

# Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

Einrichtung  
Straße Nr.

PLZ Ort

---

- nachstehend „Verantwortlicher“ genannt -

und der

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen  
vertreten durch den Geschäftsführer Prof. Dr. Ramin Yahyapour  
Burckhardtweg 4  
37077 Göttingen

---

- nachstehend „Auftragsverarbeiter“ genannt -

## § 1 Gegenstand und Dauer des Auftrags

Der Auftragsverarbeiter führt die vereinbarte Leistung ausschließlich im Rahmen der Inanspruchnahme der Dienstleistungen ChatAI und LLM-Backend durch den Verantwortlichen aus.

Dieser Vertrag ersetzt jegliche bisherige ADV-Verträge zu vergleichbaren Diensten, die in der Academic Cloud angeboten werden.

## § 2 Umfang, Art und Zweck der vorgesehenen Datenverarbeitung

- (1) Art, Umfang und Zweck der Verarbeitung personenbezogener Daten sowie die Schutzstufe sind in Anlage 1 festgelegt.
- (2) Der Auftragsverarbeiter darf die personenbezogenen Daten nur im Rahmen der dokumentierten Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen. Der Auftragsverarbeiter ist während der gesamten Laufzeit des Vertrages an die Weisungen des Verantwortlichen gebunden.
- (3) Sämtliche vertragsgegenständlichen Daten dürfen im Rahmen dieses Vertrags nur in Staaten, die Mitglied der Europäischen Union oder ein Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind, verarbeitet und gespeichert werden. Der Auftragsverarbeiter sichert zu, die vertragsgegenständlichen Daten vor einem Zugriff

staatlicher Stellen außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums zu schützen.

- (4) Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Diese sind gesondert festzulegen.
- (5) Der Auftragsverarbeiter verwendet Daten, die ihm im Rahmen der vertraglichen Erfüllung oder im Zusammenhang damit bekannt geworden sind, nur für die vorgesehenen Zwecke. Kopien oder Duplikate dürfen ohne Wissen und schriftlicher Zustimmung des Verantwortlichen nicht erstellt werden. Hiervon ausgenommen sind Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung, sowie zur Erfüllung von Haftungs- und Gewährleistungsansprüchen.
- (6) Auskünfte an Dritte, auch an Datenschutzaufsichtsbehörden, darf der Auftragsverarbeiter nicht ohne vorherige Konsultation des Verantwortlichen erteilen.

### **§ 3 Rechte und Pflichten des Verantwortlichen**

- (1) Der Verantwortliche ist Verantwortlicher nach Art. 4 Ziff. 7 DS-GVO für die Verarbeitung von Daten im Auftrag durch den Auftragsverarbeiter. Für die Beurteilung der Rechtmäßigkeit der Datenverarbeitung ist der Verantwortliche verantwortlich.
- (2) Der Verantwortliche ist für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragsverarbeiter geltend machen.
- (3) Der Verantwortliche erteilt dem Auftragsverarbeiter die Anweisung, sämtliche Pflichten nach diesem Vertrag einzuhalten. Der Verantwortliche hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragsverarbeiter zu erteilen. Weisungen können schriftlich oder per digital signierter E-Mail erfolgen.

### **§ 4 Rechte und Pflichten des Auftragsverarbeiters**

- (1) Der Auftragsverarbeiter kontrolliert regelmäßig die Datenverarbeitung und die internen Prozesse und informiert den Verantwortlichen unverzüglich bei Verdacht der Verletzung des Schutzes personenbezogener Daten, über Fälle von schwerwiegenden Betriebsstörungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Der Auftragsverarbeiter trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Verantwortlichen ab. Der

Auftragsverarbeiter erteilt dem Verantwortlichen unverzüglich alle verlangten Auskünfte, insbesondere die für die Meldungen nach Artikel 33, 34 DS-GVO erforderlichen Informationen, und unterstützt ihn bei der Erfüllung seiner Pflichten nach Artikel 33, 34 DS-GVO. Der Auftragsverarbeiter gestattet dem Verantwortlichen oder von ihm benannten Dritten unverzüglich eigene Untersuchungen der Datenverarbeitung.

- (2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die Datenschutz-Grundverordnung oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedsstaaten verstößt.
- (3) Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, bevor eine angekündigte Kontrolle einer Datenschutzaufsichtsbehörde stattfindet, sofern vertraglich geschuldete Leistungen hiervon betroffen sind oder sich aus der Überprüfung der Aufsichtsbehörde Konsequenzen für die Art und Weise der Vertragserfüllung ergeben können. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen auch, soweit eine Behörde im Rahmen eines Strafverfahrens-, oder Bußgeldverfahrens in Bezug auf die Verarbeitung der personenbezogenen Daten oder sonst im Zusammenhang mit diesen Daten bei dem Auftragsverarbeiter ermittelt.
- (4) Ferner ist der Auftragsverarbeiter verpflichtet, dem Verantwortlichen sämtliche für dessen etwaige Auskunftspflichten gegenüber Betroffenen oder den zuständigen Behörden erforderlichen Informationen und Auskünfte zu Erhebung, Speicherung, Verarbeitung und Übertragung von personenbezogenen Daten auf erstes Verlangen unverzüglich und vollumfänglich zu erteilen. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Pflichten nach Art. 35, 36 DS-GVO (Datenschutz-Folgenabschätzung und vorherige Konsultation) und erteilt alle hierzu erforderlichen Auskünfte.
- (5) Der Auftragsverarbeiter wird den Verantwortlichen in Verfahren vor der Aufsichtsbehörde, in Bußgeld-, Straf- oder Verwaltungsverfahren, in Auseinandersetzungen mit Betroffenen oder Dritten, die im Zusammenhang mit der Auftragsverarbeitung oder den personenbezogenen Daten stehen, insbesondere bei einer Inanspruchnahme wegen etwaiger Ansprüche nach Art. 82 DS-GVO, nach besten Kräften unterstützen. Soweit diese Tätigkeiten über den vertraglich vereinbarten Leistungsumfang hinausgehen, kann der Auftragsverarbeiter eine angemessene Vergütung mit dem jeweils aktuellen Stundensatz der GWVG verlangen.
- (6) Die in Absatz 1 bis 5 genannten Unterstützungsleistungen erbringt der Auftragsverarbeiter unentgeltlich, soweit sie ihm zumutbar und angemessen sind.

- (7) Berichtigungen, Löschungen oder Sperrungen von personenbezogenen Daten nimmt der Auftragsverarbeiter nur auf Anweisung bzw. nach vorheriger Zustimmung des Verantwortlichen vor. Der Auftragsverarbeiter ist verpflichtet, seine Infrastruktur so zu gestalten, und alle weiteren Vorkehrungen zu treffen, damit er entsprechenden Vorgaben des Verantwortlichen unverzüglich nachkommen kann. Er unterstützt den Verantwortlichen im Rahmen seiner Möglichkeiten und im Rahmen der Weisungen des Verantwortlichen bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO.
- (8) Der Auftragsverarbeiter sichert zu, eine/n fachkundige/n und zuverlässige/n betriebliche/n Datenschutzbeauftragte/n bestellt zu haben, der/dem die erforderliche Zeit zur Erledigung ihrer/seiner Aufgaben nach Art. 38 und 39 DS-GVO gewährt wird. Er teilt dem Verantwortlichen die Kontaktdaten unverzüglich mit. Das gilt auch für eventuelle Wechsel der/des Datenschutzbeauftragten. Ist der Auftragsverarbeiter nicht zur Bestellung einer oder eines Datenschutzbeauftragten verpflichtet, so teilt er dies dem Verantwortlichen mit.

## **§ 5 Vertraulichkeitsverpflichtung**

- (1) Der Auftragsverarbeiter gewährleistet, dass es den mit der Verarbeitung der Daten des Verantwortlichen befassten Mitarbeiter und andere für den Auftragsverarbeiter tätigen Personen untersagt ist, die Daten außerhalb der Weisungen des Verantwortlichen zu verarbeiten. Ferner gewährleistet der Auftragsverarbeiter, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
- (2) Der Auftragsverarbeiter sichert zu, dass er die für den Auftrag eingesetzten Beschäftigten mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht hat. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften und der Weisungen.

## **§ 6 Technische und Organisatorische Maßnahmen**

- (1) Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen treffen, um – ausgehend von der durch den Verantwortlichen festgelegten Schutzstufe der Daten – ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

- (2) Die technischen und organisatorischen Maßnahmen müssen den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen und die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, insb. durch mögliche Verletzungen des Schutzes personenbezogener Daten gemäß Art. 32 Abs. 2 DS-GVO, zu berücksichtigen.
- (3) Die vom Auftragsverarbeiter zu ergreifenden technischen und organisatorischen Maßnahmen werden in Anlage 1 festgelegt.
- (4) Der Auftragsverarbeiter setzt ein Verfahren gemäß Art. 32 Abs. 1 lit. d) DS-GVO zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung ein und informiert den Verantwortlichen über die Ergebnisse der Überprüfung.
- (5) Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Änderungen sind schriftlich zu vereinbaren.
- (6) 6 Die sichere Kommunikation per E-Mail hat mittels End-zu-End-Verschlüsselung zu erfolgen. Werden besondere Kategorien von personenbezogenen Daten im Sinne des Art. 9 DS-GVO sowie vertrauliche Daten per E-Mail kommuniziert, ist die Verwendung von S/MIME vorgesehen. Der Auftragsverarbeiter stellt dafür während der gesamten Vertragslaufzeit sicher, dass seine Beschäftigten über S/MIME-fähige Mail-Clients mit Signatur und Verschlüsselungsfunktion sowie über gültige Zertifikate verfügen, die den Mindestanforderungen der "Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)" entsprechen und die von einer gängigen Zertifizierungsstelle ausgestellt sind. Ausgehende E-Mails der Beschäftigten des Auftragsverarbeiters sind standardmäßig digital zu signieren. Benötigt der Empfänger für die Entschlüsselung ein Kennwort oder eine andere Form von Schlüsselmaterial, ist dieses auf einem anderen Wege als der zu verschlüsselnden Verbindung zu übertragen. Der Auftragsverarbeiter trägt bei ihm anfallende Kosten der Verschlüsselung selbst.
- (7) Der Auftragsverarbeiter berät und unterstützt den Verantwortlichen bei der Auswahl und Umsetzung der geeigneten technischen und organisatorischen Maßnahmen, um die Datenschutzgrundsätze der Datenschutz-Grundverordnung (z.B. Datenminimierung) wirksam umzusetzen, die notwendigen Garantien in die Verarbeitung

aufzunehmen, um den Anforderungen der Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen (Privacy by design). Gleiches gilt für technische und organisatorische Maßnahmen, die sicherstellen, dass durch die Voreinstellung grundsätzlich nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist (Privacy by default).

## **§ 7 Nachweise und Kontrollrechte des Verantwortlichen**

- (1) Der Auftragsverarbeiter weist dem Verantwortlichen die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.
- (2) Der Verantwortliche hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer, dessen Kosten der Verantwortliche trägt, durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieses Vertrags durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.
- (3) Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- (4) Der Auftragsverarbeiter kann auch folgende Nachweise vorlegen:
  - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
  - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor, Qualitätsauditor);
  - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI Grundschutz).Die Rechte des Verantwortlichen nach Abs. 2 und 3, Überprüfungen durchzuführen und Auskunft zu verlangen, bleiben unberührt.
- (5) Die sonstigen jeweils auf ihrer Seite anfallenden Kosten tragen die Vertragsparteien jeweils selbst.

## **§ 8 Unterauftragsverhältnisse**

- (1) Der Verantwortliche stimmt der Einschaltung der in Anlage 2 genannten Unterauftragsverarbeiter zu.
- (2) Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder der Ersetzung anderer Unterauftragsverarbeiter. Der Verantwortliche ist berechtigt, gegen derartige Änderungen Einspruch zu erheben.
- (3) Der Auftragsverarbeiter hat vertraglich sicher zu stellen, dass der Unterauftragsverarbeiter gegenüber dem Auftragsverarbeiter in entsprechender Weise verpflichtet ist, wie der Auftragsverarbeiter gegenüber dem Verantwortlichen nach diesem Vertrag verpflichtet ist. Der Auftragsverarbeiter hat die Einhaltung dieser Pflichten des Unterauftragsverarbeiters, insbesondere die Einhaltung der dort

vereinbarten technischen und organisatorischen Maßnahmen, vor Beginn der Datenverarbeitung und sodann regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

- (4) Der Auftragsverarbeiter stellt ferner sicher und sichert vertraglich ab, dass der Verantwortliche gegenüber dem Unterauftragsverarbeiter die gleichen Kontrollrechte wie der Verantwortliche sie gegenüber dem Auftragsverarbeiter selbst hat. Diese vertragliche Absicherung ist so zu gestalten, dass sie den Verantwortlichen – unbeschadet der Verantwortlichkeit des Auftragsverarbeiters für den Unterauftragsverarbeiter – unmittelbar gegenüber dem Unterauftragsverarbeiter berechtigt. Auf Anforderung ist der Auftragsverarbeiter verpflichtet, dem Verantwortlichen Auskunft über den für die Kontrollrechte wesentlichen Vertragsinhalt und über die Umsetzung der datenschutzrelevanten Verpflichtungen durch den Subunternehmer zu geben.
- (5) Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- (6) Der Einsatz von Unter-Unterauftragsverarbeitern ist unzulässig. Der Auftragsverarbeiter wird seinen Unterauftragsverarbeitern vertraglich untersagen, ihrerseits weitere Unterauftragsverarbeiter einzusetzen.
- (7) Nicht zu den Unterauftragsverhältnissen gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistung, Post-/Transportdienstleistungen, Wartung und Benutzerservice, die Entsorgung von Datenträgern sowie Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Software- und der IT-Systeme in Anspruch nimmt. Der Auftragsverarbeiter ist jedoch verpflichtet, auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen und Kontrollmaßnahmen zu ergreifen, um den Datenschutz und die Datensicherheit der Daten des Verantwortlichen zu gewährleisten.

## **§ 9 Rückgabe, Löschung und Beendigung**

- (1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung des Auftrages – hat der Auftragsverarbeiter die Daten des Verantwortlichen sowie die weiteren Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, sämtliche in seinen Besitz gelangten Unterlagen sowie erstellte Verarbeitungs- und Nutzungsergebnisse dem Verantwortlichen nach dessen schriftlicher

Anweisung auszuhändigen oder datenschutzkonform zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung oder der Vernichtung ist auf Anforderung vorzulegen.

- (2) Unberührt bleiben Sicherungskopien zur Erfüllung von Haftungs- und Gewährleistungsansprüchen. Der Auftragsverarbeiter wird diese Gegenstände bis zu deren vollständiger Übergabe an den Verantwortlichen für diesen verwahren und ihm auf erstes Anfordern herausgeben. Der Auftragsverarbeiter sichert diese Gegenstände insbesondere durch ordnungsgemäße Verwahrung und Archivierung gegen Beschädigung und Verlust. Sicherungskopien sind durch geeignete Maßnahmen zu sperren, so dass eine Nutzung durch den Auftragsverarbeiter ausgeschlossen ist. Der Auftragsverarbeiter erteilt dem Verantwortlichen jederzeit Auskunft über solche Sicherungskopien.
- (3) Nicht mehr benötigte Unterlagen und Dateien dürfen erst nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen datenschutzgerecht unter Erbringung eines Nachweises vernichtet werden.
- (4) Dokumentationen, die dem Nachweis der Auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

## **§ 10 Haftung**

- (1) Die Parteien haften gegenüber Dritten nach Art. 82 DS-GVO.
- (2) Der Innenausgleich zwischen Verantwortlichem und Auftragsverarbeiter richtet sich nach Art. 82 Abs. 5 DS-GVO.

## **§ 11 Kündigung**

Der Verantwortliche kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

## **§ 12 Schlussbestimmungen**

- (1) Sollten Daten des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (z.B. Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse

gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen. Der Auftragsverarbeiter hat außerdem den Dritten darauf hinzuweisen, dass es sich um Daten des Verantwortlichen handelt und der Auftragsverarbeiter die Daten nur im Auftrag verarbeitet.

- (2) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (3) Bei etwaigen Widersprüchen zu anderen vertraglichen Regelungen gehen die Regelungen dieses Vertrags vor.
- (4) Änderungen und Ergänzungen dieses Vertrags und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung, die auch in elektronischer Form erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (5) Die Unwirksamkeit einer Bestimmung dieses Vertrags berührt die Gültigkeit der übrigen Bestimmungen nicht. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.
- (6) Es gilt deutsches Recht.

-----  
Datum und  
Unterschrift Verantwortlicher

-----  
Datum und  
Unterschrift Auftragsverarbeiter

# Anlage 1 zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

## Technische und organisatorische Maßnahmen für KI-Services der GWDG

### Inhalt

|                          |   |
|--------------------------|---|
| Chat AI .....            | 2 |
| LLM-Backend via API..... | 7 |

## Chat AI

Der Auftragnehmer führt die vereinbarte Leistung ausschließlich im Rahmen der getroffenen Vereinbarungen nach dem Gegenstand und der Dauer des Auftrags durch.

### § 1 Umfang, Art und Zweck der vorgesehenen Datenverarbeitung

- (1) Der Auftragnehmer verarbeitet im Rahmen seines Auftrags folgende personenbezogenen Daten: von Nutzer\*innen abgelegte Massendaten ("Prompt-Inhalte"). Über den Inhalt der Daten kann keine Aussage getroffen werden. Eine Ablage von Daten oberhalb der für diesen Dienst angegebenen Schutzstufe ohne weitere Schutzmaßnahmen widerspricht der Nutzungsordnung.
- (2) Die personenbezogenen Daten betreffen die folgenden Personengruppen:  
Auszubildende\*n; Autoren\*innen; Arbeitnehmer\*innen/Beschäftigte;  
Besucher\*innen; Bewerber\*innen; Diplomanden\*innen; Doktoranden\*innen;  
Drittmittelgeber\*innen; ehem. Beschäftigte/Emeriti\*e; Fachbeiratsmitglieder;  
Familienmitglieder; Förderer\*innen / Zuwendungsgeber\*innen; Gäste (mit dem Gastvertrag); Gutachter\*innen; Hilfskräfte; Honorarkräfte; Interne Gremien;  
Kooperations-/Projektpartner\*innen; Kuratorium Mitglieder; Mieter\*innen;  
Nutzer\*innen; Patienten\*innen; Praktikanten\*innen; Stipendiaten\*innen;  
Studenten\*innen; Studienteilnehmer\*innen/Testpersonen/Probanden\*innen;  
Vereinsmitglieder der MPG;  
Vertragspartner\*innen/Dienstleister\*innen/Berater\*innen; Wissenschaftliche Mitglieder (auswärtige/MPG)
- (3) Die Datenverarbeitung erfolgt ausschließlich zu folgenden Zwecken: Erbringung und Abrechnung eines KI-getriebenen Chat Services.
- (4) Die Daten werden nach dem Schutzstufenkonzept der Landesdatenschutzbehörde Niedersachsen eingeordnet.  
☐ A  
  
☒ B  
☐ C  
☐ D  
☐ E

### § 2 Technische und organisatorische Maßnahmen

Die vom Auftragnehmer zu ergreifenden technischen und organisatorischen Maßnahmen werden wie folgt festgelegt:

#### A.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b) DS-GVO)

Schutz vor physischem Zutritt

Wie wird sichergestellt, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird?

☒ Gebäudesicherung: Videoüberwachung und/oder Wachdienst und/oder schlüsselbasierte Zutrittskontrollsystem

☒ Zutrittsberechtigungen: Schlüsselregelung und/oder Personenkontrolle durch Pförtner\*innen

☒ Dokumentation des Zutritts

### Zugangskontrolle

Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?

☒ Einsatz von Verschlüsselungsverfahren von (mobilen) Datenträgern und/oder Firewall-Systemen und/oder Virens Scanner

☒ Authentifizierung gegenüber dem System: Benutzerkennung mit Password, ggf. Zweifaktor Authentifizierung

☒ Einsatz von VPN bei administrativen Remote-Zugängen

### Zugriffskontrolle

Wie wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können?

☒ Rollenkonzept zur Vergabe der Zugriffsberechtigung für Systeme und Papierakten

☐ Unterschiedliche Berechtigungen für Lese- und Schreibzugriffe

☐ Einsatz von Verschlüsselungsverfahren von Daten/Dateien

### Trennungskontrolle

Wie stellt der Auftragnehmer sicher, dass Daten des Auftraggebers von sonstigen Datenbeständen getrennt werden?

☒ (Logische und/oder physische) Trennung der Daten auf Netz-/Systemebene

☐ (Logische) Trennung über Zugriffsregelung

☐ Mandanten - Trennung: Mandanten - Aufteilung ist ermöglicht

☒ Funktionstrennung: Trennung von Test, Entwicklungs- und Produktivprogrammen

## Pseudonymisierung

Die Verarbeitung personenbezogener Daten in der Weise, dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer betroffenen Person zugeordnet werden können, vorausgesetzt, die zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen entsprechenden technischen und organisatorischen Maßnahmen.

☐ Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System

## A.2 Integrität (Art. 32 Abs. 1 lit. b) DS-GVO)

### Weitergabekontrolle

Wie wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist?

☒ Transportverschlüsselung

☒ E-Mail: Digitale Signatur

☐ E-Mail-Verschlüsselung

☒ Umsetzung der Regelungen zum Gebrauch von mobilen Datenträgern (optische Datenträger, Magnetbänder, USB-Sticks)

☐ Verschlüsselung von mobilen Datenträgern

☒ Transportsicherung: Umsetzung der Regelungen zur sicheren Lagerung und zum sicheren Transport von mobilen Datenträgern und Papierakten (mechanische Sicherung)

### Eingabekontrolle

Wie wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind?

☒ Protokollierung der Systemnutzung

☐ Protokollierung der Eingaben

☒ Benutzer\*innen dürfen Protokolle nicht ändern oder löschen können

### Löschkontrolle

Wie wird gewährleistet, dass personenbezogene Daten ordnungsgemäß gelöscht werden?

- ☒ Kontrollierte Datenlöschung: Umsetzung der technisch/organisatorischen Vorgaben wie/wann gelöscht werden soll
- ☒ Umsetzung der Regelungen zur Datenträgervernichtung und/oder Papierakten
- ☒ Verfahren beim Ausscheiden von Beschäftigten: Deaktivieren/Löschen der Benutzerkonten

### A.3 Betriebskontinuität und Belastbarkeit (Art. 32 Abs. 1 lit. b) DS-GVO)

#### Betriebskontinuitätsmanagement

Wie wird gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind?

- ☒ Getesteter Backup-Prozess
- ☒ Redundanz auf System-/Speicherebene
- ☒ Brandschutzkonzept: Branderkennung und/oder Brandschutzmaßnahme
- ☒ Schutz vor Wasserschäden
- ☒ Unterbrechungsfreie Stromversorgung und/oder Notstromaggregate
- ☒ Notfallplan

#### A.4 Auftragskontrolle (Art. 28 Abs. 3 lit. a), lit b), 32 Abs. 4 DS-GVO)

##### Auftragskontrolle

Der Auftragnehmer stellt sicher, dass allen von ihm eingesetzten Beschäftigten vor Aufnahme ihrer Tätigkeit alle für sie relevanten Datenschutzvorgaben bekannt sind. Hierzu gehören insbesondere die Anweisungen des Auftraggebers zur Erbringung der im Dienstleistungsvertrag festgelegten Leistungen.

☐ Auswahl von Auftragnehmer: Kriterien zur Auswahl der Auftragnehmer bestehen

☒ Vertrag: Das Muster der Academic Cloud zur Auftragsverarbeitung wird verwendet

☒ Die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen ist sichergestellt: Vor-Ort-Kontrolle, Zertifikate, etc.

☐ Datenverarbeitung außerhalb der EU/EWR

#### A.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DS-GVO, Art. 25 Abs. 1 DS-GVO)

##### Beschreibung der internen/externen Audits und Managementbewertung

☒ Überprüfung der technischen und organisatorischen Maßnahmen wird auf Wirksamkeit mindestens jährlich durchgeführt

## LLM-Backend via API

Der Auftragnehmer führt die vereinbarte Leistung ausschließlich im Rahmen der getroffenen Vereinbarungen nach dem Gegenstand und der Dauer des Auftrags durch.

### § 1 Umfang, Art und Zweck der vorgesehenen Datenverarbeitung

- (1) Der Auftragnehmer verarbeitet im Rahmen seines Auftrags folgende personenbezogenen Daten: Berechtigungen/Profile; Kontaktdaten; Verbindungsdaten/Nutzungsdaten, Massendaten der Nutzer\*innen (über den Inhalt der Daten kann keine Aussage getroffen werden. Eine Ablage von Daten oberhalb der für diesen Dienst angegebenen Schutzstufe ohne weitere Schutzmaßnahmen widerspricht der Nutzungsordnung), Anzahl der Anfragen pro Nutzer\*In, Anzahl der Input und Output Tokens pro Anfrage.
- (2) Die personenbezogenen Daten betreffen die folgenden Personengruppen: Auszubildende\*n; Autoren\*innen; Arbeitnehmer\*innen/Beschäftigte; Besucher\*innen; Bewerber\*innen; Diplomanden\*innen; Doktoranden\*innen; Drittmittelgeber; ehem. Beschäftigte/Emeriti\*e; Fachbeirat Mitglieder; Familienmitglieder; Förderer\*innen / Zuwendungsgeber\*innen; Gäste (mit dem Gastvertrag); Gutachter\*innen; Hilfskräfte; Honorarkräfte; Interne Gremien; Kooperations-/Projektpartner\*innen; Kuratorium Mitglieder; Mieter\*innen; Nutzer\*innen; Patienten\*innen; Praktikanten\*innen; Stipendiaten\*innen; Studenten\*innen; Studienteilnehmer\*innen/Testpersonen/Probanden\*innen; Vereinsmitglieder der MPG; Vertragspartner\*innen/Dienstleister\*innen/Berater\*innen; Wissenschaftliche Mitglieder (auswärtige/MPG)
- (3) Die Datenverarbeitung erfolgt ausschließlich zu folgenden Zwecken: Erbringung und Abrechnung Services zur Bereitstellung von Large Language Models (LLM)
- (4) Die Daten werden nach dem Schutzstufenkonzept der Landesdatenschutzbehörde Niedersachsen eingeordnet.
  - ☐ A
  - ☒ B
  - ☐ C
  - ☐ D
  - ☐ E

### § 2 Technische und organisatorische Maßnahmen

Die vom Auftragnehmer zu ergreifenden technischen und organisatorischen Maßnahmen werden wie folgt festgelegt:

#### A.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b) DS-GVO)

Schutz vor physischem Zutritt

Wie wird sichergestellt, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird?

☒ Gebäudesicherung: Videoüberwachung und/oder Wachdienst und/oder schlüsselbasierte Zutrittskontrollsystem

☒ Zutrittsberechtigungen: Schlüsselregelung und/oder Personenkontrolle durch Pförtner\*innen

☒ Dokumentation des Zutritts

### Zugangskontrolle

Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?

☒ Einsatz von Verschlüsselungsverfahren von (mobilen) Datenträgern und/oder Firewall-Systemen und/oder Virens Scanner

☒ Authentifizierung gegenüber dem System: Benutzerkennung mit Password, ggf. Zweifaktor Authentifizierung

☒ Einsatz von VPN bei administrativen Remote-Zugängen

### Zugriffskontrolle

Wie wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können?

☒ Rollenkonzept zur Vergabe der Zugriffsberechtigung für Systeme und Papierakten

☐ Unterschiedliche Berechtigungen für Lese- und Schreibzugriffe

☐ Einsatz von Verschlüsselungsverfahren von Daten/Dateien

### Trennungskontrolle

Wie stellt der Auftragnehmer sicher, dass Daten des Auftraggebers von sonstigen Datenbeständen getrennt werden?

☒ (Logische und/oder physische) Trennung der Daten auf Netz-/Systemebene

☐ (Logische) Trennung über Zugriffsregelung

☐ Mandanten - Trennung: Mandanten - Aufteilung ist ermöglicht

☒ Funktionstrennung: Trennung von Test, Entwicklungs- und Produktivprogrammen

## Pseudonymisierung

Die Verarbeitung personenbezogener Daten in der Weise, dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer betroffenen Person zugeordnet werden können, vorausgesetzt, die zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen entsprechenden technischen und organisatorischen Maßnahmen.

- ☐ Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System

## A.2 Integrität (Art. 32 Abs. 1 lit. b) DS-GVO)

### Weitergabekontrolle

Wie wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist?

- ☒ Transportverschlüsselung
- ☒ E-Mail: Digitale Signatur
- ☐ E-Mail-Verschlüsselung
- ☒ Umsetzung der Regelungen zum Gebrauch von mobilen Datenträgern (optische Datenträger, Magnetbänder, USB-Sticks)
- ☐ Verschlüsselung von mobilen Datenträgern
- ☒ Transportsicherung: Umsetzung der Regelungen zur sicheren Lagerung und zum sicheren Transport von mobilen Datenträgern und Papierakten (mechanische Sicherung)

### Eingabekontrolle

Wie wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind?

- ☒ Protokollierung der Systemnutzung
- ☐ Protokollierung der Eingaben
- ☒ Benutzer\*innen dürfen Protokolle nicht ändern oder löschen können

### Löschkontrolle

Wie wird gewährleistet, dass personenbezogene Daten ordnungsgemäß gelöscht werden?

- ☒ Kontrollierte Datenlöschung: Umsetzung der technisch/organisatorischen Vorgaben wie/wann gelöscht werden soll
- ☒ Umsetzung der Regelungen zur Datenträgervernichtung und/oder Papierakten
- ☒ Verfahren beim Ausscheiden von Beschäftigten: Deaktivieren/Löschen der Benutzerkonten

### A.3 Betriebskontinuität und Belastbarkeit (Art. 32 Abs. 1 lit. b) DS-GVO)

#### Betriebskontinuitätsmanagement

Wie wird gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind?

- ☒ Getesteter Backup-Prozess
- ☒ Redundanz auf System-/Speicherebene
- ☒ Brandschutzkonzept: Branderkennung und/oder Brandschutzmaßnahme
- ☒ Schutz vor Wasserschäden
- ☒ Unterbrechungsfreie Stromversorgung und/oder Notstromaggregate
- ☒ Notfallplan

### A.4 Auftragskontrolle (Art. 28 Abs. 3 lit. a), lit b), 32 Abs. 4 DS-GVO)

#### Auftragskontrolle

Der Auftragnehmer stellt sicher, dass allen von ihm eingesetzten Beschäftigten vor Aufnahme ihrer Tätigkeit alle für sie relevanten Datenschutzvorgaben bekannt sind. Hierzu gehören insbesondere die Anweisungen des Auftraggebers zur Erbringung der im Dienstleistungsvertrag festgelegten Leistungen.

- ☐ Auswahl von Auftragnehmer: Kriterien zur Auswahl der Auftragnehmer bestehen
- ☒ Vertrag: Das Muster der Academic Cloud zur Auftragsverarbeitung wird verwendet
- ☒ Die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen ist sichergestellt: Vor-Ort-Kontrolle, Zertifikate, etc.
- ☐ Datenverarbeitung außerhalb der EU/EWR

A.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung  
(Art. 32 Abs. 1 lit. d) DS-GVO, Art. 25 Abs. 1 DS-GVO)

Beschreibung der internen/externen Audits und Managementbewertung

☒ Überprüfung der technischen und organisatorischen Maßnahmen wird auf Wirksamkeit mindestens jährlich durchgeführt

Anlage 2 zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Unterauftragsverarbeiter gemäß § 8 Absatz 1

| Firma                                                                      | Funktion                                                                 |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------|
| SerNet Service Network GmbH<br>Bahnhofsallee 1b<br>37081 Göttingen         | Service Monitoring und Fehlerbehebung                                    |
| B1 Systems<br>Osterfeldstraße 7<br>85088 Vohburg an der Donau              | Support für Installation und Wartung von<br>Compute und Storage Services |
| T-Systems<br>Querstraße 1<br>04103 Leipzig                                 | Netzwerkunterstützung                                                    |
| Bechtle GmbH<br>IT-Systemhaus Meschede<br>Dünnefeldweg 1<br>59872 Meschede | Zugang zu Microsoft Azure Cloud Services                                 |
| DFN-Verein<br>Alexanderplatz 1<br>10178 Berlin                             | Netzwerkunterstützung                                                    |