AUFTRAGSVERARBEITUNGSVERTRAG · ART. 28 DSGVO

Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO

Version 1.6 · Stand: 6. November 2026 · ersetzt Version 1.5 (24. September 2026)

anymize GmbH · Schauenburgerstr. 116 · 24118 Kiel · Deutschland · datenschutz@anymize.ai

anymize

ANYMIZE GMBH · SCHAUENBURGERSTR. 116 · 24118 KIEL · DEUTSCHLAND

Handelsregister AG Kiel HRB 29239 KI · Geschäftsführer Nikolai Raitschew, Raitschin Raitschew · Datenschutzbeauftragter Manuel Langeheinecke (digitalNORD GmbH) · datenschutz@anymize.ai

Vertragsschluss ohne Unterschrift

Dieser Auftragsverarbeitungsvertrag tritt automatisch in Kraft, sobald der Kunde

1. ein Nutzerkonto bei anymize erstellt und die AGB akzeptiert, oder
2. den Service anymize erstmalig nutzt.

Eine gesonderte Unterzeichnung durch die Parteien ist nicht erforderlich. Dieser AVV ist Bestandteil der Allgemeinen Geschäftsbedingungen (AGB) für den Service anymize. Auf Wunsch des Kunden schließen die Parteien diesen Vertrag zusätzlich in beidseitig unterzeichneter Form; der Inhalt bleibt dabei unverändert.

Der Kunde kann dieses Dokument für seine Unterlagen herunterladen und bei Bedarf mit seinen Unternehmensdaten ergänzen.

Präambel

Zwischen

anymize GmbH

Schauenburgerstr. 116, 24118 Kiel, Deutschland

Handelsregister: AG Kiel HRB 29239 KI

USt-IdNr.: DE461722394

Geschäftsführer: Nikolai Raitschew, Raitschin Raitschew

E-Mail: datenschutz@anymize.ai

Datenschutzbeauftragter: Manuel Langeheinecke (digitalNORD GmbH, Kiel), erreichbar unter datenschutz@anymize.ai oder postalisch: anymize GmbH, z. Hd. Datenschutzbeauftragter, Schauenburgerstr. 116, 24118 Kiel

– nachfolgend „Auftragsverarbeiter" –

und

dem Kunden (wie im Nutzerkonto registriert)

– nachfolgend „Verantwortlicher" –

wird folgender Auftragsverarbeitungsvertrag geschlossen:

---

§ 1

Gegenstand und Dauer der Verarbeitung

1.1 Gegenstand

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Rahmen der Nutzung des Services „anymize".

(2) Der Service umfasst die Pseudonymisierung personenbezogener Daten in Dokumenten und Eingaben durch Hash-Tokenisierung sowie die optionale De-Pseudonymisierung durch autorisierte Nutzer. Auf erster Ebene erfolgt eine Pseudonymisierung der personenbezogenen Daten. Die pseudonymisierten Daten werden anschließend, bei Nutzung der Chat-Funktion mit externen Modellen, an LLM-Anbieter übermittelt; für den LLM-Anbieter sind diese Daten ohne den beim Auftragsverarbeiter gespeicherten Zuordnungsschlüssel keiner natürlichen Person zuzuordnen. Der Auftragsverarbeiter behandelt diese Übermittlung gleichwohl als Verarbeitung personenbezogener Daten und bindet die LLM-Anbieter als Unterauftragsverarbeiter nach § 5.4 und Anlage 2 ein.

(3) Hinweis zur Terminologie: Im Service und im Marketing verwendet der Auftragsverarbeiter den Begriff „Anonymisierung" als vereinfachte Beschreibung. Rechtlich handelt es sich um eine Pseudonymisierung gemäß Art. 4 Nr. 5 DSGVO. Pseudonymisierte Daten bleiben personenbezogene Daten; die Pseudonymisierung ist eine Schutzmaßnahme im Sinne von Art. 25 und Art. 32 Abs. 1 lit. a DSGVO.

1.2 Dauer

(1) Dieser Vertrag gilt für die Dauer der Nutzung des Services anymize.

(2) Er endet automatisch mit Beendigung des Hauptvertrags (AGB) bzw. der Löschung des Nutzerkontos.

---

§ 2

Art und Zweck der Verarbeitung

2.1 Art der Verarbeitung

Die Verarbeitung umfasst folgende Tätigkeiten:

- Hochladen und temporäre Verarbeitung von Dokumenten
- Automatische Erkennung personenbezogener Daten mittels KI
- Ersetzung personenbezogener Daten durch Hash-Codes (Pseudonymisierung)
- Speicherung von Hash-Original-Paaren für die De-Pseudonymisierung
- Optionale Weitergabe eines pseudonymisierten Prompts oder Dokuments an die vom Verantwortlichen ausgewählten LLM-Anbieter (Chat-Funktion). Bei aktivierter

Pseudonymisierung erhalten externe LLM-Anbieter ausschließlich pseudonymisierte Inhalte. Der Verantwortliche kann die Pseudonymisierung für einzelne Anfragen deaktivieren oder sie für alle Nutzer seines Workspaces verbindlich vorgeben (§ 6.3 Abs. 3 und 6).

- Verarbeitung durch die vom Auftragsverarbeiter selbst betriebenen Modelle, sofern der Verantwortliche diese auswählt; in diesem Fall ist kein externer LLM-Anbieter beteiligt
- Wiederherstellung der Originaldaten auf Anfrage (De-Pseudonymisierung)
- Löschung der Daten nach Ablauf der gewählten Speicherfrist

2.2 Zweck der Verarbeitung

Die Verarbeitung erfolgt zum Zweck der

- DSGVO-konformen Nutzung von KI-/LLM-Diensten durch den Verantwortlichen,
- Pseudonymisierung personenbezogener Daten vor Weitergabe an Dritte,
- Ermöglichung der kontrollierten De-Pseudonymisierung durch den Verantwortlichen,
- Bereitstellung, Hosting, Betrieb und Wartung der Anwendung „anymize",
- Erbringung von Support-Leistungen und Bearbeitung von Kundenanfragen.

---

§ 3

Art der personenbezogenen Daten

3.1 Kategorien personenbezogener Daten

Der Service verarbeitet potenziell alle Kategorien personenbezogener Daten, die in den vom Verantwortlichen hochgeladenen Dokumenten oder Eingaben enthalten sind, insbesondere:

- Namen (Vor-, Nachname, Firmenname)
- Kontaktdaten (Adresse, E-Mail, Telefon)
- Identifikationsnummern (Personalausweis, Reisepass, Steuernummer, Sozialversicherungsnummer)
- Finanzielle Daten (Bankverbindung, Kreditkartennummer)
- Gesundheitsdaten (sofern in Dokumenten enthalten)
- Beschäftigungsdaten
- Sonstige in Dokumenten enthaltene personenbezogene Daten
- Technische Metadaten (IP-Adressen, Zeitstempel, Sitzungs-IDs, Protokolldaten, Login-Informationen)

3.2 Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)

(1) Der Service kann, abhängig von den durch den Verantwortlichen eingegebenen Inhalten, auch besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO verarbeiten, sofern der Verantwortliche solche Daten in die Anwendung eingibt oder hochlädt.

(2) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung, insbesondere für das Vorliegen einer Rechtsgrundlage gemäß Art. 6 DSGVO sowie, soweit einschlägig, einer Ausnahme nach Art. 9 Abs. 2 DSGVO, verantwortlich.

(3) Die Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt ausschließlich im Rahmen der vertraglich vereinbarten Leistungen und unter Anwendung der vereinbarten technischen und organisatorischen Maßnahmen, einschließlich der Pseudonymisierung vor einer etwaigen Weiterverarbeitung durch externe KI-Dienste, soweit der Verantwortliche die Pseudonymisierung nicht deaktiviert hat.

(4) Eine Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt nur insoweit, als der Verantwortliche diese eigenständig und bewusst in die Anwendung eingibt. Der Auftragsverarbeiter führt keine gezielte Erhebung solcher Daten durch.

(5) Für die Verarbeitung besonderer Kategorien in größerem Umfang (etwa Patientendaten) empfiehlt der Auftragsverarbeiter, ausschließlich seine eigenen Modelle zu nutzen, bei denen kein externer Modellanbieter beteiligt ist, und die übrigen Modelle über die Modellfreigabe auszuschließen. Auch pseudonymisierte Texte können solche Daten enthalten, weil Fachinhalte wie Diagnosen lesbar bleiben; die Vertragsbedingungen des AI-Gateways und mehrerer LLM-Anbieter sehen die gezielte Übermittlung besonderer Kategorien nicht vor.

§ 4

Kategorien betroffener Personen

Die betroffenen Personen umfassen alle Personen, deren Daten in den vom Verantwortlichen verarbeiteten Dokumenten enthalten sind, insbesondere:

- Kunden und Mandanten des Verantwortlichen
- Mitarbeiter und Bewerber
- Geschäftspartner und Lieferanten
- Zeugen und Beteiligte (bei Rechtsangelegenheiten)
- Versicherungsnehmer und Anspruchsteller
- Patientinnen und Patienten (bei Gesundheitsdaten)
- Sonstige in Dokumenten genannte Personen

§ 5

Pflichten des Auftragsverarbeiters

5.1 Weisungsgebundenheit

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen.

(2) Weisungen sind schriftlich oder in Textform zu erteilen. Einzelne Nutzungs- und Bedienhandlungen innerhalb der vereinbarten Funktionalitäten (z. B. Eingabe von Prompts, Pseudonymisierung personenbezogener Daten, Auswahl eines Modells) gelten als Abruf der vereinbarten Leistung und nicht als gesonderte Weisung im Sinne von Art. 28 Abs. 3 lit. a DSGVO.

(3) Mündliche Weisungen sind vom Verantwortlichen unverzüglich in Textform zu bestätigen. Der Auftragsverarbeiter kann die Ausführung bis zur Bestätigung zurückstellen.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt.

5.2 Vertraulichkeit

(1) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten.

(3) Alle Mitarbeitenden mit Zugang zu personenbezogenen Daten werden regelmäßig im Datenschutz geschult.

5.3 Sicherheit der Verarbeitung

(1) Der Auftragsverarbeiter hat die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung dokumentiert und stellt die Dokumentation dem Verantwortlichen zur Prüfung zur Verfügung.

(2) Der Auftragsverarbeiter hat die Sicherheit gemäß Art. 28 Abs. 3 lit. c und Art. 32 DSGVO, insbesondere in Verbindung mit Art. 5 DSGVO, herzustellen. Einzelheiten regelt Anlage 1.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragsverarbeiter darf einzelne Maßnahmen ändern oder durch andere ersetzen, sofern das Sicherheitsniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

(4) Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen.

5.4 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt hiermit eine allgemeine Genehmigung zur Beauftragung der in Anlage 2 genannten Unterauftragsverarbeiter.

(2) Anlage 2 unterscheidet ständig eingesetzte Unterauftragsverarbeiter (Abschnitt A) und nutzungsabhängige Unterauftragsverarbeiter (Abschnitt B). Nutzungsabhängige Unterauftragsverarbeiter, insbesondere LLM-Anbieter, werden nur tätig, wenn der Verantwortliche oder seine Nutzer das jeweilige Modell auswählen. Der Verantwortliche kann die Auswahl der verfügbaren Modelle und Anbieter für seinen Workspace einschränken. Eine aktuelle Liste ist zudem jederzeit unter https://anymize.ai/legal/unterauftragsverarbeiter einsehbar.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen bezüglich der Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern per E-Mail an die im Nutzerkonto hinterlegte Adresse mindestens 30 Tage im Voraus.

(4) Der Verantwortliche kann der beabsichtigten Änderung innerhalb von 14 Tagen nach Zugang der Information in Textform widersprechen. Eine Begründung ist nicht erforderlich. Erfolgt innerhalb der Widerspruchsfrist kein Widerspruch, gilt die Änderung als genehmigt.

(5) Widerspricht der Verantwortliche, wird der neue Unterauftragsverarbeiter für Daten des Verantwortlichen nicht eingesetzt, solange keine Einigung erzielt ist. Der Auftragsverarbeiter unterbreitet dem Verantwortlichen innerhalb von 14 Tagen nach Zugang des Widerspruchs einen Lösungsvorschlag, etwa den Verzicht auf den Unterauftragsverarbeiter für den Workspace des Verantwortlichen oder eine alternative Konfiguration. Kommt innerhalb von weiteren 14 Tagen keine Einigung zustande, kann jede Partei den Vertrag mit einer Frist von 30 Tagen zum Monatsende kündigen. Bis zum Wirksamwerden der Kündigung wird der neue Unterauftragsverarbeiter für Daten des Verantwortlichen nicht eingesetzt. Kündigt der Verantwortliche, erstattet der Auftragsverarbeiter bereits gezahlte Entgelte für Leistungszeiträume nach Vertragsende anteilig; ungenutzte Credits bleiben davon unberührt (§ 12.3 AGB).

(6) Der Auftragsverarbeiter stellt sicher, dass Unterauftragsverarbeiter durch einen Vertrag nach Art. 28 Abs. 4 DSGVO denselben Datenschutzpflichten unterworfen werden, die für den Auftragsverarbeiter nach diesem Vertrag gelten.

(7) Die Weitergabe personenbezogener Daten des Verantwortlichen an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(8) Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragsverarbeiter im Vorfeld sicher, dass die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (§ 5.4a).

(9) Der Auftragsverarbeiter überprüft die Unterauftragsverarbeiter regelmäßig, mindestens jährlich, hinsichtlich Zertifizierungsstatus, Vertragslage und bekannt gewordener Sicherheitsvorfälle und dokumentiert das Ergebnis.

5.4a Drittlandübermittlungen

(1) Soweit im Rahmen der Chat-Funktion Inhalte an LLM-Anbieter mit Sitz außerhalb der EU/des EWR (insbesondere USA) übermittelt werden, stellt der Auftragsverarbeiter sicher, dass hierfür geeignete Garantien gemäß Art. 44 ff. DSGVO bestehen.

(2) Für Übermittlungen in die USA gilt der Angemessenheitsbeschluss der EU-Kommission zum EU-US Data Privacy Framework (Durchführungsbeschluss (EU) 2023/1795), soweit der jeweilige Empfänger zertifiziert ist. Ergänzend und als Rückfallebene sind mit den Empfängern EU-Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914 vereinbart. Für die Betreiberin des AI-Gateways mit Sitz im Vereinigten Königreich (Anlage 2 B) gilt der Angemessenheitsbeschluss der EU-Kommission für das Vereinigte Königreich (Durchführungsbeschluss (EU) 2021/1772, am 19. Dezember 2025 bis zum 27. Dezember 2031 verlängert); die Verarbeitung selbst erfolgt über den EU-Endpunkt des Gateways in Deutschland. Der Zertifizierungsstatus und die vereinbarten Garantien sind je Anbieter in Anlage 2 ausgewiesen.

(3) Soweit Standardvertragsklauseln als Garantie eingesetzt werden, führt der Auftragsverarbeiter vor Beginn der Übermittlung eine Transferfolgenabschätzung (Transfer Impact Assessment, TIA) durch, hält sie aktuell und stellt sie dem Verantwortlichen auf Anfrage zur Verfügung.

(4) Bei aktivierter Pseudonymisierung erhält der LLM-Anbieter ausschließlich pseudonymisierte Inhalte. Es kann nicht in allen Fällen ausgeschlossen werden, dass technische Metadaten (Zeitpunkt, Modell, Tokenzahl) übertragen werden.

(5) Der Auftragsverarbeiter beobachtet die Rechtsentwicklung zum EU-US Data Privacy Framework (Urteil des Gerichts der EU vom 3. September 2025, T-553/23; Rechtsmittel C-703/25 P anhängig) und informiert den Verantwortlichen, sobald sich die Übermittlungsgrundlage ändert.

5.4b Besondere Regelungen bei Berufsgeheimnissen (§ 203 StGB)

(1) Der Verantwortliche teilt dem Auftragsverarbeiter mit, wenn die im Rahmen des Auftrags zu verarbeitenden Daten einem Berufsgeheimnis unterliegen, das nach § 203 StGB strafrechtlich geschützt ist. Berufsgeheimnisträger im Sinne dieser Ziffer sind insbesondere Rechtsanwälte, Notare, Steuerberater, Wirtschaftsprüfer, Patentanwälte, Ärztinnen und Ärzte sowie Psychotherapeutinnen und Psychotherapeuten, einschließlich der bei ihnen oder bei ihrem Träger beschäftigten mitwirkenden Personen im Sinne von § 203 Abs. 4 StGB.

(2) Der Auftragsverarbeiter wahrt dann in Kenntnis der strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht gemäß § 203 StGB (Freiheitsstrafe bis zu einem Jahr oder Geldstrafe) sämtliche fremden Geheimnisse. Alle Mitarbeitenden und Auftragnehmer mit potenziellem Datenzugang sind in Textform zur Verschwiegenheit verpflichtet und über die Strafbarkeit nach §§ 203, 204 StGB belehrt.

(3) Die Vertraulichkeits- und Verschwiegenheitspflicht aus diesem Unterabschnitt besteht auch nach Beendigung des Auftrages fort.

(4) Der Auftragsverarbeiter stellt sicher, dass die in Anlage 2 A genannten Unterauftragsverarbeiter, soweit dort ausgewiesen, in Textform zur Verschwiegenheit verpflichtet und über die Strafbarkeit nach §§ 203, 204 StGB belehrt werden (§ 203 Abs. 4 StGB). Nachweise erhält der Verantwortliche auf Anfrage.

(5) Hinweis zu LLM-Anbietern: Bei aktivierter Pseudonymisierung erhalten LLM-Anbieter keine unpseudonymisierten Inhalte; die Zuordnungstabelle und der Workspace-Schlüssel verbleiben beim Auftragsverarbeiter. Der Verantwortliche stellt sicher, dass bei Nutzung der Chat-Funktion keine dem Berufsgeheimnis unterliegenden Inhalte übermittelt werden, die nicht zuvor ausreichend pseudonymisiert wurden. Der Auftragsverarbeiter empfiehlt Berufsgeheimnisträgern, die Pseudonymisierung und die manuelle Freigabe für alle Nutzer verbindlich vorzugeben oder die eigenen Modelle des Auftragsverarbeiters zu nutzen. Das AI-Gateway und die LLM-Anbieter (Anlage 2 B) sind nach Art. 28 DSGVO gebunden, jedoch nicht nach § 203 Abs. 4 StGB verpflichtet. Weil das Berufsgeheimnis auch nicht personenbezogene Informationen umfasst, kann auch ein pseudonymisierter Text ein Geheimnis enthalten; für solche Inhalte empfiehlt der Auftragsverarbeiter seine eigenen Modelle, bei denen kein Dritter beteiligt ist. Deaktiviert ein Nutzer die Pseudonymisierung (§ 6.3 Abs. 6), erhalten Gateway und LLM-Anbieter unpseudonymisierte Inhalte.

(6) Ergänzend bietet der Auftragsverarbeiter Berufsgeheimnisträgern den Abschluss seiner Verschwiegenheitsvereinbarung (§ 43e BRAO, § 62a StBerG, § 50a WPO, § 39c PAO, § 26a BNotO, § 9 MBO-Ä; derzeit Version 2.5) an, auf Wunsch in Schriftform.

(7) Behördliche Auskunfts- und Herausgabeersuchen prüft der Auftragsverarbeiter auf ihre Rechtmäßigkeit. Er gibt keine Daten freiwillig heraus und informiert den Verantwortlichen unverzüglich, soweit dies gesetzlich zulässig ist.

5.5 Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei:

(1) Betroffenenrechten (Art. 12 bis 22 DSGVO): Wendet sich eine betroffene Person mit Anträgen gemäß Art. 15 bis 21 DSGVO an den Auftragsverarbeiter, wird dieser die betroffene Person unverzüglich an den Verantwortlichen verweisen. Der Service ist so gestaltet, dass der Verantwortliche die meisten Betroffenenrechte selbst erfüllen kann (Einsicht, Export, Löschung im Workspace). Unterstützungsanfragen beantwortet der Auftragsverarbeiter in der Regel innerhalb von zehn Werktagen.

(2) Sicherheitspflichten (Art. 32 bis 36 DSGVO): Sicherstellung eines angemessenen Schutzniveaus, Meldung von Datenschutzverletzungen nach § 5.6, Unterstützung bei einer Datenschutz-Folgenabschätzung mit den erforderlichen Angaben zu Risiken und Maßnahmen (Anlage 1, Auszüge aus dem Sicherheitskonzept) sowie bei der Konsultation der Aufsichtsbehörde.

5.6 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die Daten des Verantwortlichen betrifft, unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung (Erstmeldung, Art. 33 Abs. 2 DSGVO). Kenntniserlangung liegt vor, sobald der Auftragsverarbeiter nach einer ersten Bewertung mit hinreichender Sicherheit von einer Verletzung ausgeht. Die Erstbewertung nimmt der Auftragsverarbeiter unverzüglich nach Erkennung eines Sicherheitsvorfalls vor, in der Regel innerhalb von vier Stunden.

(2) Die Erstmeldung enthält die zu diesem Zeitpunkt verfügbaren Angaben nach Art. 33 Abs. 3 DSGVO: Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen sowie Ansprechpartner. Noch nicht verfügbare Angaben reicht der Auftragsverarbeiter unverzüglich nach, spätestens innerhalb von 72 Stunden nach Kenntniserlangung, soweit sie bis dahin vorliegen (Art. 33 Abs. 4 DSGVO entsprechend). Nach Abschluss der Untersuchung erhält der Verantwortliche einen Abschlussbericht mit Ursache, Auswirkungen und getroffenen Maßnahmen.

(3) Die Meldung erfolgt an die im Nutzerkonto hinterlegte E-Mail-Adresse sowie an einen vom Verantwortlichen zusätzlich benannten Ansprechpartner, etwa den Datenschutzbeauftragten. Der Verantwortliche hält diese Adressen aktuell. Ansprechpartner des Auftragsverarbeiters ist der Datenschutzbeauftragte (datenschutz@anymize.ai); Sicherheitsvorfälle können jederzeit an security@anymize.ai gemeldet werden.

(4) Die Meldung an die Aufsichtsbehörde (Art. 33 DSGVO) und die Benachrichtigung betroffener Personen (Art. 34 DSGVO) obliegen dem Verantwortlichen. Der Auftragsverarbeiter unterstützt ihn mit den erforderlichen Informationen und stimmt sich mit ihm ab, bevor er selbst Dritte über den Vorfall informiert, soweit gesetzliche Pflichten dem nicht entgegenstehen.

(5) Eine Meldung nach dieser Ziffer stellt kein Anerkenntnis einer Pflichtverletzung oder Haftung dar.

5.7 Löschung und Rückgabe

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien sowie gesetzlich erforderliche Aufbewahrungen.

(2) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter alle personenbezogenen Daten oder gibt sie nach Wahl des Verantwortlichen zurück. Das Wahlrecht gemäß Art. 28 Abs. 3 Satz 2 lit. g DSGVO liegt beim Verantwortlichen. Vor Vertragsende kann der Verantwortliche seine Daten über die Oberfläche und die API exportieren.

(3) Hash-Original-Paare werden entsprechend der vom Verantwortlichen gewählten Speicherfrist gelöscht (24 Stunden, 7 Tage, 30 Tage, unbegrenzt oder sofortige Löschung nach der Verarbeitung).

(4) Hochgeladene Originaldokumente werden nach der Inhaltsextraktion nicht in ihrer Ursprungsform gespeichert. Extrahierte Dokumentinhalte und Chat-Verläufe werden verschlüsselt im Workspace des Verantwortlichen gespeichert, bis der Verantwortliche sie löscht, spätestens bis zur Kontolöschung.

(5) Nach Beendigung des Vertrags oder Löschung des Kontos löscht der Auftragsverarbeiter alle personenbezogenen Daten des Verantwortlichen im Produktivsystem innerhalb von 30 Tagen. Sicherungen werden turnusmäßig überschrieben; Einzelheiten regelt Anlage 1.

(6) Auf Verlangen bestätigt der Auftragsverarbeiter die Löschung in Textform.

§ 6

Pflichten des Verantwortlichen

6.1 Rechtmäßigkeit

Der Verantwortliche ist dafür verantwortlich, dass

(1) die Verarbeitung personenbezogener Daten rechtmäßig erfolgt,

(2) betroffene Personen ordnungsgemäß informiert wurden,

(3) die erforderlichen Rechtsgrundlagen für die Verarbeitung vorliegen.

6.2 Weisungen

(1) Der Verantwortliche erteilt Weisungen schriftlich oder in Textform. Mündlich erteilte Weisungen sind unverzüglich in Textform zu bestätigen.

(2) Die Nutzung des Services entsprechend der Dokumentation bestimmt den vereinbarten Nutzungsumfang (vgl. § 5.1 Abs. 2).

6.3 Prüfpflicht und Eigenverantwortung

(1) Der Verantwortliche ist verpflichtet, alle pseudonymisierten Dokumente und Eingaben vor der Weitergabe an LLM-Dienste oder Dritte eigenständig zu prüfen.

(2) Der Service erreicht eine Zielerkennungsrate von über 95 %. Eine vollständige Erkennung aller personenbezogenen Daten kann technisch nicht garantiert werden. Nicht erkannte Werte oder identifizierende Kontextinformationen können im Text verbleiben.

(3) Der Verantwortliche entscheidet in eigener Verantwortung, ob die Pseudonymisierung für seinen Anwendungsfall ausreicht. Er kann hierfür die vom Service bereitgestellten Kontrollen nutzen: Anzeige der ersetzten Werte vor der Übermittlung, aktive Freigabe vor

jedem Senden sowie, in den Plänen Team Business und Team Enterprise, die Möglichkeit für Administratoren, Pseudonymisierung und aktive Freigabe für alle Nutzer des Workspaces verbindlich vorzugeben.

(4) Die Haftung richtet sich nach § 8. Soweit ein Schaden darauf beruht, dass der Verantwortliche die vom Service angezeigten Pseudonymisierungsergebnisse und für ihn erkennbare Lücken vor der Weitergabe nicht geprüft hat, wird dies beim Ausgleich zwischen den Parteien berücksichtigt: bei Ansprüchen betroffener Personen im Rahmen von Art. 82 Abs. 5 DSGVO, bei eigenen Ansprüchen des Verantwortlichen nach § 254 BGB.

(5) Der Verantwortliche nimmt zur Kenntnis, dass insbesondere bei ungewöhnlichen Schreibweisen von Namen, branchenspezifischen Fachbegriffen, kontextabhängigen Identifikatoren, handschriftlichen Dokumenten sowie bei Bildern und Scans eine manuelle Nachprüfung besonders wichtig ist.

(6) Deaktiviert ein Nutzer des Verantwortlichen die Pseudonymisierung für eine Anfrage, werden die Inhalte dieser Anfrage im Klartext an den gewählten LLM-Anbieter übermittelt. Die Zulässigkeit einer solchen Übermittlung, einschließlich einer etwaigen Drittlandübermittlung, verantwortet der Verantwortliche. Er kann die Deaktivierung für alle Nutzer seines Workspaces ausschließen.

§ 7

Kontrollrechte

7.1 Nachweispflicht

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung.

(2) Auf Anfrage stellt der Auftragsverarbeiter die aktuelle TOM-Dokumentation (Anlage 1), Auszüge aus dem Sicherheitskonzept gegen Vertraulichkeitsverpflichtung, Zertifikate und Testate der Infrastrukturbetreiber, Zusammenfassungen von Penetrationstests sowie Nachweise über Verschwiegenheitsverpflichtungen zur Verfügung.

7.2 Inspektionen

(1) Der Verantwortliche ist berechtigt, Überprüfungen durchzuführen oder durch einen beauftragten Prüfer durchführen zu lassen.

(2) Inspektionen sind mit einer Frist von 14 Tagen anzukündigen und finden ohne konkreten Anlass höchstens einmal je Kalenderjahr statt.

(3) Der Auftragsverarbeiter kann anstelle einer Vor-Ort-Inspektion die schriftliche Beantwortung eines Prüffragebogens, die Teilnahme an einem Sammelaudit oder die Vorlage eines aktuellen Prüfberichts anbieten.

(4) Die Kosten der Inspektion trägt der Verantwortliche, sofern keine Verstöße festgestellt werden.

§ 8

Haftung

8.1 Haftungsverteilung

(1) Die Haftung der Parteien für Verstöße gegen datenschutzrechtliche Pflichten richtet sich nach Art. 82 DSGVO. Gegenüber betroffenen Personen wird diese Haftung weder beschränkt noch ausgeschlossen.

(2) Dieser AVV hat in Bezug auf datenschutzrechtliche Regelungen Vorrang gegenüber den AGB. Die Haftungsregelungen dieses AVV gehen den Haftungsregelungen der AGB für datenschutzrechtliche Sachverhalte vor.

(3) Im Verhältnis der Parteien zueinander haftet der Auftragsverarbeiter für Schäden aus der Verletzung datenschutzrechtlicher Pflichten unbeschränkt bei Vorsatz und grober Fahrlässigkeit sowie bei Verletzung des Lebens, des Körpers oder der Gesundheit. Im Übrigen ist die Haftung auf den vorhersehbaren, vertragstypischen Schaden begrenzt, höchstens auf das vom Verantwortlichen in den zwölf Monaten vor dem schädigenden Ereignis gezahlte Nettoentgelt.

8.2 Ausgleich im Innenverhältnis und Freistellung

Im Innenverhältnis haften die Parteien einander nach Maßgabe ihres jeweiligen Anteils an der Verantwortung für den Schaden (Art. 82 Abs. 5 DSGVO). Jede Partei stellt die andere Partei von Ansprüchen Dritter insoweit frei, als der Anspruch auf einer Verletzung datenschutzrechtlicher Pflichten durch die freistellende Partei beruht.

§ 9

Schlussbestimmungen

9.1 Vorrang des AVV

Bei Widersprüchen zwischen diesem AVV und den AGB hat dieser AVV in Bezug auf datenschutzrechtliche Regelungen Vorrang. Die Bestimmungen dieses AVV sind nicht durch einseitige Änderungen der AGB abzuändern.

9.2 Änderungen

(1) Änderungen dieses Vertrags bedürfen der Textform.

(2) Der Auftragsverarbeiter kann diesen Vertrag ohne Zustimmung des Verantwortlichen anpassen, soweit die Änderung (a) durch Gesetz, Rechtsprechung oder Vorgaben einer Aufsichtsbehörde erforderlich wird oder (b) das Schutzniveau und die Rechte des Verantwortlichen nicht nachteilig berührt, insbesondere bei redaktionellen Änderungen, zusätzlichen Schutzmaßnahmen oder Fristverkürzungen zugunsten des Verantwortlichen. Solche Änderungen kündigt der Auftragsverarbeiter mindestens 30 Tage vor dem Wirksamwerden per E-Mail an. Änderungen bei Unterauftragsverarbeitern richten sich ausschließlich nach § 5.4.

(3) Alle übrigen Änderungen, insbesondere solche zum Nachteil des Verantwortlichen bei Weisungsrechten, Sicherheitsniveau (Anlage 1), Melde- und Löschfristen, Verarbeitungsorten, Kontrollrechten oder Haftung, werden nur wirksam, wenn der Verantwortliche ihnen in Textform zustimmt, auch über die Kontofunktion des Services. Der Auftragsverarbeiter übermittelt den Änderungsvorschlag mit Begründung mindestens 30 Tage vor dem vorgesehenen Wirksamwerden. Stimmt der Verantwortliche nicht zu, gilt die bisherige Fassung fort. Ist dem Auftragsverarbeiter das Festhalten an der bisherigen Fassung unzumutbar, kann jede Partei den Vertrag mit einer Frist von 30 Tagen zum Monatsende kündigen; bereits gezahlte Entgelte für Leistungszeiträume nach Vertragsende erstattet der Auftragsverarbeiter anteilig, ungenutzte Credits bleiben davon unberührt (§ 12.3 AGB).

9.3 Anwendbares Recht

Es gilt deutsches Recht. Gerichtsstand ist Kiel.

9.4 Salvatorische Klausel

Sollten einzelne Bestimmungen unwirksam sein, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

9.5 Rechtsnachfolge

(1) Im Falle einer Umwandlung des Auftragsverarbeiters tritt der jeweilige Rechtsnachfolger in die Rechte und Pflichten aus diesem AVV ein.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über bevorstehende Umwandlungen mindestens 30 Tage im Voraus per E-Mail.

Anlage 1: Technische und organisatorische Maßnahmen (TOM)

(1) Anlage 1 ist die Dokumentation „Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DSGVO für den Service anymize" der anymize GmbH in der jeweils aktuellen Fassung, derzeit Version 3.2 vom 6. November 2026. Der Auftragsverarbeiter stellt sie

dem Verantwortlichen auf Anfrage zur Verfügung und darf einzelne Maßnahmen ändern oder ersetzen, sofern das Sicherheitsniveau insgesamt nicht unterschritten wird (§ 5.3 Abs. 3).

(2) Kernmaßnahmen im Überblick:

- Verschlüsselung aller Datenübertragungen (TLS 1.3); Verschlüsselung gespeicherter Inhalte und Hash-Original-Paare mit AES-256 und workspace-spezifischen Schlüsseln, getrennt verwahrt
- Betrieb aller Produktionssysteme in zertifizierten Rechenzentren in Deutschland (ISO/IEC 27001, BSI C5); verschlüsselte Sicherungen auf getrennter Infrastruktur in Deutschland/Frankreich (EU)
- Logische Mandantentrennung je Workspace; rollenbasierte Berechtigungen; Prinzip der minimalen Rechte; kein Klartextzugriff von Mitarbeitenden im Regelbetrieb
- Zwei-Faktor-Authentifizierung und VPN für administrative Zugänge; persönliche Administratorkonten; Protokollierung administrativer Zugriffe
- Tägliche Sicherungen; Recovery Time Objective unter 4 Stunden; Recovery Point Objective unter 24 Stunden; regelmäßige Wiederherstellungstests
- Verpflichtung aller Mitarbeitenden und relevanten Auftragnehmer zur Vertraulichkeit und nach § 203 Abs. 4 StGB; jährliche Datenschutz- und Sicherheitsschulungen
- Dokumentiertes Incident-Response-Verfahren mit Erstmeldung an den Verantwortlichen innerhalb von 24 Stunden nach Kenntniserlangung (§ 5.6)
- Pseudonymisierung vor jeder Verarbeitung durch externe Modelle bei aktivierter Pseudonymisierung; Erzwingungsfunktionen für Administratoren; eigene Modelle ohne Beteiligung externer Anbieter
- Jährliche Überprüfung der Unterauftragsverarbeiter; Transferfolgenabschätzung für Übermittlungen in Drittländer

Anlage 2: Genehmigte Unterauftragsverarbeiter

A. Ständig eingesetzte Unterauftragsverarbeiter

Unternehmen	Anschrift	Verarbeitungszweck	Ort der Verarbeitung	Garantien
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Hosting und Betrieb der Plattform, Speicherung aller Kundendaten, Betrieb der eigenen Modelle	Deutschland (Falkenstein, Nürnberg)	AVV nach Art. 28 DSGVO; ISO/IEC 27001:2022; BSI C5 Typ 2; Verpflichtung nach § 203 Abs. 4 StGB
OVH GmbH	St. Johanner Str. 41-43, 66111 Saarbrücken,	Hosting, Server-Infrastruktur, Datenspeicherung,	Deutschland (eigene Modelle und KI-Hilfsfunktionen);	AVV nach Art. 28 DSGVO; ISO/IEC 27001; Verpflichtung

	Deutschland	insbesondere verschlüsselte Sicherungen; Betrieb der eigenen Modelle und von KI-Hilfsfunktionen (z. B. Titel, Zusammenfassungen)	Deutschland / Frankreich (EU) (Sicherungen)	nach § 203 Abs. 4 StGB
GRVITY GmbH (mit der anymize GmbH gesellschaftsrechtlich verbunden, Betreiberin von Florentin.ai)	Schauenburgerstr. 116, 24118 Kiel, Deutschland	Konto-, Team-, Abrechnungs- und API-Schlüssel-Verwaltung (SaaS-Backend); kein Zugriff auf Dokumentinhalte oder Hash-Original-Paare	Deutschland	AVV nach Art. 28 DSGVO; Verpflichtung nach § 203 Abs. 4 StGB
Stripe, Inc. / Stripe Technology Europe Ltd.	354 Oyster Point Blvd, South San Francisco, CA 94080, USA / Dublin, Irland	Zahlungsabwicklung und Rechnungsstellung (Kontodaten des Verantwortlichen; keine Dokumentinhalte)	EU / USA	AVV; EU-US Data Privacy Framework und EU-Standardvertragsklauseln; PCI DSS Level 1. Für Betrugsprävention und regulatorische Pflichten ist Stripe eigenständig Verantwortlicher.

B. Nutzungsabhängige Unterauftragsverarbeiter (AI-Gateway und LLM-Anbieter)

Die folgenden Anbieter werden nur tätig, wenn der Verantwortliche oder seine Nutzer ein externes Modell auswählen. Bei aktivierter Pseudonymisierung erhalten sie ausschließlich pseudonymisierte Inhalte (§ 1.1 Abs. 2, § 6.3 Abs. 6). Der Auftragsverarbeiter nutzt ausschließlich die Geschäftskunden-Schnittstellen (API) der Anbieter, für die ein Auftragsverarbeitungsvertrag besteht, nie Verbraucherprodukte. Die Anbindung hängt von der Modellgruppe ab: In der EU gehostete Modelle (im Service als „EU-gehostete Modelle" gekennzeichnet) sind über das AI-Gateway der Requesty Ltd angebunden. Das Gateway arbeitet ausschließlich über seinen EU-Endpunkt in Frankfurt am Main, leitet die Anfragen an den vom Verantwortlichen oder seinen Nutzern gewählten Anbieter weiter und speichert deren Inhalte nicht. Die Inferenz dieser Modelle erfolgt auf Cloud-Plattformen in EU-Regionen, die Requesty als eigene Unterauftragnehmer einsetzt (siehe Tabelle). Internationale Modelle mit Verarbeitung in den USA, die Websuche und die Modelle von Mistral AI (Verarbeitung in Frankreich) sind direkt über die Schnittstelle des jeweiligen Anbieters angebunden.

Unternehmen	Sitz	Verarbeitungszweck	Ort der Verarbeitung	Garantien
Requesty Ltd	71-75 Shelton Street, Covent Garden, London WC2H 9JQ, Vereinigtes Königreich (Companies House 15165717)	AI-Gateway für die in der EU gehosteten Modelle (GPT, Claude, Gemini einschließlich Bildgenerierung, GLM): technische Weiterleitung der Modellaufrufe (Lastverteilung, Nutzungssteuerung); keine eigene Modellverarbeitung. Die Inferenz führen Unterauftragnehmer von Requesty in EU-Regionen aus: Microsoft Azure, Amazon Web Services (Bedrock), Google Cloud (Vertex AI) und Nebius; die Plattform ist je Workspace wählbar	Gateway: Deutschland (EU-Endpunkt, Rechenzentrum Amazon Web Services Frankfurt am Main); Inferenz: EU-Regionen der genannten Plattformen	AVV/DPA nach Art. 28 Abs. 4 DSGVO; keine Speicherung von Eingaben und Ausgaben (Zero Data Retention), nur technische Metadaten; kein Training; Verschlüsselung bei Übertragung und Speicherung; Angemessenheitsbeschluss der EU-Kommission für das Vereinigte Königreich (Durchführungsbeschluss (EU) 2021/1772, verlängert bis 27.12.2031)
OpenAI Ireland Ltd. (Konzern: OpenAI, L.L.C., San Francisco, USA)	Dublin, Irland	Sprach- und Bildmodelle (GPT)	USA (internationale Modelle, direkte Anbindung)	AVV/DPA nach Art. 28 Abs. 4 DSGVO; kein Training mit API-Daten; Zero Data Retention (keine Speicherung von Eingaben und Ausgaben, nur technische Metadaten); EU-Standardvertragsklauseln (keine Zertifizierung nach dem EU-US Data Privacy Framework)
Anthropic, PBC	San Francisco, USA	Sprachmodelle (Claude, einschließlich Claude Fable)	USA (internationale Modelle, direkte Anbindung)	AVV/DPA nach Art. 28 Abs. 4 DSGVO; kein Training mit API-Daten; Zero Data Retention (keine Speicherung von Eingaben und Ausgaben, nur technische Metadaten); Ausnahme Claude Fable 5 und Claude Fable 5.1: Speicherung von

				Eingaben und Ausgaben für 30 Tage zur Sicherheitsüberwachung durch Anthropic, Zero Data Retention für diese Modelle nicht verfügbar; EU-Standardvertragsklauseln
Mistral AI SAS	15 rue des Halles, 75001 Paris, Frankreich	Sprachmodelle (Mistral)	Frankreich (EU), direkte Anbindung	AVV/DPA nach Art. 28 Abs. 4 DSGVO; kein Training mit API-Daten (Opt-out); Zero Data Retention (keine Speicherung von Eingaben und Ausgaben, nur technische Metadaten); keine Drittlandübermittlung
Perplexity AI, Inc.	San Francisco, USA	Sprachmodelle mit integrierter Websuche (Perplexity) im Chat; Websuche des Services, bei der nur die Suchanfrage übermittelt wird	USA (direkte Anbindung)	AVV/DPA nach Art. 28 Abs. 4 DSGVO; kein Training; Zero Data Retention (keine Speicherung von Eingaben und Ausgaben, nur technische Metadaten); EU-US Data Privacy Framework; EU-Standardvertragsklauseln
SpaceXAI LLC (xAI)	USA	Sprachmodelle (Grok)	USA (direkte Anbindung)	AVV/DPA nach Art. 28 Abs. 4 DSGVO; Verarbeitung ausschließlich nach Weisung, kein Training; Zero Data Retention (keine Speicherung von Eingaben und Ausgaben, nur technische Metadaten); EU-Standardvertragsklauseln (keine Zertifizierung nach dem EU-US Data Privacy Framework)

Der in Version 1.4 genannte Vermittlungsdienst OpenRouter, Inc. wird nicht mehr eingesetzt; für die in der EU gehosteten Modelle ist an seine Stelle das AI-Gateway der Requesty Ltd getreten. Welche Modellanbieter in einem Workspace verfügbar sind, legen der Verantwortliche und seine Administratoren fest; nicht freigegebene Anbieter erhalten keine Daten des Verantwortlichen.

Die Anbieter verwenden Eingaben nicht zum Training. Für alle Anbieter ist Zero Data Retention eingerichtet: Eingaben und Ausgaben werden beim Anbieter nicht gespeichert; es fallen nur technische Metadaten an (etwa Zeitpunkt, Modell und Tokenzahl). Einzige Ausnahme sind die Modelle Claude Fable 5 und Claude Fable 5.1: Für sie verlangt Anthropic eine Speicherung von Eingaben und Ausgaben für 30 Tage zur Sicherheitsüberwachung; Zero Data Retention ist für diese Modelle nicht verfügbar. Bei aktivierter Pseudonymisierung betrifft diese Speicherung nur pseudonymisierte Inhalte. Der Verantwortliche kann diese Modelle über die Modellfreigabe für seinen Workspace ausschließen.

C. Keine Unterauftragsverarbeiter des Auftragsverarbeiters

Bei Nutzung der eigenen Modelle des Auftragsverarbeiters (Betrieb bei den in Abschnitt A genannten Betreibern Hetzner und OVH in Rechenzentren in Deutschland) ist kein externer Modellanbieter beteiligt. Vom Verantwortlichen selbst angebundene Modelle (Bring Your Own Model) und von ihm freigegebene Drittdienste (z. B. Google Workspace, Microsoft 365 über Connectoren) sind Vertragspartner des Verantwortlichen und keine Unterauftragsverarbeiter des Auftragsverarbeiters.

Hinweis zum Vertragsschluss

Dieser Auftragsverarbeitungsvertrag wurde durch die anymize GmbH verbindlich erstellt und tritt mit Akzeptanz der AGB bzw. erstmaliger Nutzung des Services automatisch in Kraft. Eine separate Unterzeichnung ist nicht erforderlich; sie ist auf Wunsch möglich.

Der Verantwortliche bestätigt durch die Nutzung des Services die Kenntnisnahme dieses AVV, die Einbeziehung in das Vertragsverhältnis und die Genehmigung der in Anlage 2 aufgeführten Unterauftragsverarbeiter.

Änderungshistorie

Version	Stand	Änderungen
1.6	06.11.2026	Zero Data Retention bei allen Modellanbietern ausgewiesen, einzige Ausnahme Claude Fable 5 und Claude Fable 5.1 mit 30 Tagen Speicherung bei Anthropic zur Sicherheitsüberwachung (Anlage 2

		B); Google LLC als direkt angebundener Anbieter gestrichen, Gemini nur noch als in der EU gehostetes Modell über das AI-Gateway (Anlage 2 B); Garantie für Anthropic auf EU-Standardvertragsklauseln präzisiert (Anlage 2 B); Empfehlung für besondere Kategorien in größerem Umfang auf die eigenen Modelle ausgerichtet (§ 3.2 Abs. 5); Verweise auf die TOM-Dokumentation Version 3.2 (Anlage 1) und die Verschwiegenheitsvereinbarung Version 2.5 (§ 5.4b Abs. 6).
1.5	24.09.2026	LLM-Anbieter als nutzungsabhängige Unterauftragsverarbeiter mit Vertrag nach Art. 28 Abs. 4 DSGVO (§ 1.1, § 5.4 Abs. 2, Anlage 2 neu strukturiert in A/B/C); Widerspruch gegen neue Unterauftragsverarbeiter ohne Begründungspflicht, Lösungs- und Kündigungsverfahren (§ 5.4 Abs. 4 und 5); jährliche Überprüfung der Unterauftragsverarbeiter (§ 5.4 Abs. 9); Rechtsentwicklung DPF (§ 5.4a Abs. 5); § 203 StGB: Personenkreis präzisiert, Verpflichtung der ständig eingesetzten Unterauftragsverarbeiter nach § 203 Abs. 4 StGB, Klarstellung, dass AI-Gateway und LLM-Anbieter nicht nach § 203 StGB verpflichtet sind, behördliche Ersuchen, Verschwiegenheitsvereinbarung Version 2.4 (§ 5.4b); Erstmeldung von Datenschutzverletzungen innerhalb von 24 Stunden, Nachmeldung bis 72 Stunden, Abschlussbericht, Definition der Kenntniserlangung (§ 5.6); Löschfristen konkretisiert (§ 5.7); Prüfpflicht ohne pauschalen Haftungsausschluss, Mitverantwortung nach Art. 82 Abs. 5 DSGVO und § 254 BGB, Klartextmodus transparent geregelt (§ 6.3); Haftung nach Art. 82 DSGVO ohne Beschränkung gegenüber Betroffenen, Haftungsgrenze nur im Innenverhältnis (§ 8); Änderungen nur noch zustimmungsfrei bei gesetzlicher Notwendigkeit oder zugunsten des Verantwortlichen, sonst Textform-Zustimmung und Sonderkündigungsrecht (§ 9.2); Datenschutzbeauftragter als Ansprechpartner (Präambel, § 5.6); Anlage 1 verweist auf TOM-Dokumentation v3.1; Stripe und GRVITY GmbH in Anlage 2 ergänzt, OpenRouter gestrichen (nicht mehr im Einsatz), AI-Gateway Requesty Ltd für die in der EU gehosteten Modelle (EU-Endpunkt Frankfurt am Main, Zero Data Retention, Angemessenheitsbeschluss für das Vereinigte Königreich) in Anlage 2 B und § 5.4a Abs. 2 aufgenommen, internationale Modelle direkt beim Anbieter angebunden; Perplexity AI und xAI (Grok) in Anlage 2 B aufgenommen, Plattformen für die in der EU gehosteten Modelle als Unterauftragnehmer von Requesty benannt, Garantien je Anbieter nach Zertifizierungsstatus ausgewiesen; Fehler der v1.4 korrigiert (Fußzeile Seite 3, Zweckangabe OpenAI).
1.4	Mai 2026	Terminologie Pseudonymisierung (§ 1.1), besondere Kategorien nach Art. 9 DSGVO (§ 3.2), Weisungsregelung (§ 5.1), Drittlandübermittlungen (§ 5.4a), Berufsgeheimnisse neu gefasst (§ 5.4b), LLM-Anbieter in Anlage 2 aufgeführt, USt-IdNr. ergänzt.
1.3	Mai 2026	Umstellung der Firmierung GRVITY GmbH auf anymize GmbH, neue Handelsregisternummer.
1.2	Februar 2026	Regelungen zu Unterauftragsverarbeitern erweitert (§ 5.4), besondere Regelungen für Berufsgeheimnisträger (§ 5.4a alt), OVH GmbH in Anlage 2 aufgenommen.
1.1	vor Februar 2026	Fassung unter der GRVITY GmbH.

Version: 1.6 · **Stand:** 6. November 2026 · **Erstellt durch:** anymize GmbH

Kontakt für Datenschutzangelegenheiten: datenschutz@anymize.ai