Auftragsverarbeitungsvertrag
Data Processing Agreement

Dieser Auftragsverarbeitungsvertrag wird zwischen der Melious AI GmbH, Campus Starterzentrum, Geb. A1.2, 66123 Saarbrücken (im Folgenden als „Auftragsnehmerin“ bezeichnet) und dem Unternehmen, das diesen akzeptiert (im Folgenden als „Auftragsgeberin“ bezeichnet; einzeln als „Partei“ und gemeinsam als „Parteien“ bezeichnet), geschlossen.

This Data Processing Agreement is entered into by Melious AI GmbH, Campus Starterzentrum, Geb. A1.2 , 66123 Saarbrücken (hereinafter referred to as “Processor”) and the entity accepting them (herein after referred to as “Controller”; individually referred to as “Party” and together as the “Parties”).

Präambel	**Preamble**
Die Auftragnehmerin erbringt für die Auftraggeberin Leistungen im Bereich der KI-Inferenz und der ergänzenden Plattformdienste aufgrund der unter https://melious.ai/legal/terms akzeptierten Allgemeinen Geschäftsbedingungen der Auftragnehmerin (im Folgenden: „Hauptvertrag“).	The Processor provides the Controller with services in the field of AI inference and complementary platform services on the basis of the General Terms and Conditions of the Processor accepted at https://melious.ai/legal/terms (hereinafter: "Principal Agreement").
Teil der Durchführung des Hauptvertrags ist die Verarbeitung von personenbezogenen Daten im Sinne der Datenschutz-Grundverordnung („DS-GVO“). Zur Erfüllung der Anforderungen der DS-GVO an derartige Konstellationen schließen die Parteien den nachfolgenden Vertrag.	Part of the performance of the Principal Agreement is the processing of personal data within the meaning of the General Data Protection Regulation ("GDPR"). In order to meet the requirements of the GDPR for constellations of this kind, the Parties enter into the following Agreement.
1. Vertragsgegenstand	**1. Subject Matter of the Agreement**
1.1 Die Zusammenarbeit der Parteien bringt mit sich, dass die Auftragnehmerin im Rahmen der Durchführung des Hauptvertrags personenbezogene Daten, welche die Auftraggeberin gemäß Art. 4 Nr. 7 DS-GVO verantwortet (nachfolgend „Auftraggeberdaten“), verarbeitet.	1.1 The cooperation between the Parties entails that, within the scope of performing the Principal Agreement, the Processor processes personal data for which the Controller is responsible pursuant to Art. 4 No. 7 GDPR (hereinafter "Controller Data").
1.2 Die Verarbeitung der Auftraggeberdaten durch die Auftragnehmerin erfolgt ausschließlich zur Erfüllung des Hauptvertrages und ist auch beschränkt auf diesen Zweck. Zweck der Verarbeitung ist die Erbringung der im Hauptvertrag vereinbarten Leistungen, insbesondere die Bereitstellung von KI-Modellen zur Inferenz über API und Weboberfläche sowie der ergänzenden Plattformdienste. Die dementsprechende Datenverarbeitung wird in Anlage 1 in fortlaufender Versionierung hinsichtlich der Verarbeitungsvorgänge (Art der Verarbeitung), Datenkategorien und Kategorien betroffener Personen beschrieben und dokumentiert. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.	1.2 The Processor processes Controller Data exclusively for the purpose of performing the Principal Agreement, and the processing is also limited to this purpose. The purpose of the processing is the provision of the services agreed in the Principal Agreement, in particular the provision of AI models for inference via API and web interface as well as the complementary platform services. The respective data processing is described and documented in Annex 1, under continuous versioning, in terms of processing operations (type of processing), categories of data and categories of data subjects. The duration of the processing corresponds to the term of the Principal Agreement.
1.3 Die Verarbeitung der Auftraggeberdaten findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf, vorbehaltlich der Ziffer 6.4. der vorherigen schriftlichen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DS-GVO erfüllt sind.	1.3 The processing of Controller Data takes place in principle within the territory of the Federal Republic of Germany, in a Member State of the European Union or in another Contracting State to the Agreement on the European Economic Area. Any transfer to a third country requires, subject to Clause 6.4, the Controller’s prior written consent and may only take place if the specific conditions of Art. 44 to 49 GDPR are met.
1.4 Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen die Auftragnehmerin oder ihre Erfüllungsgehilfen Auftraggeberdaten verarbeiten.	1.4 The provisions of this Agreement shall apply to all activities connected with the Principal Agreement in which the Processor or its vicarious agents process Controller Data.

2. Weisungsbefugnisse der Auftraggeberin

2.1 Die Auftragnehmerin verarbeitet die Auftraggeberdaten ausschließlich nach Weisung der Auftraggeberin. Dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Die Auftraggeberin hat insoweit das alleinige Recht, Weisungen über Zwecke und Mittel der Verarbeitung von Auftraggeberdaten zu erteilen (nachfolgend auch „Weisungsrecht“). Wird die Auftragnehmerin durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem sie unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt sie der Auftraggeberin diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht verbietet.

2.2 Weisungen werden von der Auftraggeberin grundsätzlich schriftlich, im erweiterten Sinne des § 127 Abs. 2 BGB, erteilt; mündlich erteilte Weisungen sind von der Auftragnehmerin in dieser Form zu bestätigen. Die weisungs- und empfangsberechtigten Personen aufseiten der Parteien ergeben sich aus Anlage 2. Bei einem Wechsel oder einer längerfristigen Verhinderung der in Anlage 2 benannten Personen ist der anderen Partei unverzüglich der Nachfolger bzw. Vertreter in Schriftform zu benennen. Bis zum Zugang einer solchen Mitteilung beim Auftraggeber gelten die benannten Personen weiter als empfangsberechtigt.

2.3 Ist die Auftragnehmerin der Ansicht, dass eine Weisung der Auftraggeberin gegen datenschutzrechtliche Bestimmungen verstößt, hat sie die Auftraggeberin unverzüglich unter Angabe von Gründen darauf hinzuweisen. Die Auftragnehmerin ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch die Auftraggeberin bestätigt oder geändert wird.

2. The Controller’s Authority to Issue Instructions

2.1 The Processor processes Controller Data exclusively on the instructions of the Controller. This applies in particular to the transfer of personal data to a third country or to an international organisation. In this respect, the Controller has the exclusive right to issue instructions on the purposes and means of the processing of Controller Data (hereinafter also "right to instruct"). If the Processor is bound by the law of the European Union or the Member States to which it is subject to carry out further processing, it shall notify the Controller of these legal requirements prior to the processing, insofar as the relevant law does not prohibit such notification.

2.2 Instructions shall as a rule be issued by the Controller in writing within the extended meaning of § 127 (2) of the German Civil Code (BGB); instructions issued orally shall be confirmed by the Processor in that form. The persons entitled to give and to receive instructions on the part of the Parties are set out in Annex 2. In the event of a change or a longer-term impediment of the persons named in Annex 2, the successor or representative shall be notified to the other Party without delay in written form. Until such notification is received by the Controller, the persons named shall continue to be deemed authorised recipients.

2.3 If the Processor takes the view that an instruction of the Controller infringes data protection provisions, it shall point this out to the Controller without delay, stating the reasons. The Processor shall be entitled to suspend execution of the instruction concerned until it has been confirmed or amended by the Controller.

3. Schutzmaßnahmen der Auftragnehmerin

3.1 Die Auftragnehmerin ist verpflichtet, Auftraggeberdaten gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik dem jeweiligen Risiko angemessen zu sichern.

3.2 Ferner wird die Auftragnehmerin sämtliche Personen, die von ihr mit der Verarbeitung von Auftraggeberdaten betraut sind oder werden, Kenntnis von diesen haben oder erlangen, Zugang zu ihnen haben oder erlangen oder denen Auftraggeberdaten in sonstiger Weise verfügbar sind oder werden (im Folgenden „Mitarbeiter“ genannt), in Schriftform zur Vertraulichkeit verpflichten und die Einhaltung dieser Verpflichtung mit der gebotenen Sorgfalt sicherstellen. Auf Verlangen der Auftraggeberin wird die Auftragnehmerin ihr die entsprechende Verpflichtung der Mitarbeiter in geeigneter Form nachweisen.

3.3 Die Auftragnehmerin wird ihre betriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie verpflichtet sich, jederzeit sämtliche geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeberdaten gem. Art. 32 DS-GVO, insbesondere die in Anlage 3 zu diesem Vertrag

3. Protective Measures of the Processor

3.1 The Processor is obliged to secure Controller Data against being taken note of by unauthorised persons, taking into account the state of the art, in a manner appropriate to the respective risk.

3.2 Furthermore, the Processor shall oblige in writing to maintain confidentiality all persons who are or will be entrusted by it with the processing of Controller Data, who have or obtain knowledge thereof, who have or obtain access thereto, or to whom Controller Data is or becomes available in any other manner (hereinafter referred to as "employees"), and shall ensure compliance with this obligation with the requisite care. Upon the Controller’s request, the Processor shall demonstrate to it the corresponding commitment of the employees in an appropriate form.

3.3 The Processor shall organise its operations in such a way that it meets the special requirements of data protection. It undertakes to take at all times all appropriate technical and organisational measures for the adequate protection of the Controller Data pursuant to Art. 32 GDPR, in particular the measures set out in Annex 3 to this Agreement, and to

aufgeführten Maßnahmen, zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrechtzuerhalten.

maintain them for the duration of the processing of the Controller Data.

3.4 Eine Änderung der implementierten technischen und organisatorischen Maßnahmen bleibt der Auftragnehmerin vorbehalten, wobei sie sicherstellt, dass weder das vertraglich vereinbarte noch das gesetzlich erforderliche Schutzniveau unterschritten werden. Die Auftragnehmerin hat die Auftraggeberin unverzüglich schriftlich zu informieren, wenn sie Grund zu der Annahme hat, dass die Maßnahmen gemäß Anlage 3 nicht mehr ausreichend sind, und wird sich mit ihr hinsichtlich weiterer technischer und organisatorischer Maßnahmen abstimmen.

3.4 The Processor reserves the right to modify the implemented technical and organisational measures, whereby it ensures that neither the contractually agreed nor the legally required level of protection is fallen short of. The Processor shall inform the Controller immediately in writing if it has reason to believe that the measures under Annex 3 are no longer sufficient, and shall consult with the Controller on further technical and organisational measures.

3.5 Auf Verlangen der Auftraggeberin wird die Auftragnehmerin der Auftraggeberin die Einhaltung und Wirksamkeit der jeweils ergriffenen technischen und organisatorischen Maßnahmen in geeigneter Form, insbesondere durch geeignete Dokumentationen nachweisen.

3.5 Upon the Controller's request, the Processor shall demonstrate to the Controller the compliance with and effectiveness of the respectively applied technical and organisational measures in an appropriate form, in particular by means of suitable documentation.

3.6 Auf den von der Auftragnehmerin selbst betriebenen Servern wie in Annex 4 entsprechend gekennzeichneten Anbietern verpflichtet sich die Auftragnehmerin zu einer Verarbeitung ohne Datenspeicherung („Zero Data Retention"): Eingaben und die daraus erzeugten Ausgaben werden ausschließlich im flüchtigen Speicher verarbeitet und weder dauerhaft gespeichert noch protokolliert noch zum Training von KI-Modellen verwendet. Ausgenommen sind Daten, die der Auftraggeber über Speicherfunktionen ablegt (insbesondere Batch-API, Dateien, Vektorspeicher, Vault), Betriebsmetadaten gemäß Anlage 1 sowie gesetzlich vorgeschriebene Verarbeitungen gemäß Ziffer 2.1 Satz 4. Für sonstige Unterauftragsverarbeiter gilt diese Ziffer nicht.

3.6 On the servers operated by the Processor itself as well as by the providers marked accordingly in Annex 4, the Processor undertakes to processing without data storage ("Zero Data Retention"): inputs and the outputs generated therefrom are processed exclusively in volatile memory and are neither permanently stored nor logged nor used for the training of AI models. Excluded are data which the Controller stores by means of storage functions (in particular batch API, files, vector store, vault), operational metadata pursuant to Annex 1 as well as processing required by law pursuant to Clause 2.1 sentence 4. This clause does not apply to other subprocessors.

4. Informations- und Unterstützungspflichten der Auftragnehmerin

4. Information and Assistance Obligations of the Processor

4.1 Werden der Auftragnehmerin Verletzungen des Schutzes von Auftraggeberdaten in ihrem Einfluss- oder Verantwortungsbereich, also im Zusammenhang mit der Verarbeitung von Auftraggeberdaten durch sie, Mitarbeiter oder Unterauftragsverarbeiter, die ihre Verarbeitung von Auftraggeberdaten mittelbar oder unmittelbar von der Auftragnehmerin ableiten, bekannt, so wird sie die Auftraggeberin hiervon unverzüglich in Kenntnis setzen. Das Gleiche gilt, wenn die Auftragnehmerin Kenntnis von Umständen erlangt, welche eine solche Verletzung des Schutzes von Auftraggeberdaten konkret befürchten lassen. Dasselbe gilt zuletzt für Prüfungen der Auftragnehmerin durch die Datenschutz-Aufsichtsbehörde. Die Meldung enthält, soweit der Auftragnehmerin bekannt, eine Beschreibung des Vorfalls, der betroffenen Datenkategorien, der ungefähren Zahl betroffener Personen und Datensätze, der wahrscheinlichen Folgen und der ergriffenen Maßnahmen sowie eine Anlaufstelle für Rückfragen. Fehlende Angaben reicht die Auftragnehmerin nach, sobald sie vorliegen; die Erstmeldung wird dadurch nicht verzögert. Eine Meldung durch die Auftragnehmerin geschieht in jedem Fall so zeitnah, dass der Auftraggeberin eine Erfüllung ihrer gesetzlichen Meldepflichten möglich ist.

4.1 If violations of the protection of Controller Data within the Processor's sphere of influence or responsibility – i.e. in connection with the processing of Controller Data by it, by employees or by subprocessors which derive their processing of Controller Data directly or indirectly from the Processor – become known to the Processor, it shall inform the Controller thereof without delay. The same applies if the Processor obtains knowledge of circumstances which give concrete cause to fear such a violation of the protection of Controller Data. The same applies, finally, to examinations of the Processor by the data protection supervisory authority. The notification shall contain, to the extent known to the Processor, a description of the incident, the categories of data affected, the approximate number of data subjects and records concerned, the likely consequences and the measures taken, as well as a contact point for enquiries. The Processor shall provide any missing information subsequently as soon as it becomes available; the initial notification shall not be delayed thereby. Any notification by the Processor shall in any case be made in due time so as to enable the Controller to comply with its statutory notification obligations.

4.2 Die Auftragnehmerin wird die Auftraggeberin im Falle des Ziffer 4.1 bei der Erfüllung ihrer diesbezüglichen

4.2 In the event referred to in Clause 4.1, the Processor shall assist the Controller to the necessary extent in fulfilling its

Aufklärungs-, Abhilfe- und Informationsmaßnahmen im erforderlichen Maß unterstützen. Die Auftragnehmerin wird insbesondere unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für betroffene Personen durchführen, die Auftraggeberin hierüber informieren und diese, soweit dies möglich ist und unverzichtbare Risikominderungs- und Abhilfemaßnahmen nicht verhindert oder verzögert, um weitere Weisungen ersuchen.

investigative, remedial and information measures. In particular, the Processor shall immediately take the necessary measures to secure the data and to mitigate possible adverse effects on data subjects, inform the Controller thereof and, insofar as this is possible and indispensable risk mitigation and remedial measures are not prevented or delayed, request further instructions.

4.3 Die Auftragnehmerin verpflichtet sich, der Auftraggeberin auf deren schriftliche Anforderung innerhalb einer angemessenen Frist sämtliche Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle gemäß Ziffer 7.1 dieses Vertrages erforderlich sind. Ferner wird die Auftragnehmerin der Auftraggeberin auf deren Wunsch ein vollständiges, korrektes und aktuelles Datenschutz- und Sicherheitskonzept betreffs der Auftraggeberdaten zur Verfügung stellen. Sie wird ferner auf Anforderung der Auftraggeberin geeignete Belege vorlegen, welche die Risikoangemessenheit, Umsetzung und Wirksamkeit der darin vorgesehenen Maßnahmen belegen.

4.3 The Processor undertakes to provide the Controller, upon its written request and within a reasonable period, with all information and evidence required for carrying out an audit pursuant to Clause 7.1 of this Agreement. Furthermore, the Processor shall, at the Controller's request, provide it with a complete, accurate and up-to-date data protection and security concept relating to the Controller Data. It shall furthermore, upon the Controller's request, submit appropriate records demonstrating the risk adequacy, implementation and effectiveness of the measures provided for therein.

5. Sonstige Verpflichtungen der Auftragnehmerin

5.1 Die Auftragnehmerin ist verpflichtet, ein vollständiges Verzeichnis der im Auftrag der Auftraggeberin durchgeführten Tätigkeiten der Verarbeitung von Auftraggeberdaten gem. Art. 30 Abs. 2 DS-GVO zu führen. Das Verzeichnis ist der Auftraggeberin auf Verlangen zur Verfügung zu stellen.

5. Other Obligations of the Processor

5.1 The Processor is obliged to maintain a complete record of the processing activities involving Controller Data carried out on behalf of the Controller pursuant to Art. 30 (2) GDPR. The record shall be made available to the Controller upon request.

5.2 Die Auftragnehmerin ist verpflichtet, die Auftraggeberin bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DS-GVO hinsichtlich der Erhebung und Analyse von Maßnahmen, Vorgängen, Verarbeitungstätigkeiten und Umständen der Datenverarbeitung in ihrem Einfluss- und Verantwortungsbereich zu unterstützen.

5.2 The Processor is obliged to assist the Controller in the preparation of a data protection impact assessment pursuant to Art. 35 GDPR and, where applicable, a prior consultation of the supervisory authority pursuant to Art. 36 GDPR, with regard to the collection and analysis of measures, processes, processing activities and circumstances of the data processing within its sphere of influence and responsibility.

5.3 Die Auftragnehmerin bestätigt, dass sie einen Datenschutzbeauftragten bestellt hat. Die Kontaktdaten des Datenschutzbeauftragten sind ePrivacy GmbH vertreten durch Prof. Dr. Christoph Bauer, Stefanie Bauer, Bei den Mühren 5, 20457 Hamburg, privacy@melious.de. Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist der Auftraggeberin unverzüglich schriftlich mitzuteilen.

5.3 The Processor confirms that it has appointed a data protection officer. The contact details of the data protection officer are: ePrivacy GmbH, represented by Prof. Dr. Christoph Bauer, Stefanie Bauer, Bei den Mühren 5, 20457 Hamburg, privacy@melious.de. Any change in the person of the operational data protection officer / data protection contact person shall be notified to the Controller without delay in writing.

5.4 Sollten die Auftraggeberdaten bei der Auftragnehmerin durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat die Auftragnehmerin die Auftraggeberin unverzüglich darüber zu informieren, sofern ihr dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Die Auftragnehmerin wird in diesem Zusammenhang alle zuständigen Stellen oder sonstigen Beteiligten unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich bei der Auftraggeberin als „Verantwortlicher" im Sinne der DS-GVO liegt.

5.4 If the Controller Data held by the Processor are put at risk by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Processor shall inform the Controller thereof without delay, insofar as it is not prohibited from doing so by a judicial or administrative order. In this context, the Processor shall immediately inform all competent authorities or other parties involved that the authority of disposition over the data lies exclusively with the Controller as the "controller" within the meaning of the GDPR.

6. Einbindung von Unterauftragsverarbeitern

6.1 Die Auftragnehmerin ist im Rahmen ihrer vertraglichen Verpflichtungen zur Begründung von Unterauftragsverhältnissen mit Unterauftragsverarbeitern („Unterauftragsverarbeitung“) befugt. Die Auftraggeberin erteilt hierzu ihre allgemeine Genehmigung im Sinne des Art. 28 Abs. 2 S. 2 DS-GVO.

6.2 Die Unterauftragsverarbeiter, welche bei Vertragsschluss durch die Auftragnehmerin mit der Verarbeitung von Auftraggeberdaten betraut sind oder werden, ergeben sich inklusive des Gegenstands ihrer Beauftragung aus Annex 4 zu diesem Vertrag.

6.3 Möchte die Auftragnehmerin eine oder mehrere weitere Unterauftragsverarbeitungen begründen oder Unterauftragsverarbeiter mit weiteren Verarbeitungen betrauen, hat die Auftragnehmerin dies der Auftraggeberin mindestens drei Wochen vor Beginn dieser Unterauftragsverarbeitung anzuzeigen. Diese Anzeige hat die Liste der Unterauftragsverarbeiter in Annex 4 in der nach Beginn dieser Unterauftragsverarbeitung maßgeblichen Fassung zu enthalten. Änderungen des Annex 4 gegenüber dem vorigen Stand sind kenntlich zu machen. Diese Anzeige hat schriftlich zu erfolgen, wobei § 127 Abs. 2 BGB gilt. Die Auftraggeberin kann der beabsichtigten Änderung innerhalb von 14 Tagen nach Zugang der Anzeige unter Angabe der datenschutzrechtlichen Gründe widersprechen. Im Falle eines Widerspruchs bemühen sich die Parteien um eine einvernehmliche Lösung; die Auftragnehmerin kann insbesondere anbieten, die betroffene Leistung ohne den betreffenden Unterauftragsverarbeiter zu erbringen. Kommt innerhalb von 14 Tagen nach Zugang des Widerspruchs keine Einigung zustande, ist jede Partei berechtigt, den Hauptvertrag und diesen Vertrag hinsichtlich der betroffenen Leistungen mit einer Frist von 14 Tagen zu kündigen. Bis zu einer Einigung oder bis zum Wirksamwerden der Kündigung verarbeitet der betreffende Unterauftragsverarbeiter keine Auftraggeberdaten. Erfolgt kein fristgerechter Widerspruch, gilt die Änderung als genehmigt. Die Auftragnehmerin hat ferner dafür Sorge zu tragen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den von ihr beauftragten Unterauftragsverarbeitern gelten, wobei der Auftraggeberin gegenüber dem Unterauftragsverarbeiter sämtliche Kontrollrechte gemäß Ziffer 7 dieses Vertrages einzuräumen sind.

6.4 Unterauftragsverarbeitungen durch Dritte außerhalb des Europäischen Wirtschaftsraumes sind nur gestattet, wenn diese Dritten

a) einem Angemessenheitsbeschluss nach Art. 45 Abs. 1 S. 1 DS-GVO unterfallen oder

b) mit diesen Unterauftragsverarbeitern Standarddatenschutzklauseln nach Art. 46 Abs. 2 lit. c DS-GVO wirksam vereinbart wurden.

Liegt keine dieser Voraussetzungen vor, ist die Unterauftragsverarbeitung nur zulässig, wenn die Voraussetzungen der Art. 46 bis 49 DS-GVO anderweitig erfüllt sind und die Auftraggeberin vorher in Textform zugestimmt hat.

6. Engagement of Subprocessors

6.1 Within the scope of its contractual obligations, the Processor is entitled to enter into sub-processing arrangements with subprocessors ("sub-processing"). The Controller hereby grants its general authorisation within the meaning of Art. 28 (2) sentence 2 GDPR.

6.2 The subprocessors which, at the time of conclusion of this Agreement, are or will be entrusted by the Processor with the processing of Controller Data, including the subject matter of their engagement, are set out in Annex 4 to this Agreement.

6.3 If the Processor intends to establish one or more further sub-processing arrangements or to entrust subprocessors with further processing, the Processor shall notify the Controller thereof at least three weeks before the commencement of such sub-processing. This notice shall contain the list of subprocessors in Annex 4 in the version applicable upon commencement of such sub-processing. Amendments to Annex 4 compared with the previous version shall be identified. The Controller may object to the intended amendment within 14 days of receipt of the notice, stating the data protection reasons. In the event of an objection, the Parties shall endeavour to reach an amicable solution; the Processor may in particular offer to provide the affected service without the subprocessor concerned. If no agreement is reached within 14 days of receipt of the objection, either Party shall be entitled to terminate the Principal Agreement and this Agreement with regard to the affected services subject to a notice period of 14 days. Until an agreement is reached or the termination takes effect, the subprocessor concerned shall not process any Controller Data. If no objection is lodged within due time, the amendment shall be deemed approved. Such notice shall be given in writing, whereby § 127 (2) BGB applies. The Processor shall furthermore ensure that the provisions agreed in this Agreement also apply vis-à-vis the subprocessors engaged by it, whereby the Controller shall be granted all audit rights pursuant to Clause 7 of this Agreement vis-à-vis the subprocessor.

6.4 Sub-processing by third parties outside the European Economic Area is only permitted if such third parties

a) are covered by an adequacy decision pursuant to Art. 45 (1) sentence 1 GDPR, or

b) Standard Data Protection Clauses pursuant to Art. 46 (2) (c) GDPR have been validly agreed with these subprocessors.

If none of these prerequisites is met, sub-processing shall only be permitted if the requirements of Art. 46 to 49 GDPR are fulfilled by other means and the Controller has given its prior consent in text form.

6.5 Eine Unterauftragsverarbeitung im Sinne dieser Bestimmungen liegt nicht vor, wenn die Auftragnehmerin Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen ohne konkreten Bezug zu Leistungen, die die Auftragnehmerin für die Auftraggeberin erbringt, anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Bewachungsdienste und Telekommunikationsleistungen. Die Pflicht der Auftragnehmerin, auch in diesen Fällen ein angemessenes Schutzniveau, insbesondere nach Ziffer 3 dieses Vertrages, zu gewährleisten, bleibt von dem Vorstehenden unberührt.

6.5 Sub-processing within the meaning of these provisions does not exist where the Processor engages third parties for services that are to be regarded as purely ancillary services without any specific connection to services which the Processor renders for the Controller. These include, for example, postal, transport and shipping services, cleaning services, guarding services and telecommunications services. The Processor's obligation to ensure an adequate level of protection, in particular pursuant to Clause 3 of this Agreement, also in such cases remains unaffected by the foregoing.

7. Kontrollrechte

7.1 Die Auftraggeberin ist berechtigt, sich regelmäßig und unregelmäßig von der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen gemäß Ziffer 3.3 dieser Vereinbarung betreffs der Verarbeitung von Auftraggeberdaten durch die Auftragnehmerin, Mitarbeiter und Unterauftragsverarbeiter, zu überzeugen. Art, Umfang und Häufigkeit dieser Überprüfung bestimmt die Auftraggeberin nach billigem Ermessen mit Blick auf die Anforderungen des Art. 32 DS-GVO und nach Maßgabe der Ziffer 7.2. Hierfür kann sie z. B. Auskünfte der Auftragnehmerin einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder Ergebnisse und Erkenntnisse aus sowie jegliche Dokumentationen betreffs internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen der Auftragnehmerin zu den üblichen Geschäftszeiten selbst persönlich bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zur Auftragnehmerin steht.

7.2 Die Auftraggeberin wird bei der Terminierung und Durchführung von Kontrollen angemessene Rücksicht auf die Betriebsabläufe der Auftragnehmerin und der Unterauftragsverarbeiter nehmen. Den Zeitpunkt sowie Art und Umfang einer jeden Prüfung oder Kontrolle nach dieser Ziffer werden die Parteien auf ein entsprechendes Verlangen der Auftraggeberin hin im Einzelfall vereinbaren.

7.3 Die Auftraggeberin dokumentiert das Ergebnis jeder Prüfung nach diesem Ziffer 7 und teilt es der Auftragnehmerin mit. Bei Fehlern, Mängeln, Rechtsverletzungen oder Unregelmäßigkeiten, die die Auftraggeberin feststellt, hat sie die Auftragnehmerin unverzüglich zu informieren. Werden bei der Prüfung Tatsachen festgestellt, welche Änderungen der betrieblichen Abläufe oder Betriebsorganisation der Auftragnehmerin erfordern, stellt die Auftragnehmerin unverzüglich die erforderlichen Anpassungen sicher, um den gesetzlichen oder vereinbarten Anforderungen an den Schutz der Auftraggeberdaten zu genügen.

7. Audit Rights

7.1 The Controller is entitled to satisfy itself, on a regular and ad hoc basis, of compliance with the provisions of this Agreement, in particular the implementation of and compliance with the technical and organisational measures pursuant to Clause 3.3 of this Agreement relating to the processing of Controller Data by the Processor, employees and subprocessors. The Controller shall determine the type, scope and frequency of such review at its reasonable discretion in view of the requirements of Art. 32 GDPR and in accordance with Clause 7.2. For this purpose, it may, for example, obtain information from the Processor, have existing expert opinions, certifications or results and findings of, as well as any documentation concerning, internal audits submitted to it, or have the Processor's technical and organisational measures audited personally or by a knowledgeable third party at normal business hours, provided that such third party is not in competition with the Processor.

7.2 The Controller shall take due account of the operational processes of the Processor and the subprocessors when scheduling and carrying out audits. The date as well as the type and scope of any examination or audit under this Clause shall be agreed between the Parties in each individual case upon a corresponding request by the Controller.

7.3 The Controller shall document the result of each audit under this Clause 7 and communicate it to the Processor. In the event of errors, defects, legal infringements or irregularities identified by the Controller, it shall inform the Processor without delay. If facts are established during the audit which require changes to the Processor's operational processes or organisation, the Processor shall immediately ensure the necessary adjustments in order to comply with the statutory or agreed requirements for the protection of the Controller Data.

8. Umgang mit Betroffenenrechten und weitere Unterstützung

8.1 Die Auftragnehmerin unterstützt die Auftraggeberin angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung ihrer Pflichten nach Art. 12 bis 22 DS-

8. Handling of Data Subjects' Rights and Further Assistance

8.1 Insofar as possible, the Processor shall assist the Controller, taking into account the nature of the processing, by means of appropriate technical and organisational measures in fulfilling its obligations under Art. 12 to 22

GVO und unter Berücksichtigung der ihr zur Verfügung stehenden Informationen bei der Erfüllung ihrer Pflichten nach Art. 32 bis 36 DS-GVO, auch hinsichtlich Verarbeitungen von Auftraggeberdaten im Einfluss- und Verantwortungsbereich der Auftragnehmerin und ihrer Unterauftragsverarbeiter. Sie wird der Auftraggeberin unverzüglich nach entsprechender Aufforderung Auskunft über Auftraggeberdaten geben, sofern die Auftraggeberin nicht selbst über die entsprechenden Informationen verfügt.

GDPR and, taking into account the information available to it, in fulfilling its obligations under Art. 32 to 36 GDPR, also with regard to processing of Controller Data within the sphere of influence and responsibility of the Processor and its subprocessors. Upon corresponding request, it shall without delay provide the Controller with information on Controller Data, insofar as the Controller does not itself have the relevant information.

8.2 Macht eine betroffene Person ihre Rechte gemäß Art. 16 bis 18 DS-GVO geltend, ist die Auftragnehmerin verpflichtet, die Auftraggeberdaten auf Weisung der Auftraggeberin unverzüglich zu berichtigen, zu löschen oder einzuschränken. Die Auftragnehmerin wird der Auftraggeberin die Löschung, Berichtigung bzw. Einschränkung der Daten auf Verlangen in geeigneter Form nachweisen.

8.2 If a data subject asserts their rights pursuant to Art. 16 to 18 GDPR, the Processor shall, upon the Controller's instruction, without delay rectify, erase or restrict the Controller Data. Upon request, the Processor shall demonstrate the erasure, rectification or restriction of the data to the Controller in an appropriate form.

8.3 Macht eine betroffene Person ihre Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich ihrer Daten, unmittelbar gegenüber der Auftragnehmerin geltend, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten und wartet deren Weisungen ab. Ohne entsprechende Einzelweisung wird die Auftragnehmerin nicht mit der betroffenen Person in Kontakt treten.

8.3 If a data subject asserts their rights, for example to information, rectification or erasure of their data, directly vis-à-vis the Processor, the Processor shall forward such request to the Controller without delay and await the Controller's instructions. Without a corresponding specific instruction, the Processor shall not enter into contact with the data subject.

9. Laufzeit und Kündigung

9.1 Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Ist der Hauptvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung entsprechend. Im Zweifel gilt eine Kündigung des Hauptvertrags auch als Kündigung dieses Vertrags und eine Kündigung dieses Vertrages als Kündigung des Hauptvertrages.

9.2 Die Parteien sind jederzeit zu einer außerordentlichen Kündigung dieses Vertrages aus wichtigem Grund berechtigt. Ein wichtiger Grund liegt für die Auftraggeberin insbesondere vor, wenn die Auftragnehmerin Bestimmungen der DS-GVO vorsätzlich oder zumindest grob fahrlässig verletzt oder eine Weisung der Auftraggeberin nicht ausführen kann oder diese Ausführung ernsthaft verweigert. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt die Auftraggeberin der Auftragnehmerin zunächst eine angemessene Frist, innerhalb welcher die Auftragnehmerin den Verstoß abstellen kann. Nach fruchtlosem Ablauf dieser Frist steht der Auftraggeberin sodann das Recht zur außerordentlichen Kündigung zu.

9. Term and Termination

9.1 The term of this Agreement corresponds to the term of the Principal Agreement. If the Principal Agreement may be terminated by ordinary notice, the provisions on ordinary termination shall apply accordingly. In case of doubt, termination of the Principal Agreement shall also constitute termination of this Agreement, and termination of this Agreement shall constitute termination of the Principal Agreement.

9.2 The Parties may terminate this Agreement at any time for cause. For the Controller, cause for termination exists in particular if the Processor intentionally or at least grossly negligently infringes provisions of the GDPR or is unable to execute an instruction of the Controller or seriously refuses such execution. In the case of simple – i.e. neither intentional nor grossly negligent – infringements, the Controller shall first set the Processor a reasonable period within which the Processor may remedy the infringement. Upon fruitless expiry of this period, the Controller shall be entitled to terminate this Agreement for cause.

10. Löschung und Rückgabe von Daten nach Vertragsbeendigung

10.1 Die Auftragnehmerin wird der Auftraggeberin nach Beendigung des Hauptvertrags oder jederzeit auf deren Verlangen alle ihr überlassenen Unterlagen, Daten und Datenträger, welche Auftraggeberdaten enthalten, speichern oder Rückschlüsse auf diese zulassen, zurückgeben oder nach billigem Ermessen der Auftraggeberin vollständig löschen, sofern nicht eine gesetzliche Aufbewahrungsfrist

10. Deletion and Return of Data upon Termination of the Agreement

10.1 Upon termination of the Principal Agreement or at any time upon the Controller's request, the Processor shall return, or completely erase at the Controller's reasonable discretion, all documents, data and data carriers provided to it which contain Controller Data, store it or allow conclusions to be drawn therefrom, insofar as no statutory retention period applies. If Controller Data is initially merely

besteht. Werden Auftraggeberdaten zunächst nur als gelöscht gekennzeichnet („soft delete“), sind sie innerhalb von 30 Tagen endgültig zu löschen („hard delete“). Auf Datensicherungen enthaltene Informationen bleiben von der Verpflichtung zur Löschung ausgenommen und dürfen bis zu ihrer turnusmäßigen Löschung (spätestens nach 30 Tagen) oder ihrer Wiederherstellung im üblichen Geschäftsbetrieb integer aufbewahrt werden. Werden diese wiederhergestellt, so sind die dort enthaltenen Auftraggeberdaten im Wege eines „hard delete“ zu löschen. Dies gilt nicht für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen. Solche Dokumentationen sind von der Auftragnehmerin in einer Form, welche dem Grundsatz der Datenminimierung entspricht, bis zum Ablauf des vierten Kalenderjahres nach der jeweiligen Datenverarbeitung aufzubewahren und auf Verlangen an die Auftraggeberin herauszugeben. Erst im Anschluss sind auch diese entsprechend den Regelungen dieser Ziffer zu löschen.

marked as deleted ("soft delete"), it shall be permanently erased ("hard delete") within 30 days. Information contained in data backups is exempt from the obligation to erase and may be kept intact until its scheduled deletion (at the latest after 30 days) or its restoration in the ordinary course of business. If such backups are restored, the Controller Data contained therein shall be erased by way of a "hard delete". This shall not apply to documentation serving as evidence of the contracted and proper processing of the Controller Data. Such documentation shall be retained by the Processor, in a form consistent with the principle of data minimisation, until the expiry of the fourth calendar year following the respective data processing and shall be handed over to the Controller upon request. Only thereafter shall such documentation also be erased in accordance with the provisions of this Clause.

10.2 Die Auftragnehmerin wird der Auftraggeberin die Erfüllung der vorstehend beschriebenen Pflichten schriftlich bestätigen. Die Auftraggeberin hat das Recht, die vollständige und vertragsgerechte Erfüllung dieser Pflichten in geeigneter Weise zu kontrollieren; Ziffern 7.1 und 7.2 dieses Vertrags gelten hierfür entsprechend. Dieses Recht steht ihr während des ersten Kalenderjahres nach der Vertragsbeendigung ohne weitere Voraussetzungen zu, anschließend nur unter der Voraussetzung, dass greifbare Anhaltspunkte dafür bestehen, dass keine vertragsgemäße Löschung erfolgte.

10.2 The Processor shall confirm to the Controller in writing the fulfilment of the obligations described above. The Controller has the right to verify the complete and contract-compliant fulfilment of these obligations in an appropriate manner; Clauses 7.1 and 7.2 of this Agreement shall apply accordingly. This right shall be available to it during the first calendar year following termination of the Agreement without further preconditions; thereafter only on the condition that there are tangible indications that no contract-compliant erasure has taken place.

11. Schlussbestimmungen

11.1 Die Parteien sind einig, dass die Einrede eines Zurückbehaltungsrechts durch die Auftragnehmerin hinsichtlich Ansprüchen, die sie aus diesem Vertrag treffen, ausgeschlossen ist, wenn dieses Zurückbehaltungsrecht nicht aufgrund von rechtskräftig festgestellten oder unbestrittenen Gegenansprüchen der Auftragnehmerin ausgeübt wird.

11.2 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

11.3 Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung oder höchstrichterlichen Rechtsprechung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

11.4 Diese Vereinbarung unterliegt deutschem Recht.

11.5 Ausschließlicher Gerichtsstand für alle Streitigkeiten, die sich aus oder in Zusammenhang mit diesem Vertrag ergeben ist Köln, Nordrhein-Westfalen.

11. Final Provisions

11.1 The Parties agree that the Processor’s plea of right of retention with regard to claims to which it is subject under this Agreement is excluded unless such right of retention is exercised on the basis of counterclaims of the Processor that have been finally judicially determined or are undisputed.

11.2 Amendments and supplements to this Agreement must be made in writing. This also applies to any waiver of this requirement as to form.

11.3 In case of doubt, the provisions of this Agreement shall take precedence over the provisions of the Principal Agreement. Should individual provisions of this Agreement prove entirely or partially invalid or unenforceable, or become invalid or unenforceable as a result of changes in legislation or supreme court case law after conclusion of the Agreement, the validity of the remaining provisions shall remain unaffected. The invalid or unenforceable provision shall be replaced by the valid and enforceable provision that comes as close as possible to the meaning and purpose of the void provision.

11.4 This Agreement is governed by German law.

11.5 The exclusive place of jurisdiction for all disputes arising out of or in connection with this Agreement is Cologne, North Rhine-Westphalia.

11.6 Dieser Vertrag wurde in deutscher und englischer Sprache geschlossen. Bei Abweichungen zwischen den Sprachfassungen gilt die deutsche Fassung.

11.6 This Agreement has been concluded in German and in English. In the event of any discrepancies between the language versions, the German version shall prevail.

ANNEX 1 — Betroffene Datenarten und Personenkategorien
ANNEX 1 — Categories of Data and Data Subjects

Leistungen, bei denen Auftraggeberdaten verarbeitet werden ***Services involving the processing of Controller Data***	**Kategorien verarbeiteter Daten** ***Categories of data processed***	**Kategorien betroffener Personen** ***Categories of data subjects***
Bereitstellung von KI-Modellen zur Inferenz (Text, Code, Bild, Audio, Embeddings, Reranking, Content Safety/Guardrails) über API und Weboberfläche *Provision of AI models for inference (text, code, image, audio, embeddings, reranking, content safety/guardrails) via API and web interface*	Eingaben wie insbesondere Prompts und Systemanweisungen, Dateien, Bilder, Audioaufnahmen sowie die daraus erzeugten Ausgaben wie insbesondere Textinhalte, Code, Bilder, Transkripte und Embeddings. *Inputs, in particular prompts and system instructions, files, images, audio recordings, as well as outputs generated therefrom, in particular text content, code, images, transcripts and embeddings.*	Alle Personen, deren Daten der Auftraggeber übermittelt, insbesondere Beschäftigte, Kunden, Interessenten und Ansprechpartner des Auftraggebers; bei Audioverarbeitung zusätzlich Personen, deren Stimme in den Aufnahmen enthalten ist; bei Bildverarbeitung zusätzlich Personen, welche auf den Bildinhalten zu sehen sind; *All persons whose data the Controller transmits, in particular employees, customers, prospects and contacts of the Controller; in the case of audio processing, additionally persons whose voice is contained in the recordings; in the case of image processing, additionally persons visible in the image content;*
Nutzer- und Zugangsverwaltung *User and access management*	Personenstammdaten, Kommunikationsdaten (z.B. E-Mail-Adresse), Zugangs- und Berechtigungsdaten (einschließlich API-Schlüsseln) *Master personal data, communication data (e.g. e-mail address), access and authorisation data (including API keys)*	Beschäftigte und sonstige Nutzer des Auftraggebers *Employees and other users of the Controller*
Betrieb, Sicherheit und Protokollierung *Operations, security and logging*	Nutzungs- und Protokolldaten (z. B. IP-Adresse, Zeitstempel, genutztes Modell, Tokenmengen, Routing- und Failover-Entscheidungen, Fehlercodes). Protokolliert werden ausschließlich Betriebsmetadaten; Nachrichteninhalte (Eingaben und Ausgaben) werden nicht protokolliert. *Usage and log data (e.g. IP address, time stamps, model used, token volumes, routing and failover decisions, error codes). Only operational metadata is logged; message contents (inputs and outputs) are not logged.*	Beschäftigte und sonstige Nutzer des Auftraggebers *Employees and other users of the Controller*
Support *Support*	Kommunikationsdaten, Zeitstempel, Inhalte von Supportanfragen *Communication data, time stamps, contents of support requests*	Ansprechpartner und Nutzer des Auftraggebers *Contacts and users of the Controller*
Tools zur Nutzung mit KI-Modellen *Tools for use with AI models*	Eingaben wie insbesondere Suchanfragen, angefragte URLs und Webinhalte, übermittelte Dokumente *Inputs, in particular search queries, requested URLs and web content, transmitted documents*	Alle Personen, deren Daten der Auftraggeber übermittelt, insbesondere Beschäftigte, Kunden, Interessenten und Ansprechpartner des Auftraggebers; *All persons whose data the Controller transmits, in particular employees, customers, prospects and contacts of the Controller;*
Vektorspeicher *Vector store*	Vom Auftraggeber hochgeladene Dokumente und Dateien, daraus erzeugte Chunks und Embeddings sowie zugehörige Metadaten; Speicherung bis zur Löschung durch den Auftraggeber. *Documents and files uploaded by the Controller, chunks and embeddings generated therefrom as well as associated metadata; storage until deletion by the Controller.*	Alle Personen, deren Daten der Auftraggeber übermittelt, insbesondere Beschäftigte, Kunden, Interessenten und Ansprechpartner des Auftraggebers; *All persons whose data the Controller transmits, in particular employees, customers, prospects and contacts of the Controller;*

ANNEX 2 — Weisungsberechtigte / Weisungsempfänger
ANNEX 2 — Persons Authorised to Give / Receive Instructions

Weisungsberechtigte Personen der Auftraggeberin ist die Person, die den Auftragsverarbeitungsvertrag im Auftrag und mit Genehmigung der Auftraggeberin akzeptiert.
The Controller's authorized representative is the person who accepts the data processing agreement on behalf of and with the approval of the Controller.

Weisungsempfänger bei der Auftragnehmerin sind:
Instruction recipients at the Processor are:

Sebastian Nell, CTO, privacy@melious.de

ANNEX 3 — Technische und organisatorische Maßnahmen
ANNEX 3 — Technical and Organisational Measures

Technische und organisatorische Maßnahmen gem. Art. 32 DS-GVO
Technical and organisational measures pursuant to Art. 32 GDPR

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)
   – Zutrittskontrolle
   Kein unbefugter Zutritt zu Datenverarbeitungsanlagen. Die Systeme werden ausschließlich in Rechenzentren der in Anlage 4 genannten Unterauftragsverarbeiter betrieben; die physische Zutrittskontrolle liegt beim jeweiligen Rechenzentrumsbetreiber, z. B.: Auswahl nach Zertifizierungen der Rechenzentren (u. a. ISO 27001), keine eigenen Rechenzentren, keine Server oder Datenträger mit Auftraggeberdaten in den Geschäftsräumen, Schließsystem und Begleitung von Besuchern in den Geschäftsräumen.
   – Zugangskontrolle
   Keine unbefugte Systembenutzung durch Nutzerauthentifizierung, z. B.: administrativer Serverzugang ausschließlich per SSH-Schlüssel bzw. kurzlebigen SSH-Zertifikaten mit Single Sign-on (Passwort- und Root-Anmeldung deaktiviert), Zwei-Faktor-Authentifizierung für Mitarbeitende und Administratoren, automatische Sperrmechanismen bei wiederholten Fehlanmeldungen, Betriebsoberflächen nur über VPN erreichbar, Firewalls nach dem Default-Deny-Prinzip, Festplattenverschlüsselung der Endgeräte, sichere Verwaltung von Secrets und API-Schlüsseln (nur als Hash gespeichert, jederzeit widerrufbar).
   – Zugriffskontrolle
   Zugriffskontrolle auf Daten; kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems; Protokollierung administrativer Zugriffe und Änderungen, z. B.: Berechtigungskonzept mit Rollenmodell, Zugriffsrechte nach dem Need-to-know-Prinzip mit dokumentierter Freigabe, Zugriffsprüfungen auf jeder Schnittstelle, API-Schlüssel mit eingeschränkten Berechtigungen (Scopes), anlassbezogene Überprüfung der Berechtigungen.
   – Trennungskontrolle
   Trennung von Fremd- und Eigendaten sowie Trennung der Datensätze verschiedener Kunden, z. B.: Mandantenfähigkeit, Trennung von Entwicklungs-, Staging- und Produktivsystemen mit eigenen Secrets, automatisierte Tests nur gegen isolierte Testdatenbanken, dedizierte Server für Kunden mit dedizierter Kapazität.
   – Personal
   Vertrauliche Behandlung von Daten in der Arbeitsorganisation; Verpflichtung aller Mitarbeitenden auf Vertraulichkeit (Ziffer 3.2), z. B.: schriftliche Verpflichtungserklärungen, anlassbezogene Datenschutz- und Sicherheitsschulungen, verbindliche interne Entwicklungsrichtlinien.

1. *Confidentiality (Art. 32(1)(b) GDPR)*
   – Physical access control
   No unauthorised physical access to data processing facilities. The systems are operated exclusively in data centres of the subprocessors listed in Annex 4; physical access control is the responsibility of the respective data centre operator, e.g.: selection based on data centre certifications (including ISO 27001), no data centres of its own, no servers or data carriers containing Controller Data on the business premises, locking system and escorting of visitors on the business premises.
   – System access control
   No unauthorised use of systems, ensured by user authentication, e.g.: administrative server access exclusively via SSH keys or short-lived SSH certificates with single sign-on (password and root login disabled), two-factor authentication for employees and administrators, automatic lockout mechanisms after repeated failed login attempts, operational interfaces accessible only via VPN, firewalls based on the default-deny principle, full disk encryption of end devices, secure management of secrets and API keys (stored only as hashes, revocable at any time).
   – Data access control
   Access control relating to data; no unauthorised reading, copying, modification or removal within the system; logging of administrative access and changes, e.g.: authorisation concept with role model, access rights based on the need-to-know principle with documented approval, access checks on every interface, API keys with restricted permissions (scopes), event-driven review of permissions.
   – Separation control
   Separation of third-party and own data and separation of different customers' data records, e.g.: multi-tenancy, separation of development, staging and production systems with separate secrets, automated tests only against isolated test databases, dedicated servers for customers with dedicated capacity.
   – Personnel
   Confidential handling of data in the working organisation; obligation of all employees to maintain confidentiality (Clause 3.2), e.g.: written confidentiality undertakings, event-driven data protection and security training, binding internal development guidelines.

2. Verschlüsselung und Pseudonymisierung (Art. 32 Abs. 1 lit. a, Art. 25 Abs. 1 DS-GVO)
– Verschlüsselung
Verschlüsselungskonzept für Daten bei der Übertragung (data in transit) und bei der Speicherung (data at rest), z. B.: TLS 1.2/1.3 für API und Weboberfläche, verschlüsseltes internes Netz, anwendungsseitige Verschlüsselung personenbezogener Felder, Verschlüsselung gespeicherter Daten, Datensicherungen und Batch-Dateien, Schlüsselverwaltung mit regelmäßiger Rotation.
– Pseudonymisierung
Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen, z. B.: Speicherung von IP-Adressen in der Datenbank nur als Hash, automatische Entfernung personenbezogener Felder aus Anwendungs- und Router-Protokollen, keine Weitergabe von Nutzerkennungen an Inferenz-Anbieter, Pseudonym statt Name und E-Mail-Adresse gegenüber dem Zahlungsdienstleister.

2. *Encryption and pseudonymisation (Art. 32(1)(a), Art. 25(1) GDPR)*
– Encryption
Encryption concept for data in transit and data at rest, e.g.: TLS 1.2/1.3 for API and web interface, encrypted internal network, application-level encryption of personal data fields, encryption of stored data, backups and batch files, key management with regular rotation.
– Pseudonymisation
Processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organisational measures, e.g.: IP addresses stored in the database only as hashes, automatic removal of personal data fields from application and router logs, no disclosure of user identifiers to inference providers, pseudonym instead of name and email address vis-à-vis the payment service provider.

3. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)
– Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z. B.: Transportverschlüsselung aller externen und internen Verbindungen, Virtual Private Networks (VPN), verschlüsselte Verbindungen zu Unterauftragsverarbeitern, Entfernung von Authentifizierungs-Headern bei Weiterleitung an Inferenz-Anbieter, Dokumentation der Datenflüsse.
– Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Nachrichteninhalte (Eingaben und Ausgaben) werden nicht protokolliert, z. B.: unveränderbares Audit-Log administrativer Aktionen, durchgängige Request-ID, Versionierung von Änderungen an Infrastruktur, Konfiguration und Code.
– Datenintegrität und Systemschutz
Konzepte zur sicheren Softwareentwicklung; Konzept zur Detektion und Behebung von Schwachstellen, Patch-Management, z. B.: Code-Review, automatisierte Sicherheitsprüfungen in der CI-Pipeline, Prüfung von Abhängigkeiten, automatische Sicherheitsupdates auf allen Servern, regelmäßiger Abgleich installierter Pakete mit Schwachstellendatenbanken, Systemhärtung.

3. *Integrity (Art. 32(1)(b) GDPR)*
– Transfer control
No unauthorised reading, copying, modification or removal during electronic transmission or transport, e.g.: transport encryption of all external and internal connections, virtual private networks (VPN), encrypted connections to subprocessors, removal of authentication headers when forwarding to inference providers, documentation of data flows.
– Input control
Determination of whether and by whom personal data have been entered into, modified in or removed from data processing systems. Message content (inputs and outputs) is not logged, e.g.: immutable audit log of administrative actions, end-to-end request ID, versioning of changes to infrastructure, configuration and code.
– Data integrity and system protection
Concepts for secure software development; concept for the detection and remediation of vulnerabilities, patch management, e.g.: code review, automated security checks in the CI pipeline, dependency checks, automatic security updates on all servers, regular comparison of installed packages against vulnerability databases, system hardening.

4. Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b und c DS-GVO)
– Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust; regelmäßige Datensicherung, z. B.: tägliche verschlüsselte Datensicherung an einen separaten Standort (off-site), Firewall, Monitoring und Alarmierung, Meldewege und Notfallpläne (Runbooks), Stromversorgung und physische Infrastruktur durch die zertifizierten

Rechenzentrumsbetreiber.
– Belastbarkeit
Konzept zur Fortführung der Leistungserbringung bei Sicherheitsvorfällen und Störungen der Infrastruktur; Ausfallsicherheit durch Multi-Provider-Routing, z. B.: redundante Infrastruktur mit automatischem Failover, Rate-Limits zur Lastbegrenzung.
– Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
Konzepte zur Wiederherstellung von Daten im Falle des Datenverlusts, z. B.: dokumentierte Wiederherstellungsverfahren, regelmäßige automatisierte und manuelle Wiederherstellungstests.

4. *Availability, resilience and recoverability (Art. 32(1)(b) and (c) GDPR)*
– Availability control
Protection against accidental or wilful destruction or loss; regular data backups, e.g.: daily encrypted backup to a separate location (off-site), firewall, monitoring and alerting, reporting channels and emergency plans (runbooks), power supply and physical infrastructure provided by the certified data centre operators.
– Resilience
Concept for the continuation of service provision in the event of security incidents and disruptions to the infrastructure; fault tolerance through multi-provider routing, e.g.: redundant infrastructure with automatic failover, rate limits for load limitation.
– Rapid recoverability (Art. 32(1)(c) GDPR)
Concepts for the restoration of data in the event of data loss, e.g.: documented recovery procedures, regular automated and manual recovery tests.

5. Datenminimierung und Löschung (Art. 5 Abs. 1 lit. c und e, Art. 25 DS-GVO)
Konzept zur Löschung und Migration von Datenbeständen; Löschung nach Vertragsende gemäß Ziffer 10, z. B.: festgelegte Löschfristen, automatische Löschläufe, begrenzte Aufbewahrungsdauer von Protokolldaten.

5. *Data minimisation and erasure (Art. 5(1)(c) and (e), Art. 25 GDPR)*
Concept for the deletion and migration of data stocks; deletion after termination of the Agreement in accordance with Clause 10, e.g.: defined deletion periods, automated deletion runs, limited retention period for log data.

6. Auftragskontrolle (Art. 28 DS-GVO)
Keine Auftragsverarbeitung ohne entsprechende Weisung der Auftraggeberin, z. B.: eindeutige Vertragsgestaltung, Auftragsverarbeitungsverträge mit allen Unterauftragsverarbeitern (Anlage 4), Auswahl der Unterauftragsverarbeiter u. a. nach Sicherheitszertifizierungen und Verarbeitungsort EU/EWR, Prüfung vor Beauftragung, anlassbezogene Nachprüfung sowie im Rahmen der jährlichen Überprüfung der Maßnahmen.

6. *Order control (Art. 28 GDPR)*
No processing on behalf of the Controller without corresponding instructions from the Controller, e.g.: clear contractual arrangements, data processing agreements with all subprocessors (Annex 4), selection of subprocessors based on, among other things, security certifications and processing location in the EU/EEA, review prior to engagement, event-driven follow-up review and review as part of the annual review of the measures.

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 DS-GVO)
– Incident-Response-Management
Konzept zur Detektion und Reaktion auf Sicherheitsvorfälle; Meldung an die Auftraggeberin gemäß Ziffer 4.1, z. B.: festgelegte Meldewege, Dokumentation von Vorfällen.
– Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
Z. B.: datensparsame Standardkonfiguration, keine Speicherung von Eingaben über die Verarbeitung hinaus, soweit nicht von der Auftraggeberin aktiviert.
– Datenschutz- und Informationssicherheitsmanagement
Benennung eines externen Datenschutzbeauftragten (Ziffer 5.3); Dokumentation der Sicherheitsmaßnahmen, regelmäßige Überprüfung durch die Geschäftsführung und Grundsatz der kontinuierlichen Verbesserung von Sicherheitsmaßnahmen, z. B.: jährliche Überprüfung der Maßnahmen sowie bei wesentlichen Änderungen, automatisierte Sicherheitsprüfungen und interne Sicherheitsreviews.

7. *Procedures for regular testing, assessment and evaluation (Art. 32(1)(d), Art. 25(1) GDPR)*
– Incident response management
Concept for the detection of and response to security incidents; notification of the Controller in accordance with Clause 4.1, e.g.: defined reporting channels, documentation of incidents.
– Data protection by default (Art. 25(2) GDPR)
E.g.: data-minimising default configuration, no storage of inputs beyond processing unless activated by the Controller.
– Data protection and information security management

Appointment of an external data protection officer (Clause 5.3); documentation of security measures, regular review by the management and the principle of continuous improvement of security measures, e.g.: annual review of the measures and in the event of material changes, automated security checks and internal security reviews.

ANNEX 4 — Unterauftragsverarbeiter bei Vertragsschluss
ANNEX 4 — Subprocessors at the Time of Conclusion of the Agreement

Name und Anschrift ***Name and address***	**Beschreibung der Leistung** ***Description of services***	**Land der Leistungserbringung** ***Country of service provision***
Berget AI AB Götgatan 18, 118 46 Stockholm, Schweden *Götgatan 18, 118 46 Stockholm, Sweden*	KI-Inferenz: Entgegennahme und Verarbeitung von API-Anfragen, Ausführung von KI-Modellen (Open-Weight-Modelle) und Rückgabe von Modellantworten; Ausfallsicherheit durch Multi-Provider-Routing *AI inference: receipt and processing of API requests, execution of AI models (open-weight models) and return of model responses; resilience through multi-provider routing*	Schweden *Sweden*
Infercom SCS 29 Boulevard Grande-Duchesse Charlotte, 1331 Luxembourg, Luxemburg *29 Boulevard Grande-Duchesse Charlotte, 1331 Luxembourg, Luxembourg*	KI-Inferenz: Entgegennahme und Verarbeitung von API-Anfragen, Ausführung von KI-Modellen (Open-Weight-Modelle) und Rückgabe von Modellantworten; Ausfallsicherheit durch Multi-Provider-Routing *AI inference: receipt and processing of API requests, execution of AI models (open-weight models) and return of model responses; resilience through multi-provider routing*	Luxemburg *Luxembourg*
Inceptron AB Scheelevägen 15, 223 70 Lund, Schweden *Scheelevägen 15, 223 70 Lund, Sweden*	KI-Inferenz: Entgegennahme und Verarbeitung von API-Anfragen, Ausführung von KI-Modellen (Open-Weight-Modelle) und Rückgabe von Modellantworten; Ausfallsicherheit durch Multi-Provider-Routing *AI inference: receipt and processing of API requests, execution of AI models (open-weight models) and return of model responses; resilience through multi-provider routing*	Schweden *Sweden*
SEEWEB s.r.l. (Regolo.ai) C.so Lazio 9/a, 03100 Frosinone, Italien *C.so Lazio 9/a, 03100 Frosinone, Italy*	KI-Inferenz: Entgegennahme und Verarbeitung von API-Anfragen, Ausführung von KI-Modellen (Open-Weight-Modelle) und Rückgabe von Modellantworten; Ausfallsicherheit durch Multi-Provider-Routing *AI inference: receipt and processing of API requests, execution of AI models (open-weight models) and return of model responses; resilience through multi-provider routing*	Italien *Italy*
Scaleway SAS 8 Rue de la Ville l'Évêque, 75008 Paris, Frankreich *8 Rue de la Ville l'Évêque, 75008 Paris, France*	KI-Inferenz: Entgegennahme und Verarbeitung von API-Anfragen, Ausführung von KI-Modellen (Open-Weight-Modelle) und Rückgabe von Modellantworten; Ausfallsicherheit durch Multi-Provider-Routing *AI inference: receipt and processing of API requests, execution of AI models (open-weight models) and return of model responses; resilience through multi-provider routing*	Frankreich *France*
TensorX Ltd. Unit 25 Classon House, Dundrum Business Park, Dublin 14, D14 N2F6, Irland *Unit 25 Classon House, Dundrum Business Park, Dublin 14, D14 N2F6, Ireland*	KI-Inferenz: Entgegennahme und Verarbeitung von API-Anfragen, Ausführung von KI-Modellen (Open-Weight-Modelle) und Rückgabe von Modellantworten; Ausfallsicherheit durch Multi-Provider-Routing *AI inference: receipt and processing of API requests, execution of AI models (open-weight models) and return of model responses; resilience through multi-provider routing*	Irland *Ireland*
DataCrunch Oy (Verda) * Lapinlahdenkatu 16, 00180 Helsinki, Finnland *Lapinlahdenkatu 16, 00180 Helsinki, Finland*	KI-Inferenz: Entgegennahme und Verarbeitung von API-Anfragen, Ausführung von KI-Modellen (Open-Weight-Modelle) und Rückgabe von Modellantworten; Ausfallsicherheit durch Multi-Provider-Routing *AI inference: receipt and processing of API requests, execution of AI models (open-weight models) and return of model responses; resilience through multi-provider routing*	Finnland *Finland*

AKI.IO GmbH Marienburger Straße 1, 10405 Berlin, Deutschland *Marienburger Straße 1, 10405 Berlin, Germany*	KI-Inferenz: Entgegennahme und Verarbeitung von API-Anfragen, Ausführung von KI-Modellen (Open-Weight-Modelle) und Rückgabe von Modellantworten; Ausfallsicherheit durch Multi-Provider-Routing *AI inference: receipt and processing of API requests, execution of AI models (open-weight models) and return of model responses; resilience through multi-provider routing*	Deutschland *Germany*
IONOS SE Elgendorfer Str. 57, 56410 Montabaur, Deutschland *Elgendorfer Str. 57, 56410 Montabaur, Germany*	Cloud-Hosting und KI-Inferenz: Bereitstellung von Cloud-Infrastruktur, Hosting von Plattformkomponenten, Verarbeitung von API-Anfragen; S3-Objektspeicher zur Speicherung clientseitig verschlüsselter Dateien (Region eu-central-1, Frankfurt) *Cloud hosting and AI inference: provision of cloud infrastructure, hosting of platform components, processing of API requests; S3 object storage for storing client-side encrypted files (region eu-central-1, Frankfurt)*	Deutschland *Germany*
OVH SAS (OVHcloud) * 2 Rue Kellermann, 59100 Roubaix, Frankreich *2 Rue Kellermann, 59100 Roubaix, France*	Cloud-Hosting, Objektspeicher und KI-Inferenz: Bereitstellung von Cloud-Infrastruktur, Hosting von Plattformkomponenten, Speicherung von Dateien und Backups (S3-kompatibler Objektspeicher), Verarbeitung von API-Anfragen *Cloud hosting, object storage and AI inference: provision of cloud infrastructure, hosting of platform components, storage of files and backups (S3-compatible object storage), processing of API requests*	Frankreich *France*
G-Core Labs S.A. (Gcore) 2-4, rue Edmond Reuter, L-5326 Contern, Luxemburg *2-4, rue Edmond Reuter, L-5326 Contern, Luxembourg*	DNS-Dienst: Auflösung von Domainnamen, Weiterleitung von DNS-Anfragen, Protokollierung von Zugriffen; Reduzierung von Ladezeiten, DDoS-Schutz *DNS service: resolution of domain names, forwarding of DNS requests, logging of accesses; reduction of loading times, DDoS protection*	Luxemburg *Luxembourg*
European Perspective SAS (Staan) 42 Avenue de la Porte de Clichy, 75017 Paris, Frankreich *42 Avenue de la Porte de Clichy, 75017 Paris, France*	Web-Suche: Durchführung von Internetsuchen auf Basis KI-generierter Suchanfragen, Rückgabe von Suchergebnissen; datenschutzfreundliche Suche ohne Speicherung personenbezogener Suchhistorie, Datenverarbeitung in der EU *Web search: performance of internet searches based on AI-generated search queries, return of search results; privacy-friendly search without storage of personal search history, data processing in the EU*	Frankreich *France*
Mollie B.V. Keizersgracht 126, 1015 CW Amsterdam, Niederlande *Keizersgracht 126, 1015 CW Amsterdam, Netherlands*	Zahlungsabwicklung: Verarbeitung pseudonymisierter Zahlungsreferenzen, Abonnement- und Mandatsverwaltung (SEPA-Lastschrift, Kreditkarte), Erstattungsabwicklung *Payment processing: processing of pseudonymised payment references, subscription and mandate management (SEPA direct debit, credit card), refund processing*	Niederlande *Netherlands*
UAB „Data troops“ (Decodo, ehemals Smartproxy) Švitrigailos str. 34, Vilnius, Litauen *Švitrigailos str. 34, Vilnius, Lithuania*	Proxy-Dienst: Weiterleitung ausgehender Plattform-Anfragen über Proxy-Infrastruktur, Verarbeitung technischer Verbindungsdaten *Proxy service: forwarding of outgoing platform requests via proxy infrastructure, processing of technical connection data*	Litauen *Lithuania*
sevDesk GmbH Im Unteren Angel 1, 77652 Offenburg, Deutschland *Im Unteren Angel 1, 77652 Offenburg, Germany*	Cloud-Buchhaltungssoftware: Verarbeitung und Speicherung von Rechnungs-, Buchhaltungs- und Finanzdaten; Erstellung und Verwaltung von Rechnungen, Belegerfassung und -archivierung, Umsatzsteuervoranmeldung *Cloud accounting software: processing and storage of invoice, accounting and financial data; creation and management of invoices, receipt capture and archiving, advance VAT return*	Deutschland *Germany*
Impossible Cloud GmbH Friesenweg 12, 22763 Hamburg, Deutschland	Objektspeicher (S3 Storage) *Object Storage (S3 Storage)*	Deutschland *Germany*

Friesenweg 12, 22763 Hamburg, Germany		

Kennzeichnung gemäß Ziffer 3.6: Bei den mit „ " gekennzeichneten Anbietern betreibt die Auftragnehmerin eigene dedizierte Server-Hardware („Melious-Server"). Ziffer 3.6 (Zero Data Retention) gilt ausschließlich für die Verarbeitung von Auftraggeberdaten auf dieser dedizierten Hardware. Diese Anbieter betreiben daneben eigene Server-Infrastruktur; für Verarbeitungen auf dieser Anbieter-Infrastruktur gilt Ziffer 3.6 nicht**,** es gelten insoweit die Regelungen für Unterauftragsverarbeiter.

Marking pursuant to Clause 3.6: For the providers marked with "", the Processor operates its own dedicated server hardware ("Melious servers"). Clause 3.6 (Zero Data Retention) applies exclusively to the processing of Controller Data on this dedicated hardware. These providers also operate their own server infrastructure; Clause 3.6 does not apply to processing on this provider infrastructure; in this respect, the provisions for subprocessors shall apply.*