at least the measures described in **Annex 3** pursuant to Art. 32 GDPR, at a level of security appropriate to the risk.
(2) Pseudonymisierung / PII-Maskierung. Der Auftragsverarbeiter stellt eine Funktion zur Maskierung/Pseudonymisierung personenbezogener Daten vor der Weiterleitung an externe KI-/LLM-Dienste bereit. Ist diese gemäß Anlage 1 aktiviert, werden identifizierende Daten vor der Weiterleitung nach dem in Anlage 3 beschriebenen Verfahren maskiert; dies gilt zugleich als ergänzende Schutzmaßnahme im Sinne von § 7.	**(2) Pseudonymisation / PII masking.** The Processor provides a function to mask/pseudonymise personal data before forwarding it to external AI/LLM services. Where activated in accordance with Annex 1, identifying data is masked before forwarding pursuant to the procedure in Annex 3; this also constitutes a supplementary safeguard within the meaning of § 7.
(3) Die Maßnahmen unterliegen dem technischen Fortschritt und dürfen fortentwickelt oder gleichwertig ersetzt werden; das Schutzniveau darf nicht unterschritten werden. Wesentliche Änderungen werden unaufgefordert mitgeteilt.	**(3)** The measures are subject to technical progress and may be further developed or replaced by equivalent ones; the level of protection must not be reduced. Material changes are communicated without being requested.

§ 5 Unterstützungspflichten · § 5 Obligations to assist

DEUTSCH	ENGLISH
Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen insbesondere bei: • Beantwortung von Anträgen betroffener Personen (Art. 12–23 DSGVO); er informiert unverzüglich über an ihn gerichtete Anträge; • Gewährleistung der Sicherheit der Verarbeitung (Art. 32 DSGVO); • Meldung und Benachrichtigung von Datenschutzverletzungen (Art. 33, 34 DSGVO; siehe § 9); • Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO); • etwaiger vorheriger Konsultation der Aufsichtsbehörde (Art. 36 DSGVO); • Wahrung der Richtigkeit und Aktualität der Daten. **Reaktionsfrist und Umfang:** Der Auftragsverarbeiter antwortet auf Anforderungen des Verantwortlichen innerhalb von **fünf (5) Arbeitstagen**. Der Umfang der Unterstützung erstreckt sich auf: • Chatverläufe und Logs (maximal 90 Tage, dann automatisch gelöscht) • Datei-Uploads (maximal 90 Tage, dann automatisch gelöscht) • Sicherungskopien (bei Beendigung gelöscht, mit Nachweis in Textform) • Technische und organisatorische Informationen zur Datenspeicherung und -löschung	Taking into account the nature of processing and the information available to it, the Processor assists the Controller in particular with: • responding to data subject requests (Art. 12–23 GDPR); informing without undue delay of requests addressed to it; • ensuring the security of processing (Art. 32 GDPR); • notifying and communicating personal data breaches (Art. 33, 34 GDPR; see § 9); • carrying out a data protection impact assessment (Art. 35 GDPR); • any prior consultation of the supervisory authority (Art. 36 GDPR); • keeping the data accurate and up to date. **Response time and scope:** The Processor responds to requests from the Controller within **five (5) business days**. The scope of assistance covers: • Chat histories and logs (maximum 90 days, then automatically deleted) • File uploads (maximum 90 days, then automatically deleted) • Backup copies (deleted upon termination, with written confirmation) • Technical and organisational information on data storage and deletion

§ 6 Unterauftragsverarbeiter · § 6 Sub-processors

DEUTSCH	ENGLISH
(1) Allgemeine Genehmigung. Der Verantwortliche erteilt die allgemeine Genehmigung zur Beauftragung der in **Anlage 2** aufgeführten Unterauftragsverarbeiter.	**(1) General authorisation.** The Controller grants general authorisation to engage the sub-processors listed in **Annex 2**.
(2) Änderungen. Beabsichtigt der Auftragsverarbeiter, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden auszutauschen, informiert er den Verantwortlichen **mindestens vier (4) Wochen** vorab in Textform unter Angabe von Name, Standort, Verarbeitungsstandort, Zweck und Schutzgarantien.	**(2) Changes.** If the Processor intends to engage an additional sub-processor or replace an existing one, it informs the Controller **at least four (4) weeks** in advance in text form, stating name, location, processing location, purpose and safeguards.
(3) Widerspruchsrecht. Der Verantwortliche kann der Änderung **innerhalb von zwei (2) Wochen** ab Zugang aus wichtigem datenschutzrechtlichem Grund widersprechen. Ohne fristgerechten Widerspruch gilt die Änderung als genehmigt. Bei berechtigtem Widerspruch suchen die Parteien eine einvernehmliche Lösung; andernfalls steht dem Verantwortlichen ein außerordentliches Kündigungsrecht bezüglich der betroffenen Leistung zu.	**(3) Right to object.** The Controller may object to the change **within two (2) weeks** of receipt on important data protection grounds. Absent a timely objection, the change is deemed approved. On a justified objection the parties seek an amicable solution; failing this, the Controller may extraordinarily terminate the affected service.
(4) Weitergabe der Pflichten. Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter durch schriftlichen (auch elektronischen) Vertrag zu denselben Pflichten wie in diesem Vertrag und haftet dem Verantwortlichen vorbehaltlich § 12 für deren Einhaltung; eine Kopie wird auf Verlangen bereitgestellt.	**(4) Flow-down of obligations.** The Processor imposes on each sub-processor, by written (including electronic) contract, the same obligations as in this Agreement and remains liable to the Controller for their compliance, subject to § 12; a copy is provided on request.

DEUTSCH	ENGLISH
(5) Umfasst eine Unterbeauftragung eine Drittlandübermittlung, gilt § 7 entsprechend.	**(5)** Where a sub-processing involves a third-country transfer, § 7 applies accordingly.
(6) Bestehende Verträge. Mit jedem in Anlage 2 genannten Unterauftragsverarbeiter besteht eine Auftragsverarbeitungsvereinbarung – gesondert abgeschlossen oder als Bestandteil der Standardvertragsbedingungen des Anbieters – einschließlich Standardvertragsklauseln, soweit eine Drittlandübermittlung erfolgt. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Verlangen eine Kopie bzw. den Fundstellennachweis zur Verfügung.	**(6) Existing agreements.** A data processing agreement is in place with each sub-processor listed in Annex 2 – concluded separately or as part of the provider's standard terms – including Standard Contractual Clauses where a third-country transfer occurs. The Processor provides the Controller with a copy or reference on request.

§ 7 Verarbeitung in Drittländern · § 7 Processing in third countries

DEUTSCH	ENGLISH
(1) Anwendungsbereich. Dieser Paragraph gilt nur, soweit gemäß der gewählten Betriebsvariante (Variante C) LLM-Dienste mit Drittlandbezug genutzt werden. In den Varianten A und B findet keine Drittlandübermittlung statt; dieser Paragraph ruht insoweit.	**(1) Scope.** This section applies only where, under the selected operating variant (Variant C), LLM services involving a third country are used. Under Variants A and B no third-country transfer occurs and this section remains dormant.
(2) Die Verarbeitung findet grundsätzlich in Deutschland, der EU oder im EWR statt. Eine Verarbeitung in einem Drittland erfolgt nur, wenn die Art. 44 ff. DSGVO erfüllt sind.	**(2)** Processing takes place in principle in Germany, the EU or the EEA. Processing in a third country occurs only if Art. 44 et seq. GDPR are met.
(3) Die betreffenden Unterauftragsverarbeiter, das Drittland, die Rechtsgrundlage und die eingesetzten Regionen/Datenstandorte sind in **Anlage 2** konkret ausgewiesen.	**(3)** The relevant sub-processors, the third country, the legal basis and the regions/data locations used are set out specifically in **Annex 2**.
(4) Fehlt ein Angemessenheitsbeschluss (Art. 45 DSGVO), stützt der Auftragsverarbeiter Übermittlungen auf die Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914, in der Regel Modul 3 (Verarbeiter-zu-Verarbeiter), und führt vor der Übermittlung ein Transfer Impact Assessment (TIA) durch, das auf Anforderung bereitgestellt wird. Ist ein Anbieter unter dem EU-US Data Privacy Framework zertifiziert, kann die Übermittlung nachrangig auch auf den Angemessenheitsbeschluss (EU) 2023/1795 gestützt werden.	**(4)** Absent an adequacy decision (Art. 45 GDPR), the Processor bases transfers on the Standard Contractual Clauses under Implementing Decision (EU) 2021/914, generally Module 3 (processor-to-processor), and carries out a Transfer Impact Assessment (TIA) before the transfer, made available on request. Where a provider is certified under the EU-US Data Privacy Framework, the transfer may additionally rely, on a subsidiary basis, on adequacy decision (EU) 2023/1795.
(5) Ergänzende Maßnahmen. Ist die PII-Maskierung gemäß Anlage 1 aktiviert, setzt der Auftragsverarbeiter diese als ergänzende technische Maßnahme (EDSA-Empfehlungen) ein, sodass identifizierende Daten vor einer etwaigen Drittlandübermittlung maskiert werden. Ist sie deaktiviert, werden personenbezogene Daten unmaskiert an die betreffenden Dienste übermittelt; der Auftragsverarbeiter weist hierauf hin, und die Entscheidung hierüber erfolgt als dokumentierte Weisung des Verantwortlichen nach § 2, der die datenschutzrechtliche Verantwortung hierfür trägt.	**(5) Supplementary measures.** Where PII masking is activated in accordance with Annex 1, the Processor uses it as a supplementary technical measure (EDPB recommendations) so that identifying data is masked before any third-country transfer. Where it is deactivated, personal data is transferred to the relevant services unmasked; the Processor points this out, and the decision is made as a documented instruction of the Controller under § 2, who bears the data protection responsibility for it.

§ 8 Kontrollrechte des Verantwortlichen · § 8 Controller's audit rights

DEUTSCH	ENGLISH
(1) Der Auftragsverarbeiter stellt alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO und diesem Vertrag erforderlich sind.	**(1)** The Processor makes available all information necessary to demonstrate compliance with the obligations under Art. 28 GDPR and this Agreement.

DEUTSCH	ENGLISH
(2) Er ermöglicht und trägt zu Überprüfungen – einschließlich Inspektionen – bei, die der Verantwortliche oder ein von ihm beauftragter unabhängiger Prüfer in angemessenen Abständen oder bei Anzeichen für Nichteinhaltung durchführt, mit angemessener Vorankündigung, unter Wahrung der Geschäftsgeheimnisse und möglichst ohne Betriebsstörung.	**(2)** It allows for and contributes to audits – including inspections – conducted by the Controller or an independent auditor it mandates, at reasonable intervals or on indications of non-compliance, with reasonable notice, respecting trade secrets and, where possible, without disrupting operations.
(3) Bei Art und Umfang einer Prüfung kann der Verantwortliche einschlägige Zertifizierungen/Testate (z. B. Art. 28 Abs. 5 DSGVO) berücksichtigen; der Auftragsverarbeiter kann geeignete Nachweise (z. B. aktuelle Prüfberichte) vorlegen.	**(3)** In deciding the nature and scope of an audit, the Controller may consider relevant certifications/attestations (e.g. Art. 28(5) GDPR); the Processor may submit suitable evidence (e.g. current audit reports).

§ 9 Meldung von Datenschutzverletzungen · § 9 Notification of personal data breaches

DEUTSCH	ENGLISH
(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, über jede Verletzung des Schutzes seiner personenbezogenen Daten.	**(1)** The Processor informs the Controller without undue delay, and no later than 24 hours after becoming aware, of any breach of the protection of its personal data.
(2) Die Meldung enthält mindestens: • Beschreibung der Art der Verletzung, soweit möglich mit Kategorien und ungefährer Zahl betroffener Personen und Datensätze; • Name und Kontaktdaten einer Anlaufstelle; • Beschreibung der wahrscheinlichen Folgen; • Beschreibung der ergriffenen/vorgeschlagenen Abhilfe- und Abmilderungsmaßnahmen.	**(2)** The notification contains at least: • a description of the nature of the breach, where possible with categories and approximate number of data subjects and records; • the name and contact details of a point of contact; • a description of the likely consequences; • a description of the measures taken/proposed to address and mitigate it.
(3) Er unterrichtet den Verantwortlichen ebenfalls, wenn getroffene Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.	**(3)** It also informs the Controller if the security measures taken do not meet the legal requirements.

§ 10 Löschung und Rückgabe · § 10 Deletion and return

DEUTSCH	ENGLISH
(1) Nach Beendigung der Verarbeitung löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück und löscht bestehende Kopien, einschließlich Sicherungskopien, sofern keine Speicherpflicht nach Unions-/mitgliedstaatlichem Recht besteht.	**(1)** Upon termination of processing, the Processor, at the Controller's choice, deletes all personal data or returns it and deletes existing copies, including backups, unless storage is required under Union/Member State law.
(2) Gesetzliche Aufbewahrungspflichten. Stehen solche einer Löschung entgegen, schränkt der Auftragsverarbeiter die Verarbeitung auf den gesetzlichen Zweck ein und löscht nach Ablauf der Frist.	**(2) Statutory retention.** Where such obligations prevent deletion, the Processor restricts processing to the statutory purpose and deletes after the period expires.
(3) Nachweis. Die Löschung wird dem Verantwortlichen in Textform angezeigt und auf Verlangen nachgewiesen.	**(3) Proof.** The deletion is notified to the Controller in text form and demonstrated on request.

§ 11 Datenschutzbeauftragter / Ansprechpartner · § 11 Data protection officer / contact

DEUTSCH	ENGLISH
(1) Soweit gesetzlich vorgeschrieben, hat der Auftragsverarbeiter einen Datenschutzbeauftragten benannt. Name und Kontaktdaten des Datenschutzbeauftragten bzw. – sofern keine Benennungspflicht besteht – des zuständigen Ansprechpartners ergeben sich aus Anlage 1.	**(1)** Where legally required, the Processor has appointed a data protection officer. The name and contact details of the DPO or – where no appointment obligation applies – of the responsible contact are set out in Annex 1.
(2) Ein Wechsel wird dem Verantwortlichen unverzüglich mitgeteilt.	**(2)** A change is communicated to the Controller without undue delay.

§ 12 Haftung und Freistellung · § 12 Liability and indemnification

DEUTSCH	ENGLISH
(1) Der Auftragsverarbeiter haftet dem Verantwortlichen nach den gesetzlichen Vorschriften für Schäden, die auf einer schuldhaften Verletzung dieser Vereinbarung, einer auf ihn als Auftragsverarbeiter anwendbaren datenschutzrechtlichen Verpflichtung oder einer rechtmäßigen Weisung des Verantwortlichen beruhen.	**(1)** The Processor shall be liable to the Controller in accordance with statutory provisions for damages arising from a culpable breach of this Agreement, of a data protection obligation applicable to it as Processor, or of a lawful instruction of the Controller.
(2) Der Auftragsverarbeiter stellt den Verantwortlichen von berechtigten Ansprüchen Dritter, insbesondere von Schadensersatzansprüchen betroffener Personen nach Art. 82 DSGVO, einschließlich der erforderlichen und angemessenen Kosten der Rechtsverteidigung frei, soweit diese auf einer vom Auftragsverarbeiter oder einem von ihm eingesetzten Unterauftragsverarbeiter zu vertretenden Pflichtverletzung im Sinne von Abs. 1 beruhen. Art. 82 Abs. 5 DSGVO bleibt unberührt.	**(2)** The Processor shall indemnify the Controller against justified third-party claims, in particular claims for damages by data subjects under Art. 82 GDPR, including the necessary and reasonable costs of legal defence, to the extent that such claims are based on a breach of duty within the meaning of para. 1 for which the Processor or a sub-processor engaged by it is responsible. Art. 82(5) GDPR remains unaffected.
(3) Voraussetzung der Freistellung nach Abs. 2 ist, dass der Verantwortliche den Auftragsverarbeiter unverzüglich, spätestens innerhalb von zehn Werktagen nach Kenntnis, in Textform über den geltend gemachten Anspruch unterrichtet, ihm alle zur Beurteilung und Abwehr erforderlichen Informationen und Unterlagen zur Verfügung stellt, ihm die Führung der außergerichtlichen und gerichtlichen Auseinandersetzung überlässt und ohne vorherige Zustimmung des Auftragsverarbeiters weder ein Anerkenntnis abgibt noch einen Vergleich schließt. Die Zustimmung darf nicht unbillig verweigert werden. Eine Verletzung dieser Mitwirkungsobliegenheiten lässt den Freistellungsanspruch unberührt, soweit und solange dem Auftragsverarbeiter hierdurch kein Nachteil bei der Rechtsverteidigung entsteht. Ein solcher Nachteil wird vermutet, wenn der Verantwortliche ohne Zustimmung des Auftragsverarbeiters ein Anerkenntnis abgegeben oder einen Vergleich geschlossen hat oder wenn der Haftpflichtversicherer des Auftragsverarbeiters seine Leistung deshalb ganz oder teilweise verweigert.	**(3)** The indemnification under para. 2 is conditional upon the Controller notifying the Processor without undue delay, and no later than ten (10) business days after becoming aware, in text form of the claim asserted, providing all information and documents required to assess and defend the claim, leaving to the Processor the conduct of the out-of-court and court proceedings, and neither making any admission nor entering into any settlement without the Processor's prior consent. Such consent shall not be unreasonably withheld. A breach of these duties to cooperate shall not affect the indemnification claim to the extent and for as long as no detriment to the Processor's legal defence arises as a result. Such detriment shall be presumed where the Controller has made an admission or entered into a settlement without the Processor's consent, or where the Processor's liability insurer refuses performance in whole or in part on that ground.
(4) Von der Freistellung nach Abs. 2 nicht erfasst sind Geldbußen und sonstige Sanktionen, die gegen den Verantwortlichen nach Art. 83 DSGVO oder § 41 BDSG verhängt werden, sowie der reguläre Aufwand des Verantwortlichen für die Erfüllung von Betroffenenrechten nach Art. 15 bis 22 DSGVO. Dies gilt nicht für erforderliche und angemessene zusätzliche Aufwendungen, die aufgrund einer vom Auftragsverarbeiter oder einem Unterauftragsverarbeiter zu vertretenden Pflichtverletzung entstehen.	**(4)** The indemnification under para. 2 does not extend to administrative fines and other sanctions imposed on the Controller under Art. 83 GDPR or Sec. 41 BDSG, nor to the Controller's regular expenditure for fulfilling data subject rights under Art. 15 to 22 GDPR. This does not apply to necessary and reasonable additional expenditure incurred as a result of a breach of duty for which the Processor or a sub-processor is responsible.

DEUTSCH	ENGLISH
(5) Ungeachtet entgegenstehender Bestimmungen dieser Vereinbarung ist die Haftung des Auftragsverarbeiters für Ansprüche im Zusammenhang mit der Verarbeitung personenbezogener Daten nach dieser Vereinbarung, einschließlich der Freistellung nach Abs. 2, auf 500.000 EUR je Schadensfall und insgesamt 1.000.000 EUR je Kalenderjahr begrenzt. Mehrere Schadensfälle, die auf derselben Ursache oder auf mehreren Ursachen gleicher Art mit innerem Zusammenhang beruhen, gelten als ein Schadensfall. Die Begrenzung gilt nicht bei Vorsatz und grober Fahrlässigkeit, bei der Verletzung von Leben, Körper oder Gesundheit sowie in sonstigen Fällen zwingender gesetzlicher Haftung. Bei der schuldhaften Verletzung wesentlicher Vertragspflichten ist die Haftung auf den vertragstypischen vorhersehbaren Schaden begrenzt; die Parteien gehen übereinstimmend davon aus, dass dieser die vorstehenden Beträge nicht übersteigt. Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.	**(5)** Notwithstanding any provision of this Agreement to the contrary, the Processor's liability for claims in connection with the processing of personal data under this Agreement, including the indemnification under para. 2, is limited to EUR 500,000 per damage event and EUR 1,000,000 in aggregate per calendar year. Several damage events based on the same cause, or on several causes of the same kind with an internal connection, shall be deemed one damage event. The limitation does not apply in cases of intent or gross negligence, injury to life, body or health, or in other cases of mandatory statutory liability. In the event of a culpable breach of essential contractual duties, liability is limited to the foreseeable damage typical for this type of contract; the parties agree that such damage does not exceed the amounts stated above. Liability towards data subjects under Art. 82 GDPR remains unaffected.
(6) Die Haftungshöchstbeträge nach Abs. 5 und nach Ziffer 8.3 der Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters gelten nicht kumulativ; die Gesamthaftung des Auftragsverarbeiters ist je Kalenderjahr auf 1.000.000 EUR begrenzt. Abs. 5 Satz 3 bleibt unberührt.	**(6)** The liability caps under para. 5 and under Section 8.3 of the Processor's General Terms and Conditions do not apply cumulatively; the Processor's total liability is limited to EUR 1,000,000 per calendar year. Para. 5 sentence 3 remains unaffected.
(7) Der Auftragsverarbeiter unterhält während der Laufzeit dieser Vereinbarung eine Betriebs- und Berufshaftpflichtversicherung mit einer Deckungssumme für Vermögensschäden von mindestens der in Abs. 5 genannten Höhe je Schadensfall, welche die gesetzliche Haftpflicht aus der Verletzung datenschutzrechtlicher Vorschriften umfasst, und weist deren Bestehen dem Verantwortlichen auf Verlangen einmal jährlich nach.	**(7)** For the term of this Agreement the Processor maintains commercial general and professional liability insurance with a sum insured for pure financial loss of at least the amount stated in para. 5 per damage event, covering statutory liability arising from breaches of data protection law, and shall evidence its existence to the Controller once a year on request.

§ 13 Schlussbestimmungen · § 13 Final provisions

DEUTSCH	ENGLISH
(1) Änderungen und Nebenabreden bedürfen der Schriftform; die elektronische Form (z. B. E-Mail, elektronische Signatur) genügt.	**(1)** Amendments and side agreements require written form; electronic form (e.g. email, electronic signature) suffices.
(2) Bei Widersprüchen gehen die Regelungen dieses Vertrags vor.	**(2)** In the event of conflicts, the provisions of this Agreement prevail.
(3) Die Unwirksamkeit einzelner Bestimmungen berührt die Wirksamkeit der übrigen nicht.	**(3)** The invalidity of individual provisions does not affect the validity of the remainder.
(4) Es gilt deutsches Recht. Gerichtsstand ist Köln, soweit zulässig.	**(4)** German law applies. Place of jurisdiction is Cologne, to the extent permissible.

Elektronischer Vertragsschluss · Electronic execution

Verantwortlicher / Controller
[Company name]
[Company address]

Elektronisch angenommen durch / electronically accepted by:
[Signatory name] ([Signatory email])
[Signature date and time]

Auftragsverarbeiter / Processor
HybridAI GmbH
Im Mediapark 5, 50670 Köln, Deutschland

Dieses Angebot ist durch den Auftragsverarbeiter elektronisch gezeichnet und wird mit der Annahme durch den Verantwortlichen wirksam. / This offer is electronically executed by the Processor and takes effect upon acceptance by the Controller.
Köln, [Signature date and time]

Dieser Vertrag wurde elektronisch geschlossen und ist ohne handschriftliche Unterschrift gültig (§ 13 Abs. 1; Art. 28 Abs. 9 DSGVO – elektronisches Format). / This Agreement was concluded electronically and is valid without handwritten signature (§ 13(1); Art. 28(9) GDPR – electronic format).
Vorlagenversion / Template version: 2026-10.11 · Abschluss-Nr. / Acceptance ID: [Document ID (auto-generated)] · IP: [IP address]

Anlage 1 – Beschreibung der Verarbeitung · Annex 1 – Description of processing

DEUTSCH	ENGLISH
Gegenstand Bereitstellung und Betrieb einer KI-Chatbot- bzw. LLM-Vermittlungsplattform als datenschutzorientierte Vermittlungsschicht zwischen dem Verantwortlichen und KI-Modellen (z. B. GPT, Gemini, Mistral, Claude), inkl. Nachrichtenverarbeitung, Function Calling und Integration mit Drittsystemen.	**Subject matter** Provision and operation of an AI chatbot / LLM mediation platform as a data-protection-oriented layer between the Controller and AI models (e.g. GPT, Gemini, Mistral, Claude), incl. message handling, function calling and integration with third-party systems.
Art & Zweck • Entgegennahme, Analyse und Beantwortung von Nutzereingaben durch KI-/LLM-Dienste; • Pseudonymisierung/PII-Maskierung vor Weiterleitung, ggf. Ent-Pseudonymisierung der Rückgaben; • Protokollierung/Speicherung von Chatverläufen und Logs zur Nachvollziehbarkeit; • Authentifizierung und Zugriffsmanagement (z. B. SSO); • optionale Integrationen (E-Mail-Erfassung, Analytics, Funktionsaufrufe).	**Nature & purpose** • receiving, analysing and responding to user inputs via AI/LLM services; • pseudonymisation/PII masking before forwarding, and de-pseudonymisation of returns where applicable; • logging/storing chat histories and logs for traceability; • authentication and access management (e.g. SSO); • optional integrations (email capture, analytics, function calls).
Kategorien personenbezogener Daten • Inhalte von Chat-Eingaben und -Ausgaben; • Namensangaben (Authentifizierung/Nennung im Text); • E-Mail-Adressen und Nutzerkennungen; • IP-Adressen, Geräte-/Browser-Metadaten; • Session- und Nutzungsdaten, Log-/Protokolldaten, Zeitstempel; • Authentifizierungsdaten (z. B. SSO-Attribute); • Cookie-/localStorage-Kennungen; • kontextbezogene Metadaten, Unternehmens-/Projektbezüge (falls enthalten).	**Categories of personal data** • content of chat inputs and outputs; • names (authentication/mention in text); • email addresses and user identifiers; • IP addresses, device/browser metadata; • session and usage data, log data, timestamps; • authentication data (e.g. SSO attributes); • cookie/localStorage identifiers; • contextual metadata, company/project references (if contained).
Kategorien betroffener Personen • Website-Besucher:innen, Chatbot-Nutzer:innen; • registrierte Nutzer:innen / Mitarbeitende des Kunden; • Endkund:innen und Dritte, sofern deren Daten in Eingaben eingebracht werden.	**Categories of data subjects** • website visitors, chatbot users; • registered users / customer's staff; • end customers and third parties whose data is entered in inputs.

DEUTSCH	ENGLISH
Hinweis zu besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) Die Plattform ist nicht für die planmäßige oder gezielte Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO vorgesehen. Der Verantwortliche wirkt durch geeignete Hinweise gegenüber den Nutzer:innen darauf hin, dass solche Daten nicht in Chat-Eingaben eingegeben werden sollen. Soweit Nutzer:innen dennoch besondere Kategorien personenbezogener Daten in Chat-Eingaben übermitteln, kann es zu einer unbeabsichtigten Verarbeitung dieser Daten im Rahmen der vertraglich vereinbarten Verarbeitungsvorgänge kommen. Die bloße Tatsache einer solchen unbeabsichtigten Übermittlung und der sich daraus ergebenden Verarbeitung stellt für sich genommen keine Pflichtverletzung des Auftragsverarbeiters im Sinne von § 12 Abs. 1 dar. Unberührt bleibt die Haftung des Auftragsverarbeiters für die Verletzung der nach Art. 32 DSGVO vereinbarten technischen und organisatorischen Maßnahmen sowie der Melde- und Unterstützungspflichten nach §§ 5 und 9 dieser Vereinbarung im Zusammenhang mit solchen Daten; für die Maskierungs- bzw. Pseudonymisierungsfunktion nach § 4 Abs. 2 gelten dabei die in Anlage 3 Ziffer 3 beschriebenen Grenzen.	**Note on special categories of personal data (Art. 9 GDPR)** The platform is not intended for the systematic or targeted processing of special categories of personal data within the meaning of Art. 9(1) GDPR. The Controller shall, by appropriate notices to users, work towards ensuring that such data is not entered into chat inputs. Where users nevertheless transmit special categories of personal data in chat inputs, unintended processing of such data may occur within the contractually agreed processing operations. The mere fact of such unintended transmission and of the processing resulting from it does not in itself constitute a breach of duty by the Processor within the meaning of § 12(1). This does not affect the Processor's liability for breaches of the technical and organisational measures agreed under Art. 32 GDPR or of the notification and assistance obligations under §§ 5 and 9 of this Agreement in connection with such data; in this respect, the limits described in Annex 3 section 3 apply to the masking/pseudonymisation function under § 4(2).
Dauer Für die Dauer des Hauptvertrags; danach Löschung/ Rückgabe nach § 10.	**Duration** For the term of the main contract; thereafter deletion/return under § 10.
PII-Maskierung / Pseudonymisierung (§ 4 Abs. 2) [X] aktiviert [ ] deaktiviert Voreinstellung für Variante C: aktiviert. Bei „deaktiviert" gilt § 7 Abs. 5 Satz 2.	**PII masking / pseudonymisation (§ 4(2))** [X] activated [ ] deactivated Default for Variant C: activated. If "deactivated", § 7(5) sentence 2 applies.
Variante C: Automatische PII-Maskierungs-Vorkonfiguration Bei Auswahl von Variante C setzt HybridAI vor Produktionsfreigabe `llm_pii_masking_enabled=true` als Produktionsstandard für den Bot. Abweichungen (explizites Deaktivieren der Maskierung für einzelne Bots/Szenarien) sind zulässig, bedürfen aber einer dokumentierten schriftlichen Weisung des Verantwortlichen mit Begründung (Art. 28 Abs. 3 lit. a DSGVO).	**Variant C: Automatic PII masking pre-configuration** When Variant C is selected, HybridAI sets `llm_pii_masking_enabled=true` as the production default for the bot prior to go-live. Deviations (explicitly disabling masking for individual bots/scenarios) are permitted but require documented written instructions from the Controller with justification (Art. 28(3)(a) GDPR).
Datenschutz-Ansprechpartner & Datenschutzbeauftragter Verantwortlicher: **[Contact person (optional)]** Auftragsverarbeiter (HybridAI GmbH): Stephan Noller, privacy@hybridai.one **Datenschutzbeauftragter der HybridAI GmbH:** Gregor Klar brainosphere 1 GmbH Witzlebenstraße 21a 14057 Berlin klar@brainosphere.de	**Data protection contact & Data Protection Officer** Controller: **[Contact person (optional)]** Processor (HybridAI GmbH): Stephan Noller, privacy@hybridai.one **Data Protection Officer of HybridAI GmbH:** Gregor Klar brainosphere 1 GmbH Witzlebenstraße 21a 14057 Berlin klar@brainosphere.de

Anlage 2 – Unterauftragsverarbeiter · Annex 2 – Sub-processors

Mit allen aufgeführten Unterauftragsverarbeitern besteht eine AVV/DPA (vgl. § 6 Abs. 6). DPF-Zertifizierungen sind vor jeder Übermittlung auf der offiziellen DPF-Liste (dataprivacyframework.gov) zu verifizieren. · A DPA is in place with every sub-processor listed (see § 6(6)). DPF certifications must be verified on the official DPF list before each transfer.

Unterauftragnehmer / Sub-processor	Zweck / Purpose	Standort / Location	Drittland? / Third country	Schutzgarantie / Safeguard
Hetzner Online GmbH	Server-Hosting / Cloud-Infrastruktur	Deutschland (Falkenstein, Nürnberg)	Nein / No	AVV / DPA, DSGVO/ GDPR
OpenAI Ireland Ltd.	KI-/LLM-Dienste (GPT)	EU und Drittländer, einschließlich USA gemäß aktueller OpenAI Sub-Processor List	Ja / Yes (USA)	SCC 2021/914 (Modul 3) + TIA; DPF nicht anwendbar
Anthropic PBC	KI-/LLM-Dienste (Claude)	USA (keine EU-Region festlegbar)	Ja / Yes (USA)	SCC 2021/914 (Modul 3) + TIA; DPF nicht anwendbar
Google Ireland Ltd. / Google LLC (Gemini Developer API)	KI-/LLM-Dienste, Bild-Generierung	Global (USA, EU, APAC)	Ja / Yes (USA)	SCC 2021/914 (Module 2/3) + DPF; siehe TIA Google
Mistral AI	KI-/LLM-Dienste	Frankreich / EU	Nein / No	EU-Verarbeitung / EU processing
Melious AI GmbH	EU-KI-/LLM-Dienste und Inferenzvermittlung / EU AI/ LLM services and inference routing	Deutschland; Inferenz in der EU durch Anbieter der Melious-Unterauftragsverarbeiterliste / subprocessor notice	Nein für diese Inferenzroute / No for this inference route	AVV / DPA; EU-Inferenz / EU inference
Brevo (Sendinblue SAS)	Transaktions-/Marketing-E-Mails	Frankreich / EU	Nein / No	EU-Verarbeitung; AVV / DPA

Anlage 3 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO) · Annex 3 – Technical and organisational measures (Art. 32 GDPR)

DEUTSCH	ENGLISH
1. Verschlüsselung / Encryption TLS 1.2+ für Daten in Übertragung; AES-256 für ruhende Daten (soweit anwendbar).	**1. Encryption** TLS 1.2+ in transit; AES-256 at rest (where applicable).
2. Zugangs-/Zugriffskontrolle Rollenbasierte Rechte, MFA für Admin-Zugänge, regelmäßige Rechteprüfung, Need-to-know.	**2. Access control** Role-based rights, MFA for admin access, regular access reviews, need-to-know.
3. Pseudonymisierung / PII-Maskierung Verfügbare Funktion zur Maskierung identifizierender Daten vor Weiterleitung an externe KI-/LLM-Dienste; Aktivierung gemäß Anlage 1. Grenzen: Die Erkennung erfolgt musterbasiert bzw. durch automatische Namenserkennung in Freitexteingaben; eine vollständige Erkennung und Maskierung aller personenbezogenen Daten ist technisch nicht gewährleistet (kein 100-%-Erkennungsgrad).	**3. Pseudonymisation / PII masking** Available function to mask identifying data before forwarding to external AI/LLM services; activation per Annex 1. Limits: detection is pattern-based or via automated name recognition in free-text inputs; complete detection and masking of all personal data is not technically guaranteed (no 100 % recall).
4. Protokollierung & Monitoring Zugriffs-/Systemlogs (mind. 12 Monate), automatisierte Anomalie-/Angriffserkennung.	**4. Logging & monitoring** Access/system logs (min. 12 months), automated anomaly/intrusion detection.
5. Datensicherung & Recovery Täglich verschlüsselte Backups: 7 tägliche + 4 wöchentliche + 12 monatliche Archive (Borg); wöchentliche Wiederherstellungstests.	**5. Backup & recovery** Daily encrypted backups: 7 daily + 4 weekly + 12 monthly archives (Borg); weekly restore tests.
6. Infrastruktursicherheit Server-Betrieb in DE/EU, Patch-Management, System-Härtung, sichere Konfigurationen.	**6. Infrastructure security** Servers in DE/EU, patch management, hardening, secure configurations.
7. Incident Response Dokumentierter Plan mit Rollen; Meldung an Verantwortlichen gemäß § 9.	**7. Incident response** Documented plan with roles; notification to Controller per § 9.
8. Datentrennung / Segregation Mandantentrennung; Trennung nach Zweck durch logische/technische Maßnahmen.	**8. Segregation** Tenant separation; purpose-based separation by logical/technical means.
9. Datenlebenszyklus / Lifecycle Löschung auf Anforderung bzw. nach Fristablauf; sichere Löschverfahren.	**9. Data lifecycle** Deletion on request or after retention; secure deletion procedures.
10. Steuerung Unterauftragsverarbeiter Verträge auf Basis SCC/Angemessenheit; periodische Compliance-Prüfungen.	**10. Sub-processor governance** Contracts based on SCC/adequacy; periodic compliance checks.
11. Audits & Überprüfung Jährliche interne Audits; Review nach wesentlichen System-/Rechtsänderungen.	**11. Audits & review** Annual internal audits; review after material system/legal changes.

Anlage 4 – Verpflichtung zur Verschwiegenheit gemäß § 203 StGB · Annex 4 – Confidentiality obligation pursuant to Sec. 203 StGB

DEUTSCH	ENGLISH
Diese Anlage entfällt für diese Vereinbarung. Sie wird nur benötigt, wenn eine oder beide Parteien an Berufe mit Verschwiegenheitspflicht (§ 203 StGB, z.B. Rechtsanwälte, Ärzte, Psychotherapeuten) gebunden sind. Sollte dies der Fall sein, bitte den Haken oben setzen und die Verschwiegenheitsverpflichtung wird automatisch in diesen Vertrag aufgenommen.	*This annex does not apply to this Agreement. It is only needed if one or both parties are bound to professions with confidentiality obligations (e.g. attorneys, physicians, psychotherapists). If this applies, please check the box above and the confidentiality obligation will be automatically included in this contract.*

Anlage 5 – Transfer Impact Assessments (TIA) für US-basierte LLM-Provider · Annex 5 – Transfer Impact Assessments for US-based LLM providers

DEUTSCH	ENGLISH
Diese Anlage dokumentiert die Risiken und Schutzmaßnahmen für Datenübermittlungen an LLM-Provider in den USA gemäß Standardvertragsklauseln (Art. 46 DSGVO) und teilweise unter dem EU-US Data Privacy Framework (Art. 45 DSGVO, für Google). Abhängig von der gewählten Konfiguration können folgende TIAs anwendbar sein:	This annex documents the risks and safeguards for data transfers to US-based LLM providers under Standard Contractual Clauses (Art. 46 GDPR) and partially under the EU-US Data Privacy Framework (Art. 45 GDPR, for Google). Depending on the configuration selected, the following TIAs may apply:

5.1 Transfer Impact Assessment für OpenAI · TIA for OpenAI

DEUTSCH	ENGLISH
Transfer Impact Assessment (TIA) für OpenAI Ireland Ltd. Dieses Dokument beschreibt die Übermittlung personenbezogener Daten in die USA zu OpenAI gemäß Art. 46 DSGVO, durchgeführt eine Risikoanalyse zu Drittlandeingriffen und dokumentiert ergänzende technische Schutzmaßnahmen. ***Basis:*** *OpenAI Data Processing Addendum (v.010126, cdn.openai.com/pdf/openai-data-processing-addendum.pdf), OpenAI Trust Portal (trust.openai.com), OpenAI Sub-Processor-Liste (openai.com/policies/sub-processor-list).*	**Transfer Impact Assessment (TIA) for OpenAI Ireland Ltd.** This document describes the transfer of personal data to the United States to OpenAI pursuant to Art. 46 GDPR, including risk analysis of third-country surveillance and documentation of supplementary technical safeguards. ***Basis:*** *OpenAI Data Processing Addendum (v.010126, cdn.openai.com/pdf/openai-data-processing-addendum.pdf), OpenAI Trust Portal (trust.openai.com), OpenAI Sub-Processor List (openai.com/policies/sub-processor-list).*

1. Beschreibung des Datentransfers · Description of data transfer

DEUTSCH	ENGLISH
Empfänger & Zuständigkeit: • **Primär:** OpenAI Ireland Ltd. (Irland) • **Sub-Prozessoren:** Siehe OpenAI Sub-Processor-Liste (Stand: aktuell von openai.com/policies/sub-processor-list, typischerweise Microsoft Azure als Cloud-Infrastruktur-Provider) **Verarbeitungszweck:** KI-/LLM-Dienste für Chat, Textgenerierung und Analyse. OpenAI verarbeitet die Eingaben, generiert Responses und speichert diese **nicht** für Training (vertraglich ausgeschlossen in § 2 Abs. 4 dieser AVV und in OpenAIs DPA). **Kategorien personenbezogener Daten:** Chat-Inhalte (Text), Nutzerkennungen, E-Mail-Adressen, IP-Adressen, Gerätemetadaten, Zeitstempel, Session-IDs. **Kategorien betroffener Personen:** Endbenutzende der KI-Chatbot-Plattform (Website-Besucher:innen, registrierte Nutzer:innen, deren Kontakte, ggf. Dritte in eingegebenen Texten erwähnt). **Übermittlungshäufigkeit & -dauer:** Ad-hoc bei jeder Nutzereingabe. Speicherung und Aufbewahrungsdauer richten sich nach den für den verwendeten API-Endpunkt geltenden OpenAI-Bedingungen. Sofern keine abweichende, dokumentierte Zero-Data-Retention-Konfiguration vereinbart ist, können API-Eingaben und -Ausgaben bis zu 30 Tage aufbewahrt werden.	**Recipient & responsibility:** • **Primary:** OpenAI Ireland Ltd. (Ireland) • **Sub-processors:** See OpenAI Sub-Processor List (current from openai.com/policies/sub-processor-list, typically Microsoft Azure as cloud infrastructure provider) **Purpose of processing:** AI/LLM services for chat, text generation and analysis. OpenAI processes inputs, generates responses, and does **not** store them for training (contractually excluded in § 2(4) of this Agreement and in OpenAI's DPA). **Categories of personal data:** Chat content (text), user identifiers, email addresses, IP addresses, device metadata, timestamps, session IDs. **Categories of data subjects:** End users of the AI chatbot platform (website visitors, registered users, their contacts, third parties mentioned in inputs where applicable). **Transfer frequency & duration:** Ad-hoc with each user input. Storage and retention duration are governed by the conditions applicable to the API endpoint used. Unless a documented Zero-Data-Retention configuration is agreed, API inputs and outputs may be retained for up to 30 days.

2. Rechtsgrundlage der Übermittlung · Legal basis for transfer

DEUTSCH	ENGLISH
Primäre Rechtsgrundlage (alleinige): Standardvertragsklauseln (SCC) nach Durchführungsbeschluss (EU) 2021/914, Module 2 und 3 (Controller-zu-Prozessor und Prozessor-zu-Prozessor). Der Auftragsverarbeitungsvertrag mit OpenAI **enthält beide Module** (siehe OpenAI Data Processing Addendum v.010126). **EU-US Data Privacy Framework (DPF) – nicht anwendbar:** OpenAI erklärt in seiner EU Privacy Policy (openai.com/policies/eu-privacy-policy/) explizit, dass das Unternehmen **nicht am DPF teilnimmt**. Verifizierung der offiziellen DPF-Liste auf dataprivacyframework.gov (Stand: 2026-08-07) bestätigt diesen Status. Das DPF ist daher für diese Übermittlung **nicht verfügbar**. Die SCC bleiben die alleinige Rechtsgrundlage. **Rechtliche Implikation:** Eine Klage gegen den Angemessenheitsbeschluss (EU) 2023/1795 wurde eingereicht (Latombe v Commission, T-553/23; Klage wurde abgewiesen, derzeit in Berufung C-703/25 P vor dem EUGH). Unabhängig vom Ausgang dieser Verfahren sind die SCCs Module 2/3 die zuverlässige Rechtsgrundlage und bleiben anwendbar. Ein negativer CJEU-Urteil würde die DPF aufheben, ändert aber nichts an den SCC-Gültigkeit.	**Primary legal basis (sole):** Standard Contractual Clauses (SCC) under Implementing Decision (EU) 2021/914, Modules 2 and 3 (controller-to-processor and processor-to-processor). The data processing agreement with OpenAI **contains both modules** (see OpenAI Data Processing Addendum v.010126). **EU-US Data Privacy Framework (DPF) – not available:** Verification of the official DPF register at dataprivacyframework.gov (as of 2026-08-07) confirms that OpenAI is **not listed as certified**. The DPF is therefore **not applicable** for this transfer. The SCC remains the sole legal basis. **Legal implication:** A case against Adequacy Decision (EU) 2023/1795 was filed (Latombe v Commission, T-553/23; case dismissed, currently on appeal C-703/25 P before the CJEU). Regardless of the outcome, SCC Modules 2/3 are the reliable legal basis and remain applicable. A negative CJEU ruling would repeal the DPF, but does not affect the validity of the SCC.

3. Drittlandrisiken – Analyse der US-amerikanischen Überwachungsgesetze · Third-country risks – analysis of US surveillance law

DEUTSCH	ENGLISH
Identifizierte Risiken: • **FISA Section 702 (50 U.S.C. § 1881a) — Foreign Intelligence Surveillance Act:** US-Geheimdienste können ohne Gericht und ohne Benachrichtigung an den Verantwortlichen Daten von „ausländischen Zielen" sammeln (Targeting). Cloud-Anbieter in den USA müssen Anfragen kooperativ beantworten. Der betroffene Nutzer erhält keine Notiz. • **CLOUD Act (18 U.S.C. § 2701-2713):** US-Strafverfolgungsbehörden können via Warrant oder Subpoena Zugriff auf Daten verlangen, auch wenn der Dateninhaber nicht-US ist. US-Cloud-Provider müssen diese erfüllen, auch bei fehlender Benachrichtigung des Verantwortlichen. • **Executive Orders & Presidential Policy:** Laufende Executive Orders (z.B. Precision Targeting) ermöglichen erweiterte Datenzugriffe für Sicherheitszwecke mit reduzierter Transparenz. **Realistischer Impact:** Während breite „Massenüberwachung" aller Daten technisch und juristisch unrealistisch ist, ist die Möglichkeit eines gezielten Zugriffs auf OpenAI-Daten zu diesem Nutzer/dieser Anfrage gegeben — mit oder ohne Vorankündigung an HybridAI oder den Verantwortlichen.	**Identified risks:** • **FISA Section 702 (50 U.S.C. § 1881a) — Foreign Intelligence Surveillance Act:** US intelligence agencies may collect data from "foreign targets" without court order or notification to the Controller. Cloud providers in the US must cooperate with requests. The affected user receives no notice. • **CLOUD Act (18 U.S.C. § 2701-2713):** US law enforcement can obtain access to data via warrant or subpoena, regardless of the data holder's non-US status. US cloud providers must comply even without notifying the Controller. • **Executive Orders & Presidential Policy:** Ongoing executive orders (e.g. Precision Targeting) enable expanded data access for national security with reduced transparency. **Realistic impact:** While broad "mass surveillance" of all data is technically and legally unrealistic, the possibility of targeted access to OpenAI data for this user/request exists — with or without prior notice to HybridAI or the Controller.

4. Ergänzende Schutzmaßnahmen · Supplementary safeguards

DEUTSCH	ENGLISH
A. Technische Datenschutz-Maßnahmen (HybridAI-seitig): • **PII-Maskierung (optional aktivierbar):** Falls in Anlage 1 vereinbart, maskiert HybridAI identifizierende Daten (`<EMAIL_1>`, `<NAME_1>`) vor Übermittlung zu OpenAI. OpenAI sieht nur Platzhalter, nicht die Originalwerte. • **Minimale Datenübermittlung:** Nur für die LLM-Verarbeitung notwendige Chat-Inhalte werden übermittelt (keine User-Metadaten, keine Log-Dateien, keine Historisierung). • **Aufbewahrungsdauer:** Speicherung und Aufbewahrung richten sich nach OpenAI-Bedingungen für den verwendeten API-Endpunkt (standardmäßig bis zu 30 Tage, vorbehaltlich dokumentierter abweichender ZDR-Konfiguration). **B. Vertragliche Zusicherungen (OpenAI-seitig):** • **Kein Training:** OpenAI versichert vertraglich (DPA v.010126, § 5.3), dass Chat-Daten NICHT für Modell-Training verwendet werden, sofern der Verantwortliche dies nicht explizit opt-in. • **Data Processing Addendum (Module 2 & 3):** OpenAI ist gebunden durch SCCs mit Informations- und Auditkooperation nach Maßgabe der OpenAI DPA. • **Sub-Processor-Transparenz:** OpenAI veröffentlicht seine Sub-Prozessor-Liste (openai.com/policies/sub-processor-list/) mit 15-Tage-Vorabbenachrichtigung bei Änderungen (Opt-out-Recht).	**A. Technical data protection measures (HybridAI-side):** • **PII masking (optionally activated):** If agreed in Annex 1, HybridAI masks identifying data (`<EMAIL_1>`, `<NAME_1>`) before transmission to OpenAI. OpenAI sees only placeholders, not original values. • **Minimal data transmission:** Only chat content necessary for LLM processing is sent (no user metadata, no log files, no history). • **Retention:** Storage and retention are governed by the conditions applicable to the API endpoint used. Unless a documented Zero Data Retention configuration applies, API inputs and outputs may be retained for up to 30 days. **B. Contractual assurances (OpenAI-side):** • **No training:** OpenAI contractually assures (DPA v.010126, § 5.3) that chat data is NOT used for model training unless the Controller explicitly opts in. • **Data Processing Addendum (Modules 2 & 3):** OpenAI is bound by SCCs with audit cooperation (per applicable OpenAI DPA). • **Sub-processor transparency:** OpenAI publishes its sub-processor list (openai.com/policies/sub-processor-list/) with 15-day advance notice of changes (opt-out right).

5. OpenAI Compliance Profil & Zertifizierungen · OpenAI Compliance Profile & Certifications

DEUTSCH	ENGLISH
Datenschutz-Abkommen: • **Data Processing Addendum (v.010126):** Verfügbar über openai.com/enterprise-privacy; unterzeichnungspflichtig, enthält Module 2 und 3 der Standardvertragsklauseln • **Art. 28 DSGVO Compliance:** OpenAI verpflichtet sich zu Art. 28-konformen Datenverarbeitungspflichten (nur auf Weisung, nur dokumentierte Subprozessoren, Audit-Kooperation) • **Audit-Recht:** Informations- und Auditkooperation unter NDA mit angemessener Vorankündigung (nach Maßgabe der OpenAI DPA) **Sicherheitszertifizierungen (OpenAI Trust Portal):** • ✅ **SOC 2 Type II:** Regelmäßig auditiert (aktuell auf trust.openai.com einsehbar) • ✅ **ISO 27001:2022:** Information Security Management • ✅ **ISO 27701:2019:** Privacy Information Management • ✅ **ISO 42001:2023:** AI Management System (neu, adressiert AI-spezifische Risiken) **Infrastruktur-Standorte:** • **Primär:** Vereinigte Staaten (USA). Standardmäßig keine EU-Region verfügbar. • **EU Data Residency (optionale Endpunkt-Konfiguration):** OpenAI bietet optional EU-Residency-Konfigurationen an (z.B. eu-Endpoint für Verarbeitung auf EU-Servern). Diese Optionen können im Service-Agreement oder der API-Konfiguration spezifiziert werden. • **Sub-Prozessoren:** Hauptsächlich Microsoft Azure (global), auch andere Cloud-Provider möglich (siehe aktuelle Sub-Processor-Liste) **Transparenz zu Behördenanfragen:** OpenAI veröffentlicht einen jährlichen Transparency Report mit Statistiken zu Behördenanfragen (Law Enforcement Requests unter FISA/CLOUD Act); verfügbar auf openai.com/policies/transparency.	**Data protection agreements:** • **Data Processing Addendum (v.010126):** Available via openai.com/enterprise-privacy; signature required; contains Modules 2 and 3 of Standard Contractual Clauses • **Art. 28 GDPR compliance:** OpenAI commits to Art. 28-compliant processing obligations (instructions only, documented sub-processors, audit cooperation) • **Audit right:** Audit cooperation under NDA with reasonable notice (per applicable OpenAI DPA) **Security certifications (OpenAI Trust Portal):** • ✅ **SOC 2 Type II:** Regularly audited (current on trust.openai.com) • ✅ **ISO 27001:2022:** Information Security Management • ✅ **ISO 27701:2019:** Privacy Information Management • ✅ **ISO 42001:2023:** AI Management System (new, addresses AI-specific risks) **Infrastructure locations:** • **Primary:** United States (USA). No EU region available by default. • **EU Data Residency (optional endpoint configuration):** OpenAI optionally offers EU residency configurations (e.g. eu-endpoint for processing on EU servers). These options can be specified in the service agreement or API configuration. • **Sub-processors:** Primarily Microsoft Azure (global), other cloud providers possible (see current sub-processor list) **Transparency on government requests:** OpenAI publishes an annual Transparency Report with statistics on government requests (Law Enforcement Requests under FISA/CLOUD Act); available at openai.com/policies/transparency.

6. Bewertung der Schutzmaßnahmen & Abschließende Einschätzung · Assessment of safeguards & final assessment

DEUTSCH	ENGLISH
Risiko-Gesamtbewertung: Das Transferrisiko ist **real** (US-Behörden können gezielt auf OpenAI-Daten zugreifen), aber **minimiert** durch technische und vertragliche Maßnahmen: • ✅ **Datenmenge:** Auf erforderliche Inhalte begrenzt; zusätzliche Minimierung durch PII-Maskierung, sofern gemäß Anlage 1 aktiviert • **Aufbewahrung:** Bis zu 30 Tage nach OpenAI-Bedingungen (sofern nicht ZDR konfiguriert) • ✅ **Kontraktuelle Zusicherungen:** Kein Training, klare SCC, Audit-Rechte • ✅ **Sicherheitszertifikation:** OpenAI SOC 2 Type II, ISO 27001, ISO 42001 • ⚠️ **Offene Restrisiken:** FISA 702 und CLOUD Act können nicht durch private Verträge aufgehoben werden **Gesamturteil:** HybridAI kommt auf Grundlage der dokumentierten Konfiguration zu der Einschätzung, dass die eingesetzten Schutzgarantien (SCC Module 2/3 gemäß Art. 46 DSGVO, Sicherheitszertifizierungen, Audit-Rechte) das identifizierte Transferrisiko reduzieren. Der Verantwortliche hat anhand seiner konkreten Verarbeitung und Datenarten zu beurteilen, ob die verbleibenden Risiken und die implementierten Schutzmaßnahmen für den jeweiligen Verarbeitungsvorgang ausreichend sind. Optionale Zusatzmaßnahmen (EU Data Residency, Zero Data Retention) können das Risiko weiter reduzieren.	**Overall risk assessment:** The transfer risk is **real** (US authorities can target OpenAI data), but **mitigated** by technical and contractual measures: • ✅ **Data volume:** Limited to required content; additional minimization through PII masking if activated per Annex 1 • **Retention:** Up to 30 days under the conditions applicable to the API endpoint used, unless a documented Zero Data Retention configuration applies • ✅ **Contractual assurances:** No training, clear SCC, audit rights • ✅ **Security certification:** OpenAI SOC 2 Type II, ISO 27001, ISO 42001 • ⚠️ **Residual risks:** FISA 702 and CLOUD Act cannot be eliminated by private contracts **Final conclusion:** HybridAI concludes on the basis of the documented configuration that the implemented safeguards (SCC Modules 2/3 per Art. 46 GDPR, security certifications, audit rights) reduce the identified transfer risk. The Controller shall assess on the basis of its specific processing and data categories whether the residual risks and implemented safeguards are sufficient for the respective processing operation. Optional supplementary measures (EU Data Residency, Zero Data Retention) can further reduce the risk.

7. Verfahren bei Änderungen & Kontrollrechte · Procedure for changes & control rights

DEUTSCH	ENGLISH
Überwachung des Transfermechanismus: HybridAI überwacht laufend die Gültigkeit der Rechtsgrundlagen und der Schutzvorkehrungen. Sollten sich folgende Rahmenbedingungen wesentlich ändern, wird der Verantwortliche unverzüglich benachrichtigt: • Aufhebung oder wesentliche Änderung des DPF-Angemessenheitsbeschlusses (CJEU-Entscheidung) • Neue oder geänderte US-Gesetze, die das Transferrisiko erheblich verschärfen • Widerruf oder Suspendierung von OpenAIs Zertifikationen (SOC 2, ISO 27001) • Wesentliche Änderungen in OpenAIs Subprozessoren oder Infrastruktur • Bestätigung von gezielten Behördenzugriffen auf Kundendata (Transparency Report) **Kontrollrechte des Verantwortlichen:** Der Verantwortliche kann schriftlich ein TIA-Review oder ein Audit bei OpenAI anfordern, in Übereinstimmung mit den Audit-Kooperationsbestimmungen der OpenAI DPA. HybridAI wird die Anfrage weiterleiten und kooperativ mit OpenAI und dem Verantwortlichen arbeiten. Die Kosten für externe Audits trägt der Verantwortliche.	**Monitoring of transfer mechanism:** HybridAI continuously monitors the validity of legal bases and safeguards. Should the following circumstances materially change, the Controller will be informed without undue delay: • Repeal or material amendment of the DPF adequacy decision (CJEU ruling) • New or amended US law materially increasing transfer risk • Revocation or suspension of OpenAI's certifications (SOC 2, ISO 27001) • Material changes to OpenAI's sub-processors or infrastructure • Confirmed targeted government access to customer data (Transparency Report) **Controller's control rights:** The Controller may request in writing a TIA review or an audit at OpenAI, in accordance with the audit cooperation provisions of the OpenAI DPA. HybridAI will forward the request and work cooperatively with OpenAI and the Controller. Costs for external audits are borne by the Controller.

Hinweis zu Verantwortlichkeiten / Note on responsibilities: *Dieses TIA dokumentiert die Schutzmaßnahmen und Risiken für diese spezifische Datenübermittlung zu OpenAI. Es ersetzt **nicht** die eigenständige Compliance-Verantwortung des Verantwortlichen gemäß Art. 46 DSGVO. Der*

*Verantwortliche bleibt verantwortlich für die Rechtskonformität dieser Übermittlung unter den dann geltenden US- und EU-Gesetzen. HybridAI stellt dieses TIA als Informations- und Entscheidungsgrundlage zur Verfügung; die Unterzeichnung dieser AVV bedeutet nicht, dass der Verantwortliche alle Risiken automatisch akzeptiert, sondern dass er diese Analyse bestätigt hat und eine bewusste Wahl für Variante C trifft. · This TIA documents safeguards and risks for this specific data transfer to OpenAI. It does **not** substitute the Controller's independent compliance responsibility under Art. 46 GDPR. The Controller remains responsible for the lawfulness of this transfer under applicable US and EU law. HybridAI provides this TIA as information and decision support; signing this Agreement does not mean the Controller automatically accepts all risks, but rather confirms this analysis and makes a conscious choice for Variant C.*

5.2 Transfer Impact Assessment für Anthropic · TIA for Anthropic

DEUTSCH	ENGLISH
Transfer Impact Assessment (TIA) für Anthropic PBC Dieses Dokument beschreibt die Übermittlung personenbezogener Daten in die USA zu Anthropic PBC gemäß Art. 46 DSGVO, durchgeführt eine Risikoanalyse zu Drittlandeingriffen und dokumentiert ergänzende technische Schutzmaßnahmen. ***Basis:*** *Anthropic Data Processing Addendum (DPA), Anthropic Trust Portal (claude.ai/trust), Anthropic Sub-Processor-Liste.*	**Transfer Impact Assessment (TIA) for Anthropic PBC** This document describes the transfer of personal data to the United States to Anthropic PBC pursuant to Art. 46 GDPR, including risk analysis of third-country surveillance and documentation of supplementary technical safeguards. ***Basis:*** *Anthropic Data Processing Addendum (DPA), Anthropic Trust Portal (claude.ai/trust), Anthropic Sub-Processor List.*

1. Beschreibung des Datentransfers · Description of data transfer

DEUTSCH	ENGLISH
Empfänger & Zuständigkeit: • **Primär:** Anthropic PBC (San Francisco, USA) • **Sub-Prozessoren:** Cloud-Infrastruktur-Provider (z.B. Google Cloud, AWS); siehe aktuelle Anthropic Sub-Processor-Liste **Verarbeitungszweck:** KI-/LLM-Dienste für Chat, Textgenerierung und Analyse mit Anthropic Claude-Modellen. Anthropic speichert die Eingaben **nicht** für Training (vertraglich ausgeschlossen in § 2 Abs. 4 dieser AVV und in Anthropics DPA). **Kategorien personenbezogener Daten:** Chat-Inhalte (Text), Nutzerkennungen, E-Mail-Adressen, IP-Adressen, Gerätemetadaten, Zeitstempel, Session-IDs. **Kategorien betroffener Personen:** Endbenutzende der KI-Chatbot-Plattform. **Übermittlungshäufigkeit & -dauer:** Ad-hoc bei jeder Nutzereingabe. Speicherung und Aufbewahrung richten sich nach Anthropic-Bedingungen für den verwendeten API-Endpunkt. Standardmäßig werden API-Eingaben und -Ausgaben innerhalb von 30 Tagen gelöscht, vorbehaltlich dokumentierter abweichender ZDR-Konfiguration, Policy-Durchsetzung oder rechtlicher Pflichten.	**Recipient & responsibility:** • **Primary:** Anthropic PBC (San Francisco, USA) • **Sub-processors:** Cloud infrastructure providers (e.g. Google Cloud, AWS); see current Anthropic sub-processor list **Purpose of processing:** AI/LLM services for chat, text generation and analysis using Anthropic Claude models. Anthropic does **not** store inputs for training (contractually excluded in § 2(4) of this Agreement and in Anthropic's DPA). **Categories of personal data:** Chat content (text), user identifiers, email addresses, IP addresses, device metadata, timestamps, session IDs. **Categories of data subjects:** End users of the AI chatbot platform. **Transfer frequency & duration:** Ad-hoc with each user input. Storage and retention are governed by Anthropic's conditions for the API endpoint used. By default, API inputs and outputs are deleted within 30 days, subject to documented Zero-Data-Retention configurations, policy enforcement, or legal obligations.

2. Rechtsgrundlage der Übermittlung · Legal basis for transfer

DEUTSCH	ENGLISH
Primäre Rechtsgrundlage (alleinige): Standardvertragsklauseln (SCC) nach Durchführungsbeschluss (EU) 2021/914, Module 2 und 3 (Controller-zu-Prozessor und Prozessor-zu-Prozessor). Der Auftragsverarbeitungsvertrag mit Anthropic enthält die geltenden SCCs. **EU-US Data Privacy Framework (DPF) – nicht verfügbar:** Verifizierung auf dataprivacyframework.gov (Stand: 2026-08-07) und Anthropic's Privacy Policy (privacy.claude.com) bestätigen, dass Anthropic **nicht am DPF teilnimmt**. Das DPF ist daher für diese Übermittlung nicht verfügbar. Die SCC bleiben die alleinige Rechtsgrundlage. **Unabhängig vom DPF-Status:** Die SCC Module 2/3 bleiben die zuverlässige Rechtsgrundlage und sind anwendbar, auch wenn die DPF-Berufung vor dem EUGH negativ ausfällt.	**Primary legal basis (sole):** Standard Contractual Clauses (SCC) under Implementing Decision (EU) 2021/914, Modules 2 and 3 (controller-to-processor and processor-to-processor). The data processing agreement with Anthropic contains the applicable SCCs. **EU-US Data Privacy Framework (DPF) – not available:** Verification on dataprivacyframework.gov (as of 2026-08-07) and Anthropic's Privacy Policy (privacy.claude.com) confirm that Anthropic **does not participate in the DPF**. Therefore, the DPF is not available for this transfer. SCC remains the sole legal basis. **Regardless of DPF status:** SCC Modules 2/3 remain the reliable legal basis and are applicable, even if the DPF appeal before the CJEU is unsuccessful.

3. Drittlandrisiken – Analyse der US-amerikanischen Überwachungsgesetze · Third-country risks – analysis of US surveillance law

DEUTSCH	ENGLISH
Identifizierte Risiken: Dieselben wie bei OpenAI (FISA Section 702, CLOUD Act, Executive Orders). US-Behörden können gezielt auf Daten zugreifen, die sich auf US-Servern befinden. **Realistischer Impact:** Während breite Massenüberwachung technisch unrealistisch ist, ist die Möglichkeit gezielten Zugriffs auf Anthropic-Daten gegeben — mit oder ohne Vorankündigung.	**Identified risks:** Same as OpenAI (FISA Section 702, CLOUD Act, Executive Orders). US authorities can target data located on US servers. **Realistic impact:** While broad mass surveillance is technically unrealistic, the possibility of targeted access to Anthropic data exists — with or without prior notice.

4. Ergänzende Schutzmaßnahmen · Supplementary safeguards

DEUTSCH	ENGLISH
A. Technische Datenschutz-Maßnahmen (HybridAI-seitig): • **PII-Maskierung (optional aktivierbar):** Falls aktiviert, maskiert HybridAI identifizierende Daten vor Übermittlung zu Anthropic. • **Minimale Datenübermittlung:** Nur für LLM-Verarbeitung notwendige Chat-Inhalte. • **Aufbewahrung:** Standardmäßig Löschung innerhalb von 30 Tagen (vorbehaltlich ZDR, Policy, rechtliche Pflichten). **B. Vertragliche Zusicherungen (Anthropic-seitig):** • **Kein Training:** Anthropic versichert vertraglich, dass Chat-Daten NICHT für Modell-Training verwendet werden. • **Data Processing Addendum:** Anthropic ist durch die geltenden SCCs gebunden und verpflichtet sich zur Audit-Kooperation nach Maßgabe der Anthropic DPA. • **Sub-Processor-Transparenz:** Anthropic veröffentlicht eine Sub-Prozessor-Liste mit Vorabbenachrichtigung bei Änderungen.	**A. Technical data protection measures (HybridAI-side):** • **PII masking (optionally activated):** Where activated, HybridAI masks identifying data before transmission to Anthropic. • **Minimal data transmission:** Only chat content necessary for LLM processing. • **Retention:** Default deletion within 30 days (subject to ZDR, policy, legal obligations). **B. Contractual assurances (Anthropic-side):** • **No training:** Anthropic contractually assures that chat data is NOT used for model training. • **Data Processing Addendum:** Anthropic is bound by SCC with audit cooperation (per applicable Anthropic DPA). • **Sub-processor transparency:** Anthropic publishes a sub-processor list with advance notice of changes.

5. Anthropic Compliance Profil & Zertifizierungen · Anthropic Compliance Profile & Certifications

DEUTSCH	ENGLISH
Datenschutz-Abkommen: • **Data Processing Addendum:** Verfügbar über Anthropic Trust Portal (claude.ai/trust) • **Art. 28 DSGVO Compliance:** Anthropic verpflichtet sich zu DSGVO-konformen Datenverarbeitungspflichten • **Audit-Recht:** Audit-Kooperation unter NDA mit angemessener Vorankündigung (nach Maßgabe der Anthropic DPA) **Sicherheitszertifizierungen:** Anthropic veröffentlicht Sicherheitsinformationen auf seinem Trust Portal; aktuelle Zertifizierungen (SOC 2, ISO-Status) sind dort einsehbar. **Infrastruktur-Standorte:** Standardmäßig USA (Cloud-Provider wie Google Cloud, AWS). EU-Residency ist nicht standardmäßig verfügbar; Kontakt mit Anthropic Sales für spezielle Anforderungen empfohlen.	**Data protection agreements:** • **Data Processing Addendum:** Available via Anthropic Trust Portal (claude.ai/trust) • **Art. 28 GDPR compliance:** Anthropic commits to GDPR-compliant processing obligations • **Audit right:** Audit cooperation under NDA with reasonable notice (per applicable Anthropic DPA) **Security certifications:** Anthropic publishes security information on its Trust Portal; current certifications (SOC 2, ISO status) are visible there. **Infrastructure locations:** Default is USA (cloud providers like Google Cloud, AWS). EU residency is not available by default; contact Anthropic Sales for special requirements.

6. Bewertung der Schutzmaßnahmen · Assessment of safeguards

DEUTSCH	ENGLISH
Gesamturteil: HybridAI kommt auf Grundlage der dokumentierten Konfiguration zu der Einschätzung, dass die eingesetzten Schutzgarantien (SCC Module 2/3 gemäß Art. 46 DSGVO, Sicherheitszertifizierungen, Audit-Rechte) das identifizierte Transferrisiko reduzieren. Das Risikoprofil ist vergleichbar mit OpenAI. Der Verantwortliche hat anhand seiner konkreten Verarbeitung und Datenarten zu beurteilen, ob die verbleibenden Risiken und die implementierten Schutzmaßnahmen für den jeweiligen Verarbeitungsvorgang ausreichend sind.	**Final conclusion:** HybridAI concludes on the basis of the documented configuration that the implemented safeguards (SCC Modules 2/3 per Art. 46 GDPR, security certifications, audit rights) reduce the identified transfer risk. The risk profile is comparable to OpenAI. The Controller shall assess on the basis of its specific processing and data categories whether the residual risks and implemented safeguards are sufficient for the respective processing operation.

5.3 Transfer Impact Assessment für Google (Gemini) · TIA for Google (Gemini)

DEUTSCH	ENGLISH
Transfer Impact Assessment (TIA) für Google Ireland Limited (Gemini) Dieses Dokument beschreibt die Übermittlung personenbezogener Daten für KI-Bild-Generierung zu Google Ireland Limited / Google LLC gemäß Art. 46 DSGVO, durchgeführt eine Risikoanalyse zu Drittlandeingriffen und dokumentiert ergänzende technische Schutzmaßnahmen. ***Basis (Stand: 2026-08-08):*** *Google Cloud DPA, Google Workspace / AI DPA, Google Trust Portal (cloud.google.com/security), DPF-Zertifizierung verified (dataprivacyframework.gov).*	**Transfer Impact Assessment (TIA) for Google Ireland Limited (Gemini)** This document describes the transfer of personal data for AI image generation to Google Ireland Limited / Google LLC pursuant to Art. 46 GDPR, including risk analysis of third-country surveillance and documentation of supplementary technical safeguards. ***Basis (as of 2026-08-08):*** *Google Cloud DPA, Google Workspace / AI DPA, Google Trust Portal (cloud.google.com/security), DPF certification verified (dataprivacyframework.gov).*

Punkt A: Beschreibung des Datentransfers · Description of data transfer

DEUTSCH	ENGLISH
Empfänger & Zuständigkeit: • **Primär:** Google Ireland Limited (Irland, EU) / Google LLC (USA, für Gemini API) • **Sub-Prozessoren:** Google Cloud-Infrastruktur; siehe aktuelle Google Sub-Processor-Liste **Verarbeitungszweck:** KI-Bild-Generierung über Gemini API (z.B. Bot-Avatare, Illustrationen). Die Eingabe-Prompts (z.B. „create a logo of a robot") werden an Google übermittelt; generierte Bilder werden zurückgesendet. Google speichert die Prompts **nicht** für Training (vertraglich ausgeschlossen). **Kategorien personenbezogener Daten:** Bild-Generierungs-Prompts (können indirekt PII enthalten, z.B. Firmenname), Bild-Metadaten, Request-ID, IP-Adressen, Zeitstempel. **Kategorien betroffener Personen:** Nutzer:innen, deren Namen/Firmen in Bild-Generierungs-Prompts erwähnt werden (indirekt); Bot-Administrator:innen, die die Anfrage stellen. **Übermittlungshäufigkeit & -dauer:** Auf Anforderung (z.B. beim Bot-Setup, nicht im Nutzerchat). Speicherung richtet sich nach Google Cloud DPA und Datenschutzrichtlinien. Input-Prompts werden nicht für Training persistiert (vertraglich ausgeschlossen).	**Recipient & responsibility:** • **Primary:** Google Ireland Limited (Ireland, EU) / Google LLC (USA, for Gemini API) • **Sub-processors:** Google Cloud infrastructure; see current Google sub-processor list **Purpose of processing:** AI image generation via Gemini API (e.g. bot avatars, illustrations). Input prompts (e.g. "create a logo of a robot") are transmitted to Google; generated images are returned. Google does **not** store prompts for training (contractually excluded). **Categories of personal data:** Image generation prompts (may indirectly contain PII, e.g. company name), image metadata, request ID, IP addresses, timestamps. **Categories of data subjects:** Users whose names/ companies are mentioned in image-generation prompts (indirectly); bot administrators making the request. **Transfer frequency & duration:** On demand (e.g. during bot setup, not in user chat). Storage and retention duration are governed by Google Cloud DPA and applicable retention policies. Input prompts are not used for model training as contractually agreed.

Punkt B: Rechtsgrundlage der Übermittlung · Legal basis for transfer

DEUTSCH	ENGLISH
Primäre Rechtsgrundlage: EU-US Data Privacy Framework (Angemessenheitsbeschluss nach Art. 45 DSGVO, Durchführungsbeschluss (EU) 2023/1795). **Google LLC ist als aktiv zertifiziert eingetragen** auf der offiziellen DPF-Liste (dataprivacyframework.gov, Stand: 2026-08-07; Frameworks: EU-U.S. DPF, Swiss-U.S. DPF, UK Extension). **Nachrangige Rechtsgrundlage:** Standardvertragsklauseln (SCC) nach Durchführungsbeschluss (EU) 2021/914, Module 2 und 3 (Art. 46 DSGVO). Der Auftragsverarbeitungsvertrag mit Google (Cloud DPA) enthält die geltenden SCCs als Fallback. **Praktische Anwendung:** Google kann sich auf den Angemessenheitsbeschluss (Art. 45) stützen. Im Falle einer CJEU-Aufhebung des DPF bleiben die SCC (Art. 46) als Fallback-Mechanismus gültig und anwendbar.	**Primary legal basis:** EU-US Data Privacy Framework (Adequacy Decision under Art. 45 GDPR, Implementing Decision (EU) 2023/1795). **Google LLC is listed as actively certified** on the official DPF register (dataprivacyframework.gov, as of 2026-08-07; frameworks: EU-U.S. DPF, Swiss-U.S. DPF, UK Extension). **Secondary legal basis:** Standard Contractual Clauses (SCC) under Implementing Decision (EU) 2021/914, Modules 2 and 3 (Art. 46 GDPR). The data processing agreement with Google (Cloud DPA) contains the applicable SCC as fallback. **Practical application:** Google can rely on the adequacy decision (Art. 45). In the event of a CJEU repeal of the DPF, the SCC (Art. 46) remains valid and applicable as fallback mechanism.

Punkt C: Drittlandrisiken – Analyse der US-amerikanischen Überwachungsgesetze · Third-country risks – analysis of US surveillance law

DEUTSCH	ENGLISH
Identifizierte Risiken: Dieselben wie bei OpenAI/Anthropic (FISA Section 702, CLOUD Act). US-Behörden können gezielt auf Daten zugreifen, die sich auf US-Servern befinden. **Besonderheit Google:** Google Workspace und Google Cloud bieten optionale EU-Data-Residency-Funktionen an, die für diese Übermittlung relevant sein können (siehe Anlage 3).	**Identified risks:** Same as OpenAI/Anthropic (FISA Section 702, CLOUD Act). US authorities can target data on US servers. **Google specifics:** Google Workspace and Google Cloud offer optional EU data residency options that may be relevant for this transfer (see Annex 3).

Punkt D: Ergänzende Schutzmaßnahmen · Supplementary safeguards

DEUTSCH	ENGLISH
A. Technische Datenschutz-Maßnahmen (HybridAI-seitig): • **Minimale Datenübermittlung:** Nur der Bild-Generierungs-Prompt wird zu Google gesendet (z.B. „create a robot logo"). Keine Metadaten, keine User-Profile, keine Log-Dateien. • **Aufbewahrung nach Google-Richtlinien:** Input-Prompts werden nicht für Training persistiert. Speicherdauer nach Google Cloud DPA. • **Keine PII in Prompts:** HybridAI-Richtlinien vorsehen, dass generische Prompts verwendet werden, nicht spezifische User-Namen oder Firmeninformationen (Best Practice). **B. Vertragliche Zusicherungen (Google-seitig):** • **Kein Training:** Google versichert vertraglich, dass Gemini-Prompts nicht für Modell-Training verwendet werden (Google Cloud DPA, Sec. 8.3). • **Speicherungsdauer:** Gemäß Google Generative AI API Terms of Service und Datenschutzrichtlinien. Globaler Standard-Endpoint, keine EU-Regionaloptionen verfügbar. • **Data Processing Addendum:** Google ist gebunden durch SCCs mit vollem Kontrollrecht des Verantwortlichen. • **Encryption in Transit:** TLS 1.3 für alle Übertragungen (Google Cloud Security). **C. Google's DPF-Zertifizierung:** Google ist auf der offiziellen DPF-Liste eingetragen (aktiv zertifiziert, Stand 2026-08-07). Das DPF bietet einen Rechtsmechanismus (Art. 45 DSGVO - Angemessenheitsbeschluss) zur Durchführung von Datentransfers. **Wichtig:** Das DPF ist ein Transfer-Framework und bietet keine technische Abschirmung vor US-Behördenzugriffen. Die in Punkt C beschriebenen Restrisiken (FISA 702, CLOUD Act) sind strukturell nicht durch das DPF aufgehoben.	**A. Technical data protection measures (HybridAI-side):** • **Minimal data transmission:** Only the image-generation prompt is sent to Google (e.g. "create a robot logo"). No metadata, no user profiles, no log files. • **Retention according to Google policies:** Storage and retention duration are governed by Google Cloud DPA and applicable retention policies. Input prompts are not used for model training as contractually agreed. • **No PII in prompts:** HybridAI policies call for generic prompts, not specific user names or company information (best practice). **B. Contractual assurances (Google-side):** • **No training:** Google contractually assures that Gemini prompts are not used for model training (Google Cloud DPA, Sec. 8.3). • **Retention duration:** Per Google Generative AI API Terms of Service and privacy policies. Global standard endpoint only; no EU regional options available. • **Data Processing Addendum:** Google is bound by SCC with audit cooperation rights (per applicable Google DPA). • **Encryption in transit:** TLS 1.3 for all transfers (Google Cloud Security). **C. Google's DPF certification:** Google is listed on the official DPF register (actively certified, as of 2026-08-07). The DPF provides a legal mechanism (Art. 45 GDPR - Adequacy Decision) for conducting data transfers. **Important:** The DPF is a transfer framework and does not provide technical shielding against US government access. The residual risks described in Point C (FISA 702, CLOUD Act) are not structurally eliminated by the DPF.

Punkt E: Google Compliance Profil & Zertifizierungen · Google Compliance Profile & Certifications

DEUTSCH	ENGLISH
Datenschutz-Abkommen: • **Google Cloud DPA:** Verfügbar auf cloud.google.com/terms/data-processing-addendum • **Art. 28 DSGVO Compliance:** Vollständig implementiert; Google unterliegt DSGVO-Kontrollen. • **Audit-Recht:** Google ermöglicht Audits durch unabhängige Prüfer; Kosten nach Vereinbarung (nach Maßgabe der Google DPA). **Sicherheitszertifizierungen:** • • **SOC 2 Type II:** Regularly audited • • **ISO 27001:2013** (in Erneuerung zu ISO 27001:2022) • • **ISO 27701:2019** (Privacy Information Management) • • **EU-US Data Privacy Framework:** Aktiv zertifiziert (dataprivacyframework.gov) **Infrastruktur-Standorte:** Gemini API (Generative AI API) verarbeitet Daten global über Google-Infrastruktur (USA, EU, APAC). Keine regionalen EU-Endpoints oder Residency-Optionen verfügbar. Datentransfer in die USA ist unumgänglich.	**Data protection agreements:** • **Google Cloud DPA:** Available at cloud.google.com/terms/data-processing-addendum • **Art. 28 GDPR compliance:** Fully implemented; Google is subject to GDPR controls. • **Audit right:** Google permits audits by independent auditors; costs per agreement (per applicable Google DPA). **Security certifications:** • • **SOC 2 Type II:** Regularly audited • • **ISO 27001:2013** (updating to ISO 27001:2022) • • **ISO 27701:2019** (Privacy Information Management) • • **EU-US Data Privacy Framework:** Actively certified (dataprivacyframework.gov) **Infrastructure locations:** Gemini API (Generative AI API) processes data globally via Google infrastructure (USA, EU, APAC). No regional EU endpoints or residency options available. Data transfer to USA is unavoidable.

Punkt F: Bewertung der Schutzmaßnahmen · Assessment of safeguards

DEUTSCH	ENGLISH
Gesamturteil: Die Übermittlung zu Google erfolgt unter angemessenen Schutzgarantien gemäß SCC nach Art. 46 DSGVO und/oder DPF nach Art. 45 DSGVO (Angemessenheitsbeschluss (EU) 2023/1795). HybridAI kommt auf Grundlage der dokumentierten Konfiguration zu der Einschätzung, dass die Schutzgarantien (SCC, DPF-Zertifizierung, Sicherheitszertifizierungen) das Transferrisiko reduzieren. Der Verantwortliche hat anhand seiner konkreten Verarbeitung und Datenarten zu beurteilen, ob die verbleibenden Risiken und die implementierten Schutzmaßnahmen ausreichend sind.	**Final conclusion:** The transfer to Google is implemented with adequate safeguards under SCC per Art. 46 GDPR and/or DPF per Art. 45 GDPR (Adequacy Decision (EU) 2023/1795). HybridAI concludes on the basis of the documented configuration that the safeguards (SCC, DPF certification, security certifications) reduce the transfer risk. The Controller shall assess on the basis of its concrete processing and data categories whether the residual risks and implemented safeguards are sufficient.

Anlage 6 – Speicher- und Löschkonzept · Annex 6 – Data Storage and Deletion Concept

DEUTSCH	ENGLISH
Speicher- und Löschkonzept für Chatverläufe, Logs und Benutzerdaten Dieses Dokument beschreibt, wie die Plattform personenbezogene Daten speichert, schützt, sichert und löscht, einschließlich Chatverläufe, Logs, Uploads und Systemdaten gemäß Art. 32 und Art. 17 DSGVO.	**Data Storage and Deletion Concept for Chat Histories, Logs and User Data** This document describes how the platform stores, protects, backs up, and deletes personal data, including chat histories, logs, uploads and system data pursuant to Art. 32 and Art. 17 GDPR.

1. Infrastruktur und Speicherorte · 1. Infrastructure and storage locations

DEUTSCH	ENGLISH
Datenbank (Chat-Verläufe, Logs, Metadaten) • **DBMS:** MySQL 8.0+ (produktiv-verwalteter Service) • **Hosting:** Hetzner Cloud (Deutschland, Falkenstein) • **Standort des Datenverzeichnisses:** Lokale Rootfs des DB-Servers (`/var/lib/mysql`), nicht auf austauschbarem Volume • **Datenkategorien:** Chat-Inhalte, Gesprächs-History, Session-Daten, Authentifizierungsmetadaten, Nutzungslogs, Systemlogs • **Datenbanken:** `hybridai` (Produktion), `hybridai_staging` (Staging) • **Zugriffskontrolle:** Netzwerkisolierung (private VPC), rollenbasierte Datenbank-Berechtigungen (App-User mit Lesezugriff, Admin-User für Wartung), TLS für Client-Verbindungen	**Database (chat histories, logs, metadata)** • **DBMS:** MySQL 8.0+ (production-managed service) • **Hosting:** Hetzner Cloud (Germany, Falkenstein data center) • **Data directory location:** Server's local root filesystem (`/var/lib/mysql`), not on detachable volume • **Data categories:** Chat content, conversation history, session data, authentication metadata, usage logs, system logs • **Databases:** `hybridai` (production), `hybridai_staging` (staging) • **Access control:** Network isolation (private VPC), role-based database privileges (app user with read access, admin user for maintenance), TLS for client connections
Object Storage (Datei-Uploads, Bot-Logos, Avatare, Generierte Bilder) • **Service:** Hetzner Object Storage (S3-kompatibel, Ceph RGW) • **Region:** nbg1 (Deutschland, Nürnberg) • **Buckets:** `hybridai-prod` (Produktion), `hybridai-staging` (Staging) • **Datenkategorien:** Nutzerdatei-Uploads (PDF, CSV, etc.), Bot-Konfigurationsbilder, Benutzer-Avatare, KI-generierte Bilder • **Zugriffskontrolle:** Private Buckets (anonyme GET = 403); Zugriff über zeitbegrenzte, signierte URLs (Presigned URLs, typischerweise 1-24 Stunden gültig) • **CORS:** GET/HEAD für alle Origins zugelassen (Sicherheit durch Signatur-Gating, nicht durch Origin-Restriction)	**Object Storage (file uploads, bot logos, avatars, generated images)** • **Service:** Hetzner Object Storage (S3-compatible, Ceph RGW) • **Region:** nbg1 (Germany, Nuremberg) • **Buckets:** `hybridai-prod` (production), `hybridai-staging` (staging) • **Data categories:** User file uploads (PDF, CSV, etc.), bot configuration images, user avatars, AI-generated images • **Access control:** Private buckets (anonymous GET = 403); access via short-lived, signed URLs (presigned URLs, typically 1–24 hours valid) • **CORS:** GET/HEAD allowed for all origins (security enforced by signature gating, not origin restriction)

2. Aufbewahrungsdauer während aktiver Nutzung · 2. Retention during active use

DEUTSCH	ENGLISH
Chatverläufe und Logs (Datenbank) • **Speicherdauer:** Maximal 90 Tage. Nach Ablauf dieser Frist werden Chatverläufe und Logs automatisch gelöscht, sofern keine gesetzliche Aufbewahrungspflicht besteht. • **Begründung:** Balancierte Aufbewahrung für Troubleshooting und Audit-Trail gemäß Art. 5 DSGVO (Speicherbegrenzung bei angemessener Aufbewahrungsdauer). Längere Aufbewahrung auf explizite Anforderung möglich.	**Chat histories and logs (database)** • **Retention period:** Maximum 90 days. After expiration of this period, chat histories and logs are automatically deleted unless statutory retention requirements apply. • **Rationale:** Balanced retention for troubleshooting and audit trail in compliance with Art. 5 GDPR (storage limitation with proportionate retention duration). Longer retention possible upon explicit request.
Datei-Uploads (Object Storage) • **Speicherdauer:** Maximal 90 Tage, solange nicht vorher vom Verantwortlichen gelöscht. Nach Ablauf werden Uploads automatisch aus dem aktiven Speicher entfernt. • **Versionierung:** Hetzner Object Storage hat Versioning aktiviert. Alte Versionen (Non-Current) werden nach 30 Tagen automatisch gelöscht. Die aktuelle Version bleibt erhalten (bis zur 90-Tage-Grenze).	**File uploads (object storage)** • **Retention period:** Maximum 90 days, unless deleted earlier by the Controller. After expiration, uploads are automatically removed from active storage. • **Versioning:** Hetzner Object Storage has versioning enabled. Old versions (non-current) are automatically deleted after 30 days. The current version is retained (until the 90-day limit).

3. Sicherung und Redundanz · 3. Backup and redundancy

DEUTSCH	ENGLISH
Datenbank-Backups (MySQL) • **Backup-Tool:** borgmatic (logische mysqldump-Archive) • **Ziel:** Hetzner Storage Box (offsite, SSH/sftp-basiert) • **Häufigkeit:** Täglich (um ca. 22:00 UTC) • **Aufbewahrung:** 7 tägliche Backups (ca. 7 Tage) + 4 wöchentliche Backups (ca. 4 Wochen) + 12 monatliche Backups (12 Monate) • **Verifikation:** Wöchentliche Wiederherstellungstests auf temporären Datenbanken (nicht-destruktiv, automatisiert) • **Zusätzlich:** Hetzner Cloud Backups (tägliche Snapshots des Servers, 7-Slot-Rotation) — Crash-Recovery, nicht als Daten-Restore-Quelle	**Database backups (MySQL)** • **Backup tool:** borgmatic (logical mysqldump archives) • **Destination:** Hetzner Storage Box (offsite, SSH/sftp-based) • **Frequency:** Daily (approx. 22:00 UTC) • **Retention:** 7 daily backups (approx. 7 days) + 4 weekly backups (approx. 4 weeks) + 12 monthly backups (12 months) • **Verification:** Weekly restore tests on temporary databases (non-destructive, automated) • **Additionally:** Hetzner Cloud Backups (daily server snapshots, 7-slot rotation) — crash recovery, not the primary data restore source
Object Storage Backups • **Versionierung in S3:** Versioning enabled; alte Versionen nach 30 Tagen automatisch gelöscht • **Off-Bucket Backup:** Täglich via rclone (S3 → Storage Box) • **Backup-Aufbewahrung:** Vollständige tägliche Snapshots unter `backups/object-storage//` ; gelöschte/veränderte Objekte in `backups/object-storage-history///` (historisches Tracking). History-Verzeichnisse älter als 90 Tage werden automatisch gelöscht. • **Restore:** Einzelne Objekte oder ganze Buckets können aus dem Storage Box Backup innerhalb des 90-Tage-Fensters wiederhergestellt werden • **Offsite-Replikation:** Konfigurierbar aber deaktiviert (kann auf Anforderung aktiviert werden)	**Object Storage Backups** • **S3 Versioning:** Versioning enabled; old versions automatically deleted after 30 days • **Off-bucket backup:** Daily via rclone (S3 → Storage Box) • **Backup retention:** Full daily snapshots under `backups/object-storage//` ; deleted/changed objects in `backups/object-storage-history///` (historical tracking). History directories older than 90 days are automatically deleted. • **Restore:** Individual objects or entire buckets can be restored from the Storage Box backup within the 90-day window • **Offsite replication:** Configurable but disabled (can be enabled on request)

4. Löschung nach Vertragskündigung · 4. Deletion upon contract termination

DEUTSCH	ENGLISH
Zeitrahmen: Nach Beendigung des Vertrags gemäß § 10 der AVV wird die Löschung oder Rückgabe durchgeführt. • **Datenbank:** Alle Chatverläufe, Logs und Metadaten des Verantwortlichen werden gelöscht oder auf Wunsch exportiert. • **Object Storage:** Alle Dateien und Uploads werden aus den Buckets gelöscht. • **Sicherungskopien:** Bestehende Backups (borgmatic-Archive in der Storage Box, Object Storage-Versionen) werden gelöscht, sofern keine gesetzliche Aufbewahrungspflicht besteht (z. B. Steuer- oder Revisionsgesetze). • **Löschverfahren:** Sichere Löschung (nicht einfach als gelöscht markiert, sondern physisch entfernt) • **Bestätigung:** Der Auftragsverarbeiter bestätigt die Löschung schriftlich.	**Timeline:** Upon contract termination, deletion or return is performed pursuant to § 10 of the DPA. • **Database:** All chat histories, logs, and metadata belonging to the Controller are deleted or exported upon request. • **Object Storage:** All files and uploads are deleted from the buckets. • **Backups:** Existing backups (borgmatic archives in Storage Box, Object Storage versions) are deleted unless statutory retention requirements apply (e.g. tax or audit laws). • **Deletion procedure:** Secure deletion (not merely marked as deleted, but physically removed) • **Confirmation:** The Processor provides written confirmation of deletion.

5. Datentrennung und Mandantenschutz · 5. Data segregation and tenant protection

DEUTSCH	ENGLISH
Logische Trennung: Alle Daten sind datenbankweit nach Verantwortlichem (User ID, Workspace ID) getrennt. SQL-Queries sind auf den berechtigten Namespace des jeweiligen Nutzers beschränkt. **Object Storage:** Buckets sind mandantenübergreifend (shared bucket), aber jedes Objekt ist mit einem eindeutigen Key versehen, der die Verantwortliche Entität identifiziert. Zugriff via signierte URLs (keine Cross-Tenant-Zugriffe durch URL-Tampering möglich).	**Logical segregation:** All data is separated at the database level by controller (user ID, workspace ID). SQL queries are constrained to the authorized namespace of each user. **Object Storage:** Buckets are cross-tenant (shared bucket), but each object has a unique key identifying the responsible entity. Access via signed URLs (no cross-tenant access possible via URL tampering).

6. Kundendaten-Integration – Isolation und Verschlüsselung · 6. Customer Data Integration – Isolation and Encryption

DEUTSCH	ENGLISH
Anwendungsbereich: Wenn Kundendaten außerhalb der Kernfunktionen (Chat und Bots) in Integrationsdiensten verarbeitet werden — beispielsweise in Business Intelligence, Datenanalysen oder anderen Custom-Integrationen — gelten zusätzliche Schutzmaßnahmen: • **Logische Datentrennung:** Jeder Kunde erhält eine eigene, isolierte Datenspeicher-Instanz (logische oder physische Segregation je nach Service-Architektur). Datensätze eines Kunden sind nicht durch SQL-Queries oder API-Zugriffe anderer Kunden erreichbar. • **Verschlüsselung auf Speicherebene:** Alle Kundendaten werden durch Verschlüsselung auf der Speicherebene (AES-256 oder äquivalent) geschützt. Dies gilt unabhängig von der zugrundeliegenden Datenbank-Technologie (SQL, NoSQL, Dateisysteme). • **Zugriffskontrolle:** Datenbank-Credentials sind kundenspezifisch konfiguriert. Admin-Zugriffe erfolgen nur mit expliziter Autorisierung und werden auditiert. • **Abfrage-Sicherung:** Datenbankabfragen sind automatisch auf den Datenbestand des jeweiligen Kunden gefiltert. Es existiert kein generischer Cross-Customer-Query-Pfad. • **Technologie-Neutralität:** Diese Maßnahmen sind unabhängig von der verwendeten Datenbank-Technologie (z. B. SQLite, PostgreSQL, MySQL) implementierbar und werden bei zukünftigen Migrationen beibehalten.	**Scope:** When customer data is processed in integration services outside core functions (chat and bots) — for example, in Business Intelligence, data analysis, or other custom integrations — additional safeguards apply: • **Logical data separation:** Each customer maintains its own isolated data storage instance (logical or physical segregation depending on service architecture). One customer's records are not accessible via SQL queries or API calls from other customers. • **Encryption at storage layer:** All customer data is protected via encryption at the storage layer (AES-256 or equivalent). This applies regardless of the underlying database technology (SQL, NoSQL, filesystems). • **Access control:** Database credentials are configured per-customer. Admin access occurs only with explicit authorization and is audited. • **Query isolation:** Database queries are automatically scoped to the respective customer's data. No generic cross-customer query path exists. • **Technology neutrality:** These measures are implementable independently of the database technology used (e.g. SQLite, PostgreSQL, MySQL) and will be retained during future migrations.

7. Compliance mit Art. 32 und Art. 17 DSGVO · 7. Compliance with Art. 32 and Art. 17 GDPR

DEUTSCH	ENGLISH
• **Art. 32 (Sicherheit):** Verschlüsselung in Transit (TLS 1.2+) und at Rest (AES-256), Zugriffskontrollen, Logging, Monitoring, regelmäßige Backups und Wiederherstellungstests. • **Art. 17 (Recht auf Löschung):** Der Verantwortliche kann jederzeit eine vollständige Löschung anfordern. Nach Vertragskündigung wird automatisch gelöscht (siehe § 10 und Punkt 4 oben). • **Audit:** Die Backup- und Löschverfahren werden jährlich überprüft und bei Bedarf aktualisiert.	• **Art. 32 (Security):** Encryption in transit (TLS 1.2+) and at rest (AES-256), access controls, logging, monitoring, regular backups and restore tests. • **Art. 17 (Right to erasure):** The Controller may request complete deletion at any time. Upon contract termination, deletion is performed automatically (see § 10 and point 4 above). • **Audit:** Backup and deletion procedures are reviewed annually and updated as necessary.

8. Kontakt bei Fragen · 8. Contact for inquiries

DEUTSCH	ENGLISH
Fragen zum Speicher-, Backup- oder Löschkonzept richten Sie an: HybridAI GmbH Datenschutz: privacy@hybridai.one Datenschutzbeauftragter: Gregor Klar (klar@brainosphere.de)	For inquiries about storage, backup, or deletion procedures, please contact: HybridAI GmbH Data Protection: privacy@hybridai.one Data Protection Officer: Gregor Klar (klar@brainosphere.de)

Anlage 7 – Sicherheits- und Compliance-Erklärung · Annex 7 – Security and Compliance Statement

DEUTSCH	ENGLISH
Sicherheits- und Compliance-Erklärung Diese Anlage dokumentiert den Status der Informationssicherheit und des Compliance-Programmes bei HybridAI GmbH zum Zeitpunkt dieser Vereinbarung (Stand: 2026-08-08). Alle genannten Zertifizierungen, Verfahrensstände und Compliance-Status gelten ab diesem Datum und sollten regelmäßig überprüft werden.	**Security and Compliance Statement** This annex documents the status of information security and compliance programme at HybridAI GmbH at the time of execution of this Agreement (as of 2026-08-08). All certifications, procedure status, and compliance details mentioned herein are current as of this date and should be reviewed periodically.

1. Sicherheits-Audit und Bewertung · Security audit and assessment

DEUTSCH	ENGLISH
Durchgeführte Bewertungen: • **Automatisiertes Security Baseline Scan (2026-07-27):** ◦ Python-Abhängigkeiten: 18 von 19 kritischen/hohen CVEs remediert (OSV.dev) ◦ Frontend-Abhängigkeiten: 0 Sicherheitslücken (npm audit) ◦ Statische Analyse (bandit): 0 wahre positiven Ergebnisse unter ~160.000 Zeilen Produktionscode **Status:** Dies ist ein **automatisiertes Basis-Scan** (Dependency-Analyse + SAST), **kein Penetration Test**. Ein Penetration Test durch einen externen Dienstleister ist geplant und wird auf Anfrage bereitgestellt.	**Assessments conducted:** • **Automated Security Baseline Scan (2026-07-27):** ◦ Python dependencies: 18 of 19 critical/high CVEs remediated (OSV.dev) ◦ Frontend dependencies: 0 security vulnerabilities (npm audit) ◦ Static analysis (bandit): 0 true positives across ~160,000 lines of production code **Status:** This is an **automated baseline scan** (dependency analysis + SAST), **not a penetration test**. A third-party penetration test is planned and will be provided on request.

2. ISO 27001:2022 Programm · ISO 27001:2022 programme

DEUTSCH	ENGLISH
Programmstatus: • **Programmstart:** 2025 • **Selbstbewertung (2025-12-08):** 85% der 93 Annex-A-Kontrollen • **Ziel-Zertifizierung:** 31. Dezember 2027 • **Aktuelle Zertifizierung:** Keine (externe Audit noch nicht durchgeführt) **Implementierte Kontrollen (verifiziert):** • • Audit Logging System (seit 2025-09-02): Administratorische Aktionen, Admin-Übernahmen, User-Switches, Monitoring-Dashboard, CSV-Export für Compliance-Reports • • Access Control: Bot-Zugriff mit gemeinsamen Secrets, Fehlerversuche protokolliert, Secret-Rotation • • Incident Management: Automatische Erkennung, strukturierter Antwort-Workflow, Tracking und Post-Incident-Review • • Externe Überwachung: ServerGuard24 (24/7 Uptime + Security), Betterstack (Infrastruktur + Logs), Sentry.io (Anwendungsfehler) • • Server-Härtung: Fail2ban, UFW Firewall, Wazuh SIEM, wöchentliche Scans (Lynis, rkhunter, chkrootkit) • • Credential Management: Bitwarden (2025-10-06): Zero-Knowledge-Architektur, MFA auf Vault-Zugriff, sichere Team-Freigabe • • Privacy-Steuerungen (Widget): Client-seitige PII-Erkennung, Server-seitige Redaktion, Privacy-Mode, AI-Safety-Hinweise	**Programme status:** • **Programme start:** 2025 • **Self-assessment (2025-12-08):** 85% of 93 Annex A controls • **Target certification:** 31 December 2027 • **Current certification:** None (external audit not yet conducted) **Implemented controls (verified):** • • Audit Logging System (since 2025-09-02): Administrative actions, admin takeovers, user switches, monitoring dashboard, CSV export for compliance reporting • • Access Control: Bot access with shared secrets, failed attempts logged, secret rotation • • Incident Management: Automated detection, structured response workflow, tracking and post-incident review • • External Monitoring: ServerGuard24 (24/7 uptime + security), Betterstack (infrastructure + logs), Sentry.io (application errors) • • Server Hardening: Fail2ban, UFW Firewall, Wazuh SIEM, weekly scans (Lynis, rkhunter, chkrootkit) • • Credential Management: Bitwarden (2025-10-06): Zero-knowledge architecture, MFA on vault access, secure team sharing • • Privacy Controls (Widget): Client-side PII detection, server-side redaction, privacy mode, AI safety disclaimers

3. Technische und organisatorische Maßnahmen · Technical and organisational measures

DEUTSCH	ENGLISH
Die detaillierten TOMs sind in Anlage 3 dieser AVV dokumentiert. Zusammengefasst: • **Verschlüsselung:** TLS 1.2+ in Transit, AES-256 in Ruhe • **Zugangssteuerung:** Rollenbasierte Rechte, MFA für Admin-Zugriffe, regelmäßige Überprüfungen, Need-to-Know-Prinzip • **PII-Maskierung:** Verfügbare Funktion (optional aktiviert in Anlage 1) zur Maskierung identifizierender Daten vor Weiterleitung an externe KI-Dienste • **Protokollierung:** Mindestens 12 Monate, automatisierte Anomalie-/Angriffserkennung • **Datensicherung:** 7 tägliche Backups + 4 wöchentliche + 12 monatliche, wöchentliche Wiederherstellungstests • **Infrastruktur:** Server in DE/EU (Hetzner), Patch-Management, System-Härtung, sichere Konfigurationen • **Mandanten-Trennung:** Logische und technische Trennung nach Zweck • **Datenlebenszyklus:** Löschung auf Anforderung oder nach Fristablauf; sichere Löschverfahren	The detailed TOMs are documented in Annex 3 of this Agreement. In summary: • **Encryption:** TLS 1.2+ in transit, AES-256 at rest • **Access control:** Role-based rights, MFA for admin access, regular reviews, need-to-know principle • **PII masking:** Available function (optionally activated in Annex 1) to mask identifying data before forwarding to external AI services • **Logging:** Minimum 12 months, automated anomaly/intrusion detection • **Backup:** 7 daily backups + 4 weekly + 12 monthly, weekly restore tests • **Infrastructure:** Servers in DE/EU (Hetzner), patch management, hardening, secure configurations • **Tenant separation:** Logical and technical segregation by purpose • **Data lifecycle:** Deletion on request or after retention period; secure deletion procedures

4. Compliance-Framework · Compliance framework

DEUTSCH	ENGLISH
GDPR / DSGVO: Vollständig implementiert. Datenschutz-Richtlinien, Einwilligungsverwaltung, Datenschutzrecht-Anfragen, Datenportabilität, Löschung. **Unterauftragsverarbeiter-Management:** Alle in Anlage 2 genannten Sub-Prozessoren haben Auftragsverarbeitungsverträge (oder gleichwertige Vertragsbedingungen mit Standard Contractual Clauses). Periodische Compliance-Überprüfungen durchgeführt. **Datenschutzverletzungen:** Meldung an Verantwortlichen innerhalb von 24 Stunden nach Kenntnis (§ 9 dieser AVV). Incident-Management-System implementiert und getestet. **Datenexpor und Import:** Kontrollierte Prozesse mit Protokollierung; Export nur auf Anforderung des Verantwortlichen oder bei Vertragsende.	**GDPR:** Fully implemented. Privacy policies, consent management, data subject rights, data portability, deletion. **Sub-processor management:** All sub-processors listed in Annex 2 have data processing agreements (or equivalent contractual terms including Standard Contractual Clauses). Periodic compliance checks performed. **Personal data breaches:** Notification to Controller within 24 hours of discovery (§ 9 of this Agreement). Incident management system implemented and tested. **Data export and import:** Controlled processes with logging; export only on request of Controller or upon contract termination.

5. Audit und Nachweis · Audit and evidence

DEUTSCH	ENGLISH
Verfügbare Nachweise (implementiert und verifiziert): • • Automatisierter Security Baseline Scan-Bericht (2026-07-27, OSV.dev + npm audit + bandit) • • ISO 27001:2022 Self-Assessment-Checkliste (2025-12-08): 85% der 93 Annex-A-Kontrollen umgesetzt • • ISMS-Dokumentation: 36 Dokumente (Policies, Procedures, Risk Register, Asset Inventory, etc.) • • Audit-Logs der letzten 12 Monate (strukturierte Protokollierung, Anomalieerkennung) **Geplante Nachweise (noch nicht verfügbar):** • • ➡ SOON Externe Penetration Test durch Drittanbieter: Geplant, auf Anfrage verfügbar (Termin: TBD) • • ➡ SOON ISO 27001:2022 externe Zertifizierung: Ziel 31. Dezember 2027 (geplantes externes Audit in 2027) **Kontrollrechte (§ 8):** Der Verantwortliche kann Audits einleiten; HybridAI arbeitet vollständig mit unabhängigen Prüfern zusammen. Geschäftsgeheimnisse bleiben geschützt.	**Evidence available (implemented and verified):** • • Automated Security Baseline Scan report (2026-07-27, OSV.dev + npm audit + bandit) • • ISO 27001:2022 self-assessment checklist (2025-12-08): 85% of 93 Annex A controls implemented • • ISMS documentation: 36 documents (policies, procedures, risk register, asset inventory, etc.) • • Audit logs for the past 12 months (structured logging, anomaly detection) **Planned evidence (not yet available):** • • ➡ SOON External penetration test by third-party vendor: Planned, available on request (schedule: TBD) • • ➡ SOON ISO 27001:2022 external certification: Target 31 December 2027 (planned external audit in 2027) **Audit rights (§ 8):** The Controller may initiate audits; HybridAI cooperates fully with independent auditors. Trade secrets remain protected.

6. Bekannte Einschränkungen · Known limitations

DEUTSCH	ENGLISH
Im Interesse der Transparenz werden folgende bekannte Einschränkungen offen kommuniziert: • **End-Benutzer-MFA:** Derzeit nicht verfügbar (Verifizierung per E-Mail/SMS). Multi-Faktor-Authentifizierung für Endkunden ist für ein zukünftiges Release geplant. • **Content Security Policy:** Derzeit im Report-Only-Modus (nicht erzwingend). Aufbau einer vollständigen Allow-List ist in Arbeit. • **Externe Penetration Test:** Noch nicht durchgeführt. Ein dritter Dienstleister wird beauftragt und sein Bericht zur Verfügung gestellt. • **ISO 27001 Zertifizierung:** Noch nicht zertifiziert. Selbstbewertung 85%; externes Audit geplant für 2027. Alle diese Punkte sind **auf der Roadmap** und der Verantwortliche wird über Fortschritte informiert. Keine dieser Einschränkungen ist ein Sicherheitsdefekt; sie sind geplante Erweiterungen des Compliance-Programmes.	In the interest of transparency, the following known limitations are communicated openly: • **End-user MFA:** Currently not available (verification via email/SMS). Multi-factor authentication for end customers is planned for a future release. • **Content Security Policy:** Currently in report-only mode (not enforced). Building a complete allow-list is in progress. • **External penetration test:** Not yet conducted. A third-party vendor will be engaged and their report provided. • **ISO 27001 certification:** Not yet certified. Self-assessment 85%; external audit planned for 2027. All of these are **on the roadmap** and the Controller will be informed of progress. None of these limitations is a security defect; they are planned enhancements to the compliance programme.

7. Kontakt für Sicherheits-/Compliance-Fragen · Contact for security/compliance questions

DEUTSCH	ENGLISH
Information Security Officer: Stephan Noller E-Mail: privacy@hybridai.one Zeitzone: Europe/Berlin Anfragen zu Audit-Nachweisen, Compliance-Status oder Sicherheits-Maßnahmen werden innerhalb von 5 Arbeitstagen beantwortet.	**Information Security Officer:** Stephan Noller Email: privacy@hybridai.one Timezone: Europe/Berlin Inquiries regarding audit evidence, compliance status or security measures will be answered within 5 business days.

Hinweis / Note: *Diese Erklärung gilt zum Zeitpunkt der Annahme dieser AVV und wird mindestens jährlich aktualisiert oder bei wesentlichen Änderungen der Sicherheitslage mitgeteilt. Ein Exemplar wird in den Compliance-Akten verwahrt und ist auf Anfrage für Audit-Zwecke verfügbar. · This statement is valid as of the execution date of this Agreement and will be updated at least annually or communicated if material changes to the security posture occur. A copy will be retained in compliance records and is available on request for audit purposes.*

Anlage 8 – PII-Maskierung und Datenschutz-Filterung · Annex 8 – PII Masking and Data Protection Filtering

DEUTSCH	ENGLISH
PII-Maskierung und Datenschutz-Filterung Dieses Dokument beschreibt die technische Implementierung von zwei unabhängigen PII-Schutzmaßnahmen: reversible Maskierung für die LLM-Übermittlung (PiiVault) und irreversible Filterung für Logs und gespeicherte Inhalte (mask_pii).	**PII Masking and Data Protection Filtering** This document describes the technical implementation of two independent PII protection measures: reversible masking for LLM transmission (PiiVault) and irreversible filtering for logs and stored content (mask_pii).

1. PII-Erkennungsmuster · 1. PII Detection Patterns

DEUTSCH	ENGLISH
Erkannte Datentypen (Regex-basiert): • **EMAIL:** Standard-Regex für E-Mail-Adressen (z.B. `user@example.com`) • **IP:** IPv4-Adressen (z.B. `192.168.1.1`) • **SSN:** US Social Security Numbers im Format XXX-XX-XXXX • **CARD:** Kreditkartennummern (4-4-4-N Format, z.B. `1234-5678-9012-3456`) • **IBAN:** Internationale Bankkontonummern (z.B. `DE89370400440532013000`) • **PHONE:** Telefonnummern mit mindestens 7 Ziffern und Trennzeichen (z.B. `+49 123 456789`) **Personennamen (NER-basiert):** • **Standard:** Deutsch — spaCy German NER-Pipeline (Modell: `de_core_news_md`) • **Label:** PER (PERSON) Entities • **Granularität:** Einzelne Wörter bis Mehrwort-Phrases (z.B. „Hans Müller") • **Weitere Sprachen:** Auf Anfrage verfügbar (z.B. Englisch via `en_core_web_md`); nicht aktiviert per Default • **Grenze:** NER läuft nur auf Texten ≤ 20,000 Zeichen (zur Latenzbegrenzung); längere Texte nutzen nur Regex-Patterns • **Fehlgeschlagensfallverhalten:** Wenn spaCy nicht verfügbar ist, werden nur Regex-Patterns verwendet (kein Fehler, fehlertolerantes Abbau)	**Detected data types (regex-based):** • **EMAIL:** Standard regex for email addresses (e.g. `user@example.com`) • **IP:** IPv4 addresses (e.g. `192.168.1.1`) • **SSN:** US Social Security Numbers in format XXX-XX-XXXX • **CARD:** Credit card numbers (4-4-4-N format, e.g. `1234-5678-9012-3456`) • **IBAN:** International bank account numbers (e.g. `DE89370400440532013000`) • **PHONE:** Phone numbers with ≥7 digits and separators (e.g. `+49 123 456789`) **Person names (NER-based):** • **Standard:** German — spaCy German NER pipeline (model: `de_core_news_md`) • **Label:** PER (PERSON) entities • **Granularity:** Single words to multi-word phrases (e.g. "Hans Müller") • **Additional languages:** Available on request (e.g. English via `en_core_web_md`); not activated by default • **Limit:** NER runs only on texts ≤20,000 characters (latency bound); longer texts use regex-patterns only • **Failure mode:** If spaCy is unavailable, regex-patterns are used only (no error, graceful degradation)

2. Reversible Maskierung für LLM-Übermittlung · 2. Reversible Masking for LLM Transmission

DEUTSCH	ENGLISH
Konzept (PiiVault): Jeder distinct PII-Wert wird durch einen eindeutigen, nummerierten Platzhalter ersetzt: • Erste E-Mail `john@example.com` → `<EMAIL_1>` • Zweite E-Mail `jane@example.com` → `<EMAIL_2>` • Wenn `john@example.com` nochmal vorkommt → wiederverwendet `<EMAIL_1>` (Deduplizierung) • Name „Hans Müller" → `<NAME_1>` **Speicherung (Pro Anfrage):** • **Mapping:** Token ↔ Originalwert wird im Speicher (PiiVault-Objekt) pro Request gehalten • **Keine Redis:** Keine Cross-Request-Persistierung; jeder Turn startet mit leerem Vault • **History:** Historische Chats werden mit echten Werten gespeichert und bei jedem Turn neu re-maskiert • **Stabilität:** Token-Nummern sind innerhalb eines Requests stabil, aber nicht über Turns hinweg **Workflow (LLM-Round-Trip):** 1. User-Eingabe kommt rein → PiiVault.mask(text) tokenisiert erkannte PII 2. Für erfolgreich erkannte und maskierte Werte werden Platzhalter an LLM übermittelt (z.B. „Kontaktiere <EMAIL_1>") — Originalwerte werden NICHT übermittelt 3. LLM-Response mit Platzhaltern kommt zurück (z.B. „Ich antworte <EMAIL_1>") 4. StreamRestorer oder PiiVault.restore() ersetzt Platzhalter mit Originalwerten BEVOR User sie sieht 5. User sieht echte Werte in der Response; erkannte PII-Werte wurden nicht an LLM-Provider übermittelt **Anweisung an LLM (System Prompt):** Beim Starten der Maskierung wird ein PRIVACY-Block zum System Prompt hinzugefügt, der das LLM instruiert, Platzhalter exakt zu reproduzieren (keine Variation, keine Erfindung neuer Platzhalter).	**Concept (PiiVault):** Each distinct PII value is replaced with a unique, numbered placeholder: • First email `john@example.com` → `<EMAIL_1>` • Second email `jane@example.com` → `<EMAIL_2>` • If `john@example.com` appears again → reuse `<EMAIL_1>` (deduplication) • Name "Hans Müller" → `<NAME_1>` **Storage (per request):** • **Mapping:** Token ↔ original value stored in memory (PiiVault object) per request • **No Redis:** No cross-request persistence; each turn starts with an empty vault • **History:** Historical chats stored with real values and re-masked from scratch each turn • **Stability:** Token numbers stable within a request but NOT across turns **Workflow (LLM round-trip):** 1. User input arrives → PiiVault.mask(text) tokenizes PII 2. LLM sees only placeholders (e.g. "Contact <EMAIL_1>") — for successfully detected and masked values, original values are not transmitted 3. LLM response with placeholders returns (e.g. "I'll reply to <EMAIL_1>") 4. StreamRestorer or PiiVault.restore() replaces placeholders with originals BEFORE user sees them 5. User sees real values in response; for successfully masked values, the LLM provider did not have access to the original data **LLM Instruction (system prompt):** When masking is active, a PRIVACY block is prepended to the system prompt instructing the LLM to reproduce placeholders exactly (no variation, no inventing new placeholders).

3. Streaming & Split-Token-Handling · 3. Streaming & Split-Token Handling

DEUTSCH	ENGLISH
Problem: LLM-Responses kommen als SSE-Stream an (z.B. Chunk 1: `"Kontaktiere <EMA"`, Chunk 2: `"IL_1> sofort"`). Naives Restore pro Chunk würde den Split-Token nicht erkennen. **Lösung (StreamRestorer):** • Buffert ein trailing Fragment nach jedem Chunk (z.B. `"<EMA"`), das Teil eines Platzhalters sein könnte • Wartet auf den nächsten Chunk, um zu sehen, ob der Platzhalter vervollständigt wird • Wenn vollständig → restore; wenn nicht (z.B. `"< Wort"`), emit den gepufferten Text unvermaskiert • Kein State über SSE-Grenzen → StreamRestorer wird pro Response neu erstellt	**Problem:** LLM responses arrive as SSE streams (e.g. chunk 1: `"Contact <EMA"`, chunk 2: `"IL_1> now"`). Naive restore-per-chunk would miss the split token. **Solution (StreamRestorer):** • Buffers a trailing fragment after each chunk (e.g. `"<EMA"`) that could be part of a placeholder • Waits for the next chunk to see whether the placeholder completes • If complete → restore; if not (e.g. `"< word"`), emit the buffered text unmasked • No state across SSE boundaries → StreamRestorer created fresh per response

4. Irreversible Filterung für Logs und Speicherung · 4. Irreversible Filtering for Logs and Storage

DEUTSCH	ENGLISH
Konzept (mask_pii): One-Way Masking für Logs, Fehler-Messages und gespeicherte Inhalte. Jeder PII-Typ wird durch einen generischen Platzhalter ersetzt: • Alle E-Mails → `<EMAIL>` (nicht numeriert) • Alle IPs → `<IP>` • Alle Telefonnummern → `<PHONE>` • Etc. für SSN, CARD, IBAN **Originalwerte werden GELÖSCHT** — es gibt kein Mapping zur Wiederherstellung. **Aktivierung:** Flag `pii_safety_enabled` (unabhängig von `llm_pii_masking_enabled`) • Kontrolliert die Filterung von Logs, Fehler-Traces und Debug-Ausgaben • Verhindert, dass sensible Daten in Log-Dateien (z.B. journalctl, syslog) landen • Kann aktiviert sein, während LLM-Maskierung deaktiviert ist (oder umgekehrt) **Anwendung:** • Alle Log-Ausgaben gehen durch `mask_pii()` bevor sie geschrieben werden • Fehler-Messages an Admins sind gefiltert (aber lesbar — generische Platzhalter) • Datenbankeinträge (z.B. `conversation_sessions`, `user_activity`) können gefiltert gespeichert werden	**Concept (mask_pii):** One-way masking for logs, error messages, and stored content. Each PII type replaced with a generic placeholder: • All emails → `<EMAIL>` (not numbered) • All IPs → `<IP>` • All phone numbers → `<PHONE>` • Etc. for SSN, CARD, IBAN **Original values are DELETED** — no mapping exists for restoration. **Activation:** Flag `pii_safety_enabled` (independent of `llm_pii_masking_enabled`) • Controls filtering of logs, error traces, and debug output • Prevents sensitive data from ending up in log files (e.g. journalctl, syslog) • Can be active while LLM masking is disabled (or vice versa) **Application:** • All log output passes through `mask_pii()` before writing • Error messages to admins are filtered (but readable — generic placeholders) • Database entries (e.g. `conversation_sessions`, `user_activity`) can be filtered on storage

5. Integration mit LLM-Providern · 5. Integration with LLM Providers

DEUTSCH	ENGLISH
Unterstützte Provider: • OpenAI • Anthropic (Claude) • Google (Gemini) • Mistral • Grok, vLLM, HaiGPU1 (erben OpenAI-Implementierung) **Aktivierung pro Anfrage:** • PiiVault wird bei Anfragestart instanziiert (falls `llm_pii_masking_enabled`) • Alle Provider nutzen die gleiche Vault-Instanz für diese Anfrage • PRIVACY-Instruction wird in den System Prompt eingefügt • Eingabe und Zwischeneingaben (nach Tools) werden maskiert • Response wird via StreamRestorer (Streaming) oder Vault.restore() (non-streaming) unmaskiert **Tool Calls (noch ausstehend):** Derzeit erhalten Tools maskierte (Platzhalter-)Argumente. Unmaskierung der Tool-Ergebnisse und Re-Maskierung für die nächste LLM-Runde ist ein offener Ausbau.	**Supported providers:** • OpenAI • Anthropic (Claude) • Google (Gemini) • Mistral • Grok, vLLM, HaiGPU1 (inherit OpenAI implementation) **Per-request activation:** • PiiVault instantiated at request start (if `llm_pii_masking_enabled`) • All providers use the same vault instance for this request • PRIVACY instruction inserted into system prompt • Input and intermediate inputs (after tools) are masked • Response unmasked via StreamRestorer (streaming) or Vault.restore() (non-streaming) **Tool calls (pending):** Currently, tools receive masked (placeholder) arguments. Unmasking tool results and re-masking for the next LLM round is an open enhancement.

6. Konfiguration und Kontrolle · 6. Configuration and Control

DEUTSCH	ENGLISH
Zwei unabhängige Flags (pro Bot): • **`pii_safety_enabled`:** One-way Filterung für Logs/ Speicherung (mask_pii). Default: off. • **`llm_pii_masking_enabled`:** Reversible Maskierung für LLM-Übermittlung (PiiVault). Default: off. Umfasst auch Deutsche Personennamen (spaCy NER, no separate flag). **Wo konfigurieren:** • Bot-Settings im Admin-Interface • Wirkung: Sofort ab nächster Anfrage • Keine Cache-Auswirkungen (re-masking läuft bei jedem Turn) **Audit & Compliance:** • Aktivierungsstatus wird in der DPA (Anlage 1) dokumentiert • Flag-Änderungen werden geloggt (unter Beachtung der `pii_safety_enabled`-Regel)	**Two independent flags (per bot):** • **`pii_safety_enabled`:** One-way filtering for logs/storage (mask_pii). Default: off. • **`llm_pii_masking_enabled`:** Reversible masking for LLM transmission (PiiVault). Default: off. Includes German person names (spaCy NER, no separate flag). **Where to configure:** • Bot settings in admin interface • Effect: Immediate from next request • No cache impact (re-masking runs each turn) **Audit & compliance:** • Activation status documented in DPA (Annex 1) • Flag changes logged (observing the `pii_safety_enabled` rule)

7. Grenzen und Bekannte Einschränkungen · 7. Limits and Known Limitations

DEUTSCH	ENGLISH
Wichtiger Disclaimer: Diese Maskierung ist ein Best-Effort-Schutzmaßnahme, **keine garantierte Vollabdeckung**. Sie schützt erkannte PII-Muster (Regex) und deutsche Personennamen (NER), aber: • Nicht alle potenziellen PII kann erkannt werden (zB Firmennamen, Kontextuelle PII) • Maskierung erfolgt nur auf erkannte Muster; unbekannte PII-Formen werden nicht behandelt • **Fail-closed:** Bei Fehler der Maskierungslogik wird die Übermittlung abgebrochen; der Nutzer erhält eine neutrale Fehlermeldung und wird aufgefordert, den Request später zu wiederholen **Technische Grenzen:** • **NER-Grenze:** Deutsche Personennamen werden nur auf Texten < 20.000 Zeichen erkannt (Latenzbegrenzung); längere Texte verwenden nur Regex • **Regex-Abdeckung:** Email, IP, SSN, CARD, IBAN, PHONE-Patterns folgen Standard-Regex und können Edge Cases nicht abdecken (zB ungewöhnliche Formate) • **spaCy-Ausfallverhalten:** Wenn `de_core_news_md` nicht geladen ist, werden nur Regex-Patterns verwendet (kein Fehler, graceful degradation) • **LLM-Treue:** Wenn das LLM einen Platzhalter mangelhaft reproduziert oder erfindet (z.B. `<EMAIL_1a>`), kann dieser Wert nicht automatisch wiederhergestellt werden • **Language-Spezifität:** Person-Namenerkennung ist auf Deutsch optimiert; andere Sprachen auf Anfrage verfügbar (zZ. nicht aktiviert) • **Cross-Turn-Stabilität:** Token-Nummern sind nicht über Turns hinweg stabil; Geschichte wird immer neu re-maskiert	**Important disclaimer:** This masking is a best-effort protective measure, **not guaranteed complete coverage**. It protects detected PII patterns (regex) and German person names (NER), but: • Not all potential PII can be detected (e.g. company names, contextual PII) • Masking occurs only on recognized patterns; unknown PII forms are not handled • **Fail-closed:** If masking logic fails (error/exception), transmission is aborted; the user receives a neutral error message and is asked to retry the request later **Technical limits:** • **NER limit:** German person names detected only on texts <20,000 chars (latency bound); longer texts use regex only • **Regex coverage:** Email, IP, SSN, CARD, IBAN, PHONE patterns follow standard regex and may not cover edge cases (e.g. unusual formats) • **spaCy failure mode:** If `de_core_news_md` model not loaded, regex-patterns used only (no error, graceful degradation) • **LLM fidelity:** If LLM poorly reproduces or invents a placeholder (e.g. `<EMAIL_1a>`), that value cannot be automatically restored • **Language specificity:** Person-name detection optimized for German; other languages available on request (currently not activated) • **Tool arguments:** Tools currently receive masked arguments; unmasking before tool execution is pending • **Cross-turn stability:** Token numbers not stable across turns; history always re-masked from scratch