Allgemeine Geschäftsbedingungen (AGB) für die Nutzung von Brainy

Stand: 13. April 2026

1. Geltungsbereich und Vertragspartner

1.1 Diese Allgemeinen Geschäftsbedingungen (AGB) gelten für die Nutzung der bereitgestellten Software "Brainy" (nachfolgend "Anwendung" genannt), sowohl in der Web-Version als auch gegebenenfalls als mobile App, die von der

Latoo.labs GmbH
FN 565855s
Kraußstraße 16
4020 Linz
Österreich
E-Mail: office@latoo.at
Website: www.abrainy.com

(nachfolgend "Anbieter" genannt) bereitgestellt wird.

1.2 Mit der Nutzung der Anwendung und durch Anklicken des Buttons "Ich stimme zu" am Ende dieser AGB im Rahmen des Registrierungsprozesses akzeptiert der jeweils verantwortliche zeichnungsberechtigte Vertreter der Organisation diese AGB, den zugehörigen Auftragsverarbeitungsvertrag (AVV) und die AI Act Compliance Notice vollinhaltlich auf elektronischem Wege. Es wird empfohlen, eine von beiden Parteien gezeichnete Version der AVV abzuschließen.

Abweichende, entgegenstehende oder ergänzende Allgemeine Geschäftsbedingungen des Nutzers werden nicht Vertragsbestandteil, es sei denn, der Anbieter stimmt ihrer Geltung ausdrücklich schriftlich zu.

1.3 Der Anbieter stellt die Anwendung ausschließlich Unternehmen bzw. Unternehmern im Sinne des § 1 UGB, nicht aber Verbrauchern zur Verfügung.

2. Definitionen

2.1 "Coins" sind die einheitliche Verbrauchseinheit für die Nutzung der Brainy-Anwendung. Ein Coin entspricht in etwa einem Euro an KI-Nutzungskosten und bietet damit eine einfache, transparente Darstellung des Verbrauchs. Der tatsächliche Coin-Verbrauch je Aktion richtet sich nach dem gewählten KI-Modell, den genutzten Funktionen sowie dem Umfang der Verarbeitung (z.B. Länge der Eingabe und Ausgabe, Anzahl der Verarbeitungsschritte). Coins können auch für einmalige oder wiederkehrende Aktionen verbraucht werden (z.B. Ausführen von Programmen, Speicherplatz pro Monat, Aktivierte Verbindungen pro Monat usw.). Kunden erhalten pro Abrechnungszeitraum ein im gewählten Paket festgelegtes Kontingent an Coins. Weitere Coins können erworben werden.

Credits, sind die Verbrauchseinheiten ohne Bezug auf tatsächliche Kosten, die bis zur Einführung von Coins abgerechnet werden.

2.2 "Speicher" bezeichnet jenen Speicherbedarf in Megabyte oder Gigabyte, den die gesamten hochgeladenen Dokumente eines Kunden in der Datenbank der Software benötigen. Jeder Kunde verfügt über ein gewisses Ausmaß an Speicher. Das zur Verfügung stehende Ausmaß an Speicher ist Bestandteil des jeweiligen Vertrags.

2.3 "Historie" bezeichnet die Aufbewahrungsfrist in Monaten, wo zurückliegende Daten/Chats/Dokumente verfügbar sind. Nach der Aufbewahrungsfrist werden Daten automatisch gelöscht.

2.4 "Max. User" ist die maximale Anzahl der Benutzerkonten für das Brainy System pro Lizenznehmer.

2.5 "Anzahl Workspace" ist die maximale Anzahl von Datenpools für das Brainy System.

2.6 "KI-Agent" oder "Agentic AI" bezeichnet eine Funktion der Anwendung, bei der ein KI-System eigenständig und mit einem gewissen Grad an Autonomie Aktionen ausführt, um ein vom Nutzer definiertes Ziel zu erreichen. Im Gegensatz zu einer einfachen Anfrage-Antwort-Interaktion kann ein KI-Agent mehrere Schritte sequenziell oder parallel ausführen, Werkzeuge (Tools) nutzen, auf Drittdienste zugreifen und Entscheidungen im Rahmen seiner Konfiguration eigenständig treffen. Die Ergebnisse der Aktionen eines KI-Agenten können außerhalb der Anwendung selbst Wirkung entfalten (z.B. Versenden von E-Mails, Bearbeiten von Dateien, Auslösen von API-Aufrufen).

2.7 "Konnektor" bezeichnet eine technische Schnittstelle (Integration), die es der Anwendung ermöglicht, sich mit einem Drittdienst zu verbinden und in dessen Namen oder Auftrag Aktionen auszuführen oder Daten abzurufen. Konnektoren werden über die Infrastruktur des Drittanbieters Nango Inc. bereitgestellt und verwaltet. Für jeden Konnektor erteilt der Nutzer der Anwendung eine Zugriffsberechtigung (typischerweise via OAuth 2.0) auf den jeweiligen Drittdienst.

2.8 "Autonome Aktion" bezeichnet jede Handlung, die ein KI-Agent im Rahmen seiner Ausführung eigenständig und ohne gesonderte manuelle Bestätigung durch den Nutzer für jeden einzelnen Schritt ausführt. Dies umfasst insbesondere das Lesen und Schreiben von Daten in Drittdiensten, das Versenden von Nachrichten oder E-Mails sowie das Auslösen von Prozessen in verbundenen Systemen.

2.9 "Drittdienst" bezeichnet jede externe Software, Plattform oder Anwendung, die nicht vom Anbieter betrieben wird und über einen Konnektor mit der Brainy-Anwendung verbunden ist. Dies umfasst beispielsweise E-Mail-Dienste (z.B. Microsoft Outlook, Google Gmail), Dateispeicher-Dienste (z.B. Microsoft OneDrive, Google Drive, Dropbox), Kommunikationsplattformen (z.B. Microsoft Teams, Slack) sowie CRM-, ERP- und sonstige Unternehmenssoftware.

2.10 "Prompt Injection" bezeichnet einen Angriff oder ein unbeabsichtigtes Szenario, bei dem schadhafte oder manipulative Inhalte aus externen Quellen (z.B. aus dem Inhalt einer E-Mail, eines Dokuments oder einer Webseite, auf die ein KI-Agent zugreift) dazu führen, dass der KI-Agent unbeabsichtigte oder schädliche Aktionen ausführt oder vertrauliche Informationen preisgibt.

2.11 „MCP-Server" (Model Context Protocol Server) bezeichnet einen Dienst, der das standardisierte Model Context Protocol (MCP) implementiert und es KI-Agenten ermöglicht, über eine definierte Schnittstelle auf externe Werkzeuge, Datenquellen und Systeme zuzugreifen sowie dort Aktionen auszuführen. MCP-Server fungieren als Vermittler zwischen dem KI-Agenten und den angebundenen Drittsystemen.

2.12 „Anbieter-MCP-Server" bezeichnet MCP-Server, die vom Anbieter (Latoo.labs GmbH) entwickelt, betrieben und als Bestandteil der Brainy-Plattform bereitgestellt werden. Anbieter-MCP-Server sind integraler Bestandteil der Brainy-Agentic-AI-Funktionen und unterliegen der vollständigen

Verantwortung des Anbieters. Sie ermöglichen die Anbindung definierter Drittsysteme im Rahmen des Konnektor-Konzepts (§ 2.7) und sind im Rahmen dieser AGB wie Konnektoren zu behandeln.

2.13 „Kunden-MCP-Server" bezeichnet MCP-Server, die vom Nutzer selbst, von ihm beauftragten Dritten oder von Drittanbietern (z.B. über MCP-Marktplätze) bereitgestellt und in die Brainy-Anwendung integriert werden. Kunden-MCP-Server werden auf eigener Infrastruktur des Nutzers oder auf vom Nutzer beauftragter Drittinfrastruktur betrieben und unterliegen vollständig der Verantwortung des Nutzers. Der Anbieter hat keinen Einblick in die Implementierung, Sicherheit oder die durch den Kunden-MCP-Server angebundenen Systeme.

2.14 „MCP-Tool" (Werkzeug) bezeichnet eine einzelne, abgrenzbare Fähigkeit oder Aktion, die ein MCP-Server bereitstellt und die ein KI-Agent aufrufen kann (z. B. „Datei lesen", „Datei schreiben", „E-Mail senden", „Datenbankeintrag erstellen"). Jedes MCP-Tool wird innerhalb der Brainy-Anwendung einzeln identifiziert und kann vom Nutzer unabhängig aktiviert oder deaktiviert werden. Sämtliche MCP-Tools sind standardmäßig deaktiviert (Default-Off).

2.15 „Filesystem-Daten" bezeichnet Dateien, Ordner und Metadaten, die Nutzer oder KI-Agenten im gemeinsamen Dateibereich der Brainy-Anwendung ablegen oder austauschen.

2.16. „Paketgebühr“ ist das monatliche Grundentgelt für die Pakete Brainy Essential, Professional oder Business.

3. Leistungsbeschreibung

3.1 Die Anwendung ermöglicht dem Nutzer, verbale Aufzeichnungen in präzise und professionelle Texte umzuwandeln. Dies erfolgt durch die Integration von KI-Modellen.

3.2 Der konkrete Leistungsumfang der Anwendung richtet sich nach dem vom Nutzer gewählten Paket:

- Das Basispaket beinhaltet ausschließlich die Nutzung der Web-Version
- Erweiterte Pakete können zusätzlich die Nutzung der mobilen App (iOS und Android) umfassen
- Die Anzahl der inkludierten Coins, der verfügbare Speicher, die Dauer der Historie, die maximale Anzahl der Benutzer sowie die Anzahl der Workspaces unterscheiden sich je nach gewähltem Paket

3.3 Die Anwendung bietet je nach gebuchtem Paket folgende Funktionen:

- Protokollieren nach Terminen oder Telefonaten via Spracheingabe
- Erstellung von strukturierten Protokollen, Notizen, To-do Listen, Mails oder Berichten mittels Ausleitungsvorlagen
- Unterstützung unterschiedlicher Sprachen und Dialekte in Eingabe sowie Ausgabe
- Upload von Audiodateien in den aktuell unterstützten Formaten
- Speichern der erstellten Dokumente in den aktuell unterstützten Formaten
- Synchronisation zwischen Desktopanwendung und App für alle Endgeräte und Browser (sofern im gebuchten Paket enthalten)
- Erstellung von sprach-, text-, und bildverarbeitenden Assistenten zur Abbildung und Automatisierung von unterschiedlichen Workflows

3.4 Agentic AI Funktionen und Konnektoren (sofern im gebuchten Paket enthalten oder gesondert freigeschaltet):

Die Anwendung bietet darüber hinaus Agentic AI Funktionen, die über die klassische Assistenten-Nutzung hinausgehen. Diese Funktionen ermöglichen es, KI-Agenten zu erstellen und zu betreiben, die eigenständig Aufgaben ausführen und mit externen Systemen interagieren:

- Erstellung und Konfiguration von KI-Agenten, die eigenständig mehrstufige Aufgaben ausführen können
- Anbindung von Drittdiensten über Konnektoren (z.B. E-Mail-Konten, Dateispeicher, Kalender, CRM-Systeme) via Nango-Infrastruktur
- Autonomes Lesen, Verarbeiten und – sofern entsprechend konfiguriert – Schreiben von Daten in verbundenen Drittdiensten
- Automatisierte Ausführung von Workflows auf Basis von Triggern oder Zeitplänen
- Protokollierung von Agentenaktionen und -ergebnissen
- Integration von Anbieter-MCP-Servern zur standardisierten Anbindung weiterer Drittsysteme und Werkzeuge
- Integration von Kunden-MCP-Servern, die der Nutzer selbst bereitstellt oder beauftragt, um eigene Systeme und Datenquellen anzubinden (vgl. § 6.8.6)
- Granulare Steuerung einzelner MCP-Tools: Der Nutzer kann für jeden MCP-Server (Anbieter- und Kunden-MCP-Server) einzelne Tools unabhängig voneinander aktivieren oder deaktivieren. Sämtliche MCP-Tools sind standardmäßig deaktiviert (Default-Off); ein KI-Agent kann ein MCP-Tool erst nutzen, nachdem der Nutzer oder ein autorisierter Administrator das Tool explizit aktiviert hat. Der Anbieter zeigt für jedes MCP-Tool die vom jeweiligen MCP-Server bereitgestellte Beschreibung an, die dem Nutzer die Einschätzung ermöglicht, ob das Tool lesend, schreibend, löschend oder kommunizierend auf Daten zugreift

3.4.1 Der Umfang der verfügbaren Konnektoren und Agentic AI Funktionen ergibt sich aus der jeweils aktuellen Produktdokumentation und dem gebuchten Paket. Der Anbieter behält sich vor, verfügbare Konnektoren zu erweitern, zu ändern oder – insbesondere aus Sicherheitsgründen – zu entfernen.

3.4.2 Die Nutzung von Konnektoren setzt voraus, dass der Nutzer dem jeweiligen Drittdienst gegenüber zur Erteilung der Zugriffsberechtigung berechtigt ist und durch die Einrichtung des Konnektors nicht gegen Nutzungsbedingungen des Drittdienstes verstößt. Die Verantwortung hierfür trägt ausschließlich der Nutzer. Dasselbe gilt sinngemäß für die Nutzung von Anbieter-MCP-Servern.

3.4.3 Der Anbieter weist ausdrücklich darauf hin, dass KI-Agenten auf Basis der ihnen zur Verfügung gestellten Informationen und Konfigurationen agieren. Die Qualität und Sicherheit der Ergebnisse hängt maßgeblich von der Konfiguration durch den Nutzer ab. Der Anbieter kann keine Garantie dafür übernehmen, dass KI-Agenten in jedem Szenario das vom Nutzer beabsichtigte Ergebnis erzielen.

3.4.4 Hinweis zum Coin-Verbrauch bei Agentic AI Funktionen: Der Nutzer wird ausdrücklich darauf hingewiesen, dass die Nutzung von KI-Agenten mit einem erheblich höheren Coin-Verbrauch verbunden sein kann als die klassische Assistenten-Nutzung. KI-Agenten führen oft mehrere aufeinanderfolgende KI-Modellanfragen aus (z.B. für Planung, Zwischenschritte, Werkzeugnutzung und Ergebnisauswertung), verarbeiten ggf. große Mengen externer Daten aus Drittdiensten und können bei automatisierten Workflows ohne weiteres Zutun des Nutzers fortlaufend Coins verbrauchen. Das monatlich im Paket inkludierte Coin-Kontingent kann bei intensiver Agent-Nutzung schnell aufgebraucht sein. Der Anbieter empfiehlt, den Coin-Verbrauch bei der Nutzung von Agentic AI Funktionen regelmäßig zu beobachten. Zusätzliche Coins können jederzeit direkt über die Brainy-Anwendung erworben werden.

3.5 Der Anbieter gewährleistet keine ununterbrochene Verfügbarkeit der Anwendung. Insbesondere folgende Umstände können zu vorübergehenden Einschränkungen führen:

- Wartungsarbeiten
- Technische Störungen
- Störungen oder Änderungen bei Drittdiensten

Bei Vorliegen höherer Gewalt gelten die Regelungen des § 13.

3.6 Der Anbieter behält sich vor, die Anwendung und deren Funktionsumfang weiterzuentwickeln. Wesentliche einschränkende Veränderungen am Funktionsumfang werden dem Nutzer mindestens 14 Tage vor Umsetzung angekündigt.

4. KI-Modelle und Datenverarbeitung

4.1 Die Anwendung nutzt verschiedene KI-Modelle zur Verarbeitung der Nutzereingaben. Diese werden in drei Kategorien eingeteilt und in der Anwendung entsprechend gekennzeichnet. Diese Kennzeichnung erfolgt entweder mit entsprechenden Icons oder mit Hinweistexten.

4.2 **EU-gehostete KI-Modelle (Kennzeichnung „EU"):**

Als „EU“ gekennzeichnete KI-Modelle werden vollständig innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums verarbeitet. Dies umfasst sowohl die Speicherung der Daten („data at rest“) als auch die Verarbeitung der Eingaben und Ausgaben („inference processing“). Eine planmäßige Übermittlung personenbezogener Daten in Drittländer erfolgt bei diesen Modellen nicht.

4.3 **DSGVO-konforme KI-Modelle (Kennzeichnung „DSGVO")**

Als „DSGVO“ gekennzeichnete KI-Modelle werden von Anbietern betrieben, mit denen ein Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO sowie geeignete Garantien nach Art. 46 DSGVO, insbesondere EU-Standardvertragsklauseln, abgeschlossen wurden. Bei diesen Modellen kann die Verarbeitung der Eingaben auch außerhalb der EU stattfinden, während die dauerhafte Speicherung der Daten innerhalb der EU verbleibt. Für diese Modelle wurde eine Bewertung der Angemessenheit der Schutzmaßnahmen (Transfer Impact Assessment) durchgeführt. Die Kennzeichnung „DSGVO“ stellt dabei die Einschätzung dar, dass die vertraglichen, technischen und organisatorischen Voraussetzungen für eine DSGVO-konforme Verarbeitung nach aktuellem Stand der Technik und Rechtsprechung erfüllt sind. Diese Kennzeichnung ersetzt jedoch nicht die eigenständige Prüfpflicht des Nutzers als Verantwortlicher im Sinne der DSGVO. Insbesondere bei der Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO wird die Nutzung EU-gehosteter Modelle empfohlen.

4.4 **Nicht-EU-gehostete KI-Modelle (Kennzeichnung „Weltweit")**

Als „Weltweit“ gekennzeichnete KI-Modelle werden aktuell von Anbietern in den Vereinigten Staaten betrieben, wobei sowohl die Verarbeitung als auch die Speicherung außerhalb der EU erfolgen kann. Es bestehen Standardvertragsklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO sowie zusätzliche technische Schutzmaßnahmen. Dennoch kann das Datenschutzniveau in den USA trotz dieser Maßnahmen möglicherweise nicht vollständig dem EU-Niveau entsprechen. Die Nutzung solcher Modelle erfolgt ausschließlich auf ausdrückliche und dokumentierte Weisung des Nutzers. Für sensible oder personenbezogene Daten wird empfohlen, ausschließlich EU- oder DSGVO-gekennzeichnete KI-Modelle zu verwenden.

4.5 **Modellnutzung in Assistenten und KI-Agenten**

4.5.1 Voller Leistungsumfang als Voreinstellung: Assistenten und KI-Agenten können im Rahmen einzelner Verarbeitungsschritte unterschiedliche KI-Modelle einsetzen. Jedem Nutzer stehen standardmäßig alle verfügbaren KI-Modelle aller Kategorien (EU, DSGVO und Weltweit) zur

Verfügung. Der Anbieter kennzeichnet jedes KI-Modell und jeden Workflow transparent mit der jeweils zutreffenden Kategorie (vgl. §§ 4.2 bis 4.4).

4.5.2 **Prinzip des schwächsten Glieds**: Der gesamte Workflow eines Assistenten oder KI-Agenten wird nach dem Prinzip des „schwächsten Glieds" gekennzeichnet: Sobald mindestens ein DSGVO-Modell verwendet wird, gilt der gesamte Workflow als „DSGVO"; sobald mindestens ein Weltweit-Modell eingesetzt wird, wird der gesamte Workflow als „Weltweit“ klassifiziert. In den Aktionsprotokollen wird jeder Verarbeitungsschritt einschließlich des jeweils verwendeten Modells und dessen Hosting-Kategorie dokumentiert.

4.5.3 **Dokumentierte Weisung durch Modellauswahl**: Die Auswahl eines KI-Modells durch einen autorisierten Nutzer in der Benutzeroberfläche gilt als dokumentierte Weisung des Verantwortlichen im Sinne des Auftragsverarbeitungsvertrags (AVV). Bei KI-Modellen der Kategorien „DSGVO" oder „Weltweit“ umfasst diese Weisung die Zustimmung zur Verarbeitung gemäß §§ 4.3 bzw. 4.4, einschließlich der dort beschriebenen Drittlandübermittlungen.

4.5.4 **Einschränkung der Modell-Kategorien auf Weisung**: Der Verantwortliche kann jederzeit durch eine einmalige, schriftliche Weisung (E-Mail an den Anbieter oder über die dafür vorgesehene Funktion in der Brainy-Anwendung) die mandantenweit zulässigen Modell-Kategorien einschränken:

- Stufe „Nur EU": Es werden ausschließlich KI-Modelle der Kategorie „EU" verwendet. KI-Modelle der Kategorien „DSGVO" und „Weltweit“ werden in der Benutzeroberfläche nicht mehr angeboten und stehen weder Nutzern noch Assistenten oder KI-Agenten zur Verfügung.
- Stufe „EU + DSGVO": Es werden KI-Modelle der Kategorien „EU" und „DSGVO" verwendet. KI-Modelle der Kategorie „Weltweit“ werden in der Benutzeroberfläche nicht mehr angeboten.

Die Einschränkung wird nach Eingang der Weisung unverzüglich, spätestens jedoch binnen 5 Werktagen, technisch umgesetzt. Bestehende Assistenten und KI-Agenten, die Modelle aus nicht mehr zugelassenen Kategorien verwenden, werden deaktiviert oder auf ein zulässiges Modell umgestellt; der Anbieter informiert den Verantwortlichen über betroffene Konfigurationen.

4.5.5 **Änderung und Aufhebung**: Die Einschränkung gilt zeitlich unbefristet, bis der Verantwortliche durch eine neue schriftliche Weisung eine andere Stufe festlegt oder die Einschränkung aufhebt (Rückkehr zum vollen Leistungsumfang). Änderungen werden nach den gleichen Fristen gemäß § 4.5.4 umgesetzt.

4.6 Der Anbieter erfüllt als Bereitsteller der Brainy-Anwendung die ihn treffenden Pflichten aus dem EU AI Act, insbesondere Transparenzpflichten gemäß Art. 50 AI Act. Die Brainy-Anwendung wird als Allzweck-KI-Werkzeug bereitgestellt und ist nicht für einen spezifischen Einsatzzweck bestimmt. Die Verantwortung für die Einhaltung der Bestimmungen des EU AI Acts, die den Betreiber (Deployer) eines KI-Systems betreffen, liegt beim Nutzer. Dies umfasst insbesondere die Einordnung des konkreten Anwendungsfalls in die Risikoklassen des AI Acts, die Erfüllung etwaiger Pflichten für Hochrisiko-KI-Systeme sowie die Sicherstellung einer angemessenen menschlichen Aufsicht. Der Nutzer ist verpflichtet, sich über die für ihn als Betreiber geltenden Anforderungen des EU AI Acts zu informieren und diese bei der Nutzung der Anwendung zu beachten. Weitere Details dazu sind im Dokument „AI ACT Compliance Notice“ festgehalten.

4.7 Im Rahmen der Agentic AI Funktionen können KI-Agenten auf externe Daten (z.B. Inhalte von E-Mails, Dateien, Webseiten) zugreifen, die an KI-Modelle zur Verarbeitung weitergegeben werden. Die Auswahl des KI-Modells, das im Rahmen von Agentic AI Workflows verwendet wird, obliegt dem Nutzer. Der Anbieter empfiehlt, für Agentic AI Anwendungen, bei denen potenziell sensible externe Daten verarbeitet werden, ausschließlich EU-gehostete KI-Modelle zu verwenden.

4.8. Bei Widersprüchen zwischen diesen AGB und der AI Act Compliance Notice hat die AI Act Compliance Notice in Fragen der AI-Act-Compliance Vorrang.

5. Registrierung und Vertragsschluss

5.1 Für die Nutzung der Anwendung ist die Bestellung, die Bestätigung dieser AGB sowie der Abschluss eines Auftragsverarbeitungsvertrags (AVV) durch den Nutzer erforderlich. Der Nutzer handelt dabei als datenschutzrechtlich Verantwortlicher im Sinne der DSGVO. Die Bestellung kommt durch ein unterfertigtes Preisblatt oder ein unterzeichnetes Angebot sowie eine schriftliche Auftragsbestätigung oder Rechnung des Anbieters zustande. Die vereinbarte Vertragslaufzeit beginnt mit dem Datum der Auftragsbestätigung oder, sollte diese nicht separat erfolgen, mit dem Rechnungsdatum.

5.2 Nach Vertragsschluss erhält der Nutzer Zugangsdaten für die Webanwendung und, falls im gewählten Paket enthalten, für die mobilen Anwendungen über den App-Store bzw. Play-Store.

5.3 Der Nutzer sichert zu, dass alle von ihm bei der Registrierung angegebenen Daten wahr und vollständig sind. Er verpflichtet sich, den Anbieter unverzüglich über Änderungen der Daten zu informieren.

6. Nutzungsrechte und Pflichten des Nutzers

6.1 Der Anbieter räumt dem Nutzer ein einfaches, nicht übertragbares, nicht unterlizenzierbares und nicht exklusives Recht ein, die Anwendung für die Dauer der vereinbarten Vertragslaufzeit bestimmungsgemäß zu nutzen.

6.2 Die Anwendung und der dieser zugrundeliegende Quellcode sowie die in der Anwendung hinterlegten Inhalte sind urheberrechtlich geschützt. Das Urheberrecht liegt ausschließlich beim Anbieter (Latoo.labs GmbH). Dem Nutzer ist es untersagt, die Anwendung:

- ganz oder teilweise zu vervielfältigen, zu vermieten oder zu verleasen
- zu bearbeiten oder anderweitig umzugestalten
- zu unterlizenzieren
- zu dekompilieren, zu disassemblieren oder zurückzuentwickeln ("Reverse Engineering"), soweit dies nicht gesetzlich ausdrücklich erlaubt ist

6.3 Der Nutzer verpflichtet sich:

- einen angemessenen Schutz auf seinem Endgerät zu implementieren
- sicherzustellen, dass die Anwendung nicht durch unbefugte Dritte genutzt wird
- diese AGB sowie alle anwendbaren gesetzlichen Bestimmungen einzuhalten
- die Anwendung nicht für rechtswidrige Zwecke zu verwenden
- nicht in die gewerblichen Schutz- und Urheberrechte des Anbieters oder Rechte Dritter einzugreifen
- die technische Infrastruktur des Anbieters nicht zu gefährden oder zu beeinträchtigen
- keine schädlichen Codes oder Programme in die Anwendung einzubringen

6.4 Die Verwendung oder Übertragung von rechtswidrigen Informationen oder Material durch den Nutzer ist untersagt. Das beinhaltet ausdrücklich, aber nicht ausschließlich, Gewaltdarstellungen, Diskriminierungen, Aufrufe zu Gewalt oder zu Straftaten, Verletzung von Urheberrechten, Markenrechten und anderen Immaterialgüterrechten und Warenzeichen-Missbrauch.

6.5 Der Nutzer verpflichtet sich, das Produkt nur innerhalb der gesetzlichen Auflagen und bestimmungsgemäß zu verwenden. Dies umfasst insbesondere die Einhaltung der datenschutzrechtlichen Bestimmungen, des EU AI Acts und anderer auf die Nutzung von KI-Technologien anwendbarer Rechtsvorschriften.

6.6 Der Nutzer stellt den Anbieter von sämtlichen Forderungen und Ansprüchen Dritter frei, die aufgrund einer Verletzung der vorgenannten Pflichten entstehen.

6.7 Der Nutzer ist verpflichtet, mindestens einen Administrator für sein Unternehmenskonto zu benennen. Administratoren sind für die Verwaltung der Nutzerkonten und Einstellungen der Organisation verantwortlich. Der Kunde bevollmächtigt den/die von ihm benannten Administrator(en), Erklärungen, die das Vertragsverhältnis betreffen, wie insbesondere die Zustimmung zu Änderungen dieser Allgemeinen Geschäftsbedingungen, mit Wirkung für die gesamte Organisation abzugeben.

6.8 **Besondere Pflichten bei der Nutzung von Agentic AI Funktionen und Konnektoren**:

Bei der Nutzung von Agentic AI Funktionen und der Einrichtung von Konnektoren treffen den Nutzer folgende zusätzliche Pflichten:

6.8.1 **Konfigurationsverantwortung**: Der Nutzer ist allein verantwortlich für die sachgemäße Konfiguration von KI-Agenten und Konnektoren. Dies umfasst insbesondere:

- Die Einrichtung angemessener Zugriffsberechtigungen nach dem Prinzip der minimalen Rechtevergabe ("Least Privilege") – KI-Agenten dürfen nur auf jene Ressourcen in Drittdiensten zugreifen, die für die jeweilige Aufgabe tatsächlich erforderlich sind
- Die Überprüfung und laufende Kontrolle der durch KI-Agenten ausgeführten Aktionen und deren Ergebnisse
- Die Einrichtung geeigneter Genehmigungsworkflows für besonders sensible oder irreversible Aktionen (z.B. Löschen von Daten, Versenden von E-Mails an externe Empfänger)
- Die Sicherstellung, dass Konnektoren nur zu Drittdiensten eingerichtet werden, auf die der Nutzer rechtlich zugreifen darf und für die er zur Erteilung der Zugriffsberechtigung befugt ist

6.8.2 **Sicherheitspflichten bei Konnektoren**: Der Nutzer verpflichtet sich:

- Connector-Zugangsdaten, OAuth-Tokens und ähnliche Zugriffsberechtigungen vertraulich zu behandeln und vor unbefugtem Zugriff zu schützen
- Nicht mehr benötigte Konnektoren unverzüglich zu deaktivieren und die Zugriffsberechtigungen beim jeweiligen Drittdienst zu widerrufen
- Den Anbieter unverzüglich zu informieren, wenn der Verdacht besteht, dass Connector-Zugangsdaten kompromittiert wurden
- Keine Konfigurationen vorzunehmen, die es externen Daten (z.B. Inhalten aus E-Mails oder Dokumenten) ermöglichen, den KI-Agenten zu manipulieren oder umzuleiten (Schutz vor Prompt Injection)

6.8.3 **Überwachungspflicht**: Der Nutzer ist verpflichtet, die Aktivitäten von KI-Agenten regelmäßig zu überwachen. Insbesondere hat der Nutzer:

- Protokolle der Agentenaktivitäten regelmäßig zu prüfen
- Bei unerwarteten oder unbeabsichtigten Agentenaktionen den Agenten unverzüglich zu stoppen oder zu deaktivieren
- Den Anbieter über schwerwiegende Vorfälle im Zusammenhang mit KI-Agenten unverzüglich zu informieren

6.8.4 **Verbotene Konfigurationen**: Es ist dem Nutzer untersagt:

- KI-Agenten so zu konfigurieren, dass diese unkontrolliert auf kritische Infrastrukturen zugreifen können
- Konnektoren zu Drittdiensten einzurichten, bei denen ein erhöhtes Risiko für Prompt Injection-Angriffe besteht, ohne angemessene Schutzmaßnahmen implementiert zu haben
- KI-Agenten mit Zugriffsrechten auszustatten, die über den für die jeweilige Aufgabe erforderlichen Umfang hinausgehen
- Agentic AI Funktionen für automatisierte Entscheidungen einzusetzen, die rechtlich relevante oder erhebliche Auswirkungen auf Personen haben, ohne ausreichende menschliche Aufsicht sicherzustellen
- KI-Agenten so zu nutzen, um bestehende Mechanismen der Brainy Anwendung auszuhebeln oder Reverse-Engineering zu machen.

6.8.5 **Bestimmungsgemäße Nutzung**: Agentic AI Funktionen sind ausschließlich für legale Geschäftszwecke zu verwenden. Eine Nutzung, die darauf abzielt, andere Systeme, Personen oder Organisationen zu schädigen, zu überwachen oder zu manipulieren, ist untersagt.

6.8.6 **Besondere Pflichten bei der Nutzung von Kunden-MCP-Servern**:

Die Integration von Kunden-MCP-Servern in die Brainy-Anwendung begründet erweiterte Verantwortlichkeiten des Nutzers, da der Anbieter keinen Einblick in die Implementierung, Sicherheitskonfiguration oder die durch den Kunden-MCP-Server angebundenen Systeme hat.

a. **Eigenverantwortung für Implementierung und Sicherheit**:
Der Nutzer ist allein verantwortlich für die sichere Implementierung und den sicheren Betrieb des Kunden-MCP-Servers. Dies umfasst insbesondere: – Implementierung nach dem aktuellen Stand der Technik (Authentifizierung, Transportverschlüsselung TLS 1.2+, Input-Validierung) – Regelmäßige Sicherheitsüberprüfungen und Aktualisierungen des MCP-Servers – Schutz vor unbefugtem Zugriff auf den MCP-Server selbst – Beschränkung der durch den MCP-Server exponierten Funktionalität auf das für den jeweiligen Agenten-Use-Case tatsächlich Erforderliche
b. **Verantwortung für angebundene Systeme**:
Der Nutzer trägt die alleinige Verantwortung für alle Systeme, Datenquellen und Dienste, die über den Kunden-MCP-Server zugänglich gemacht werden. Dies umfasst: – Die Einhaltung der Nutzungsbedingungen der angebundenen Drittsysteme – Die datenschutzrechtliche Zulässigkeit des Datenzugriffs über den Kunden-MCP-Server (DSGVO-Konformität) – Die Absicherung gegen unbeabsichtigten oder unbefugten Datenzugriff durch den KI-Agenten auf über den MCP-Server erreichbare Systeme
c. **Prompt Injection-Schutz**:
Da Kunden-MCP-Server Daten aus beliebigen Quellen an den KI-Agenten zurückliefern können, besteht ein erhöhtes Prompt Injection-Risiko. Der Nutzer verpflichtet sich: – Daten, die der Kunden-MCP-Server von externen Quellen bezieht, vor der Rückgabe an den Agenten auf manipulative Inhalte zu prüfen oder entsprechende Validierungsmaßnahmen zu implementieren – Den Anbieter unverzüglich zu informieren, wenn der Verdacht besteht, dass über den Kunden-MCP-Server ein Prompt Injection-Angriff stattgefunden hat – Die Funktionalität des Kunden-MCP-Servers so zu begrenzen, dass manipulierte Rückgabewerte keinen übermäßigen Schaden anrichten können
d. **Drittanbieter-MCP-Server**:
Integriert der Nutzer MCP-Server von Drittanbietern (z.B. aus MCP-Marktplätzen oder Open-Source-Quellen), haftet er für deren Sicherheit und Verhalten wie für selbst entwickelte Kunden-

MCP-Server. Der Nutzer hat die Vertrauenswürdigkeit und Sicherheit von Drittanbieter-MCP-Servern vor der Integration eigenständig zu prüfen.

e. **Mindestanforderungen an Kunden-MCP-Server**:
Der Nutzer verpflichtet sich, nur Kunden-MCP-Server zu integrieren, die folgende Mindestanforderungen erfüllen: – Verwendung von Transportverschlüsselung (HTTPS/TLS) für alle Kommunikation zwischen Brainy-Agent und Kunden-MCP-Server – Implementierung einer Authentifizierung, die sicherstellt, dass nur autorisierte Brainy-Agenten des Nutzers auf den Kunden-MCP-Server zugreifen können – Keine Persistierung von Daten aus den Agent-Anfragen über den für die Aufgabenerfüllung erforderlichen Zeitraum hinaus – Protokollierung aller Anfragen und Antworten für Audit-Zwecke

f. **Recht des Anbieters zur Sperrung**:
Der Anbieter ist berechtigt, die Integration eines Kunden-MCP-Servers zu sperren oder einzuschränken, wenn konkrete Anhaltspunkte dafür bestehen, dass der Kunden-MCP-Server die Sicherheit der Brainy-Plattform, anderer Kunden oder Dritter gefährdet. Der Anbieter wird den Nutzer vor einer Sperrung – sofern die Situation dies erlaubt – informieren und ihm Gelegenheit zur Behebung des Problems geben.

6.8.7 **Pflichten bei der Aktivierung von MCP-Tools**

a) **Default-Off-Prinzip**:
Alle MCP-Tools sind bei erstmaliger Einrichtung eines MCP-Servers deaktiviert. Der Nutzer aktiviert nur jene Tools, die für den jeweiligen Anwendungsfall tatsächlich erforderlich sind. Insbesondere Tools mit schreibenden, löschenden oder kommunizierenden Fähigkeiten (z. B. E-Mail-Versand, Dateilöschung, Datenbankschreibzugriff) dürfen nur nach sorgfältiger Prüfung der Erforderlichkeit und der potenziellen Auswirkungen aktiviert werden.

b) **Prüfpflicht bei Kunden-MCP-Server-Tools**:
Vor der Aktivierung eines Tools auf einem Kunden-MCP-Server ist der Nutzer verpflichtet, die vom MCP-Server bereitgestellte Tool-Beschreibung eigenständig auf Richtigkeit und Vollständigkeit zu prüfen. Der Anbieter zeigt die Beschreibung unverändert an, übernimmt jedoch keine Gewähr für deren inhaltliche Richtigkeit bei Kunden-MCP-Servern (vgl. § 2.13). Der Nutzer ist verpflichtet sicherzustellen, dass die Beschreibungen der Tools auf Kunden-MCP-Servern stets den tatsächlichen Fähigkeiten der Tools entsprechen. Ändert sich die Funktionalität eines Tools, ist der Nutzer verpflichtet, das Tool zu deaktivieren und erst nach erneuter Prüfung wieder zu aktivieren.

c) **Regelmäßige Überprüfung**:
Der Nutzer ist verpflichtet, die Liste der aktivierten MCP-Tools regelmäßig zu überprüfen und nicht mehr benötigte Tools unverzüglich zu deaktivieren.

d) **Empfehlung Human-in-the-Loop**:
Der Anbieter empfiehlt, für MCP-Tools mit schreibenden, löschenden oder kommunizierenden Fähigkeiten die in der Anwendung verfügbare Human-in-the-Loop-Funktion (manuelle Genehmigung vor Ausführung) zu aktivieren.

6.9 **In-App-Bestätigungen für risikoreiche Funktionen**

6.9.1 Der Anbieter ist berechtigt, für bestimmte Funktionen mit erhöhtem Risikopotenzial eine gesonderte in-App-Bestätigung des jeweiligen Nutzers zu verlangen, bevor dieser die entsprechende Funktion erstmalig verwenden kann. Diese Bestätigungen ergänzen die Zustimmung des Administrators zu diesen AGB, ersetzen sie jedoch nicht. Sie dienen der Sicherstellung, dass individuelle Nutzer über die spezifischen Risiken der betreffenden Funktion informiert sind, und entsprechen der Anforderung des EU AI Acts (Art. 4), wonach der Betreiber sicherzustellen hat, dass Nutzer über ein ausreichendes Maß an KI-Kompetenz verfügen.

6.9.2 In-App-Bestätigungen können insbesondere für folgende Funktionen eingeholt werden:

a. Einrichten eines Konnektors zu einem Drittdienst: Der Nutzer bestätigt, dass er zur Erteilung der Zugriffsberechtigung für den jeweiligen Drittdienst berechtigt ist, die Nutzungsbedingungen des Drittdienstes dies erlauben und er über das Risiko von Prompt Injection informiert wurde.
b. Auswahl eines KI-Modells der Kategorie „DSGVO" oder „Weltweit“: Der Nutzer nimmt zur Kenntnis, dass bei Modellen der Kategorie „DSGVO" die Inference-Verarbeitung auch außerhalb der EU erfolgen kann bzw. bei Modellen der Kategorie „Weltweit“ Daten an einen Anbieter in den USA übermittelt werden. Der Nutzer wird darauf hingewiesen, dass der Verantwortliche die zulässigen Modell-Kategorien mandantenweit auf „Nur EU" oder „EU + DSGVO" einschränken kann (vgl. § 4.5.4).
c. Erstmalige Ausführung eines Agenten-Workflows mit Schreibzugriff auf Drittdienste: Der Nutzer bestätigt durch Auswahl entsprechender Tools, dass er die Reichweite der durch den Agenten ausführbaren Aktionen (z.B. Versenden von E-Mails, Ändern von Dateien) verstanden hat und geeignete Kontrollmechanismen eingerichtet hat.
d. Erstmalige Aktivierung eines MCP-Tools mit schreibender, löschender oder kommunizierender Funktion: Der Nutzer bestätigt, dass er die Beschreibung des Tools geprüft hat, die damit verbundenen Risiken (insbesondere irreversible Aktionen und Prompt Injection) versteht und die Aktivierung für den beabsichtigten Anwendungsfall erforderlich ist. Bei Tools auf Kunden-MCP-Servern bestätigt der Nutzer zusätzlich, dass er die Richtigkeit der Tool-Beschreibung eigenständig verifiziert hat.

6.9.3 Der Anbieter protokolliert in-App-Bestätigungen revisionssicher mit Zeitstempel und Benutzer-ID.

6.9.4 Verweigert ein Nutzer eine erforderliche in-App-Bestätigung, steht ihm die betreffende Funktion nicht zur Verfügung. Eine Verpflichtung des Anbieters zur Bereitstellung der Funktion ohne diese Bestätigung besteht nicht. Die Ablehnung einer in-App-Bestätigung durch einen Nutzer stellt keinen Mangel der Anwendung im Sinne von § 9.2 dar.

7. Vergütung und Zahlungsbedingungen

7.1 Die Vergütung für die Nutzung der Anwendung basiert auf dem vom Nutzer gewählten Paket, das eine bestimmte Anzahl inkludierter Coins, verfügbaren Speicher, Dauer der Historie, maximale Anzahl an Benutzern und Anzahl an Workspaces enthält. Ein Coin entspricht in etwa einem Euro an KI-Nutzungskosten. Der Coin-Verbrauch variiert je nach gewähltem KI-Modell und Art der Nutzung.

7.2 Der Verbrauch an Coins wird laufend in Echtzeit erfasst und dem Nutzer transparent in der Anwendung angezeigt. Das im Vertrag festgelegte monatliche Coin-Kontingent steht dem Nutzer ab dem jeweiligen Abrechnungsbeginn zur Verfügung. Nicht verbrauchte Coins verfallen am Ende des jeweiligen Abrechnungszeitraums, sofern nicht anders vereinbart. Der Nutzer wird ausdrücklich darauf hingewiesen, dass die Nutzung von KI-Agenten (Agentic AI Funktionen) zu einem signifikant höheren Coin-Verbrauch führen kann als die Nutzung klassischer Assistenzfunktionen. Insbesondere bei mehrstufigen Agenten-Workflows, der Verarbeitung großer Datenmengen aus Drittdiensten sowie bei automatisierten, zeitgesteuerten Ausführungen sowie beim Einsatz von MCP-Servern (insbesondere Kunden-MCP-Servern mit umfangreichen Datenquellen) kann das monatlich inkludierte Coin-Kontingent deutlich schneller aufgebraucht werden als bei ausschließlicher Nutzung der Standard-Funktionen. Der Anbieter empfiehlt, den Coin-Verbrauch bei aktivierten Agenten regelmäßig zu prüfen.

7.3 Sind die verfügbaren Coins des Nutzers vollständig aufgebraucht, wird die Nutzung der Anwendung – einschließlich aller Assistenten- und Agentic AI Funktionen – automatisch unterbrochen, bis der Nutzer zusätzliche Coins erwirbt. Laufende Agenten-Workflows werden bei Erreichen des Coin-Limits gestoppt. Der Anbieter übernimmt keine Haftung für etwaige Schäden, die durch eine solche Unterbrechung entstehen, insbesondere nicht für unvollständig ausgeführte Agenten-Workflows oder damit verbundene Folgen in Drittdiensten. Zusätzliche Coins können vom Nutzer jederzeit direkt in der Brainy-Anwendung erworben werden und stehen unmittelbar nach dem Erwerb zur Verfügung. Der Anbieter kann bei Überschreitung des Kontingents alternativ auch zusätzliche Gebühren gemäß der aktuellen Preisliste erheben, sofern dies mit dem Nutzer im Einzelfall gesondert vereinbart wurde.

7.4 Die Abrechnung erfolgt periodisch zum Datum des Vertragsabschlusses und wird im Voraus berechnet. Der Rechnungsbetrag ist innerhalb von 14 Tagen nach Rechnungserhalt ohne Abzug zu zahlen.

7.5 Bei einer Änderung des gewählten Leistungspakets zu einem höherwertigen Paket während der laufenden Vertragslaufzeit sind die dadurch entstehenden Mehrkosten vom Nutzer unverzüglich nach Durchführung der Änderung zu bezahlen. Diese Mehrkosten werden für den Zeitraum von der Änderung bis zum Ende der vereinbarten Vertragslaufzeit berechnet.

7.6 Nach Ablauf der ursprünglich vereinbarten Vertragslaufzeit wird der Vertrag zu den Konditionen des höherwertigen Leistungspakets fortgeführt, sofern er nicht fristgerecht gekündigt wurde.

7.7 Bei Zahlungsverzug ist der Anbieter nach Mahnung und Nachfristsetzung von 14 Tagen berechtigt, den Zugang zur Anwendung zu sperren. Die vertraglichen Zahlungspflichten des Nutzers bleiben hiervon unberührt.

8. Datenschutz und Datensicherheit

8.1 Der Anbieter verarbeitet die personenbezogenen Daten des Nutzers unter Einhaltung der gesetzlichen Datenschutzbestimmungen, insbesondere der Datenschutz-Grundverordnung (DSGVO).

8.2 Die in die Anwendung eingegeben und hochgeladenen Daten werden zur Erfüllung des Vertragszwecks verarbeitet. Der Anbieter ergreift angemessene technische und organisatorische Maßnahmen zum Schutz dieser Daten.

8.3 Der Anbieter hat keinen Einfluss auf die Datenverarbeitung durch KI-Modelle, die außerhalb der EU/des EWR gehostet werden. Bei Nutzung dieser Modelle erfolgt eine Datenübermittlung in Drittländer. Soweit ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO für das jeweilige Drittland vorliegt, stützt sich die Übermittlung hierauf. Liegt kein Angemessenheitsbeschluss vor, erfolgt die Übermittlung auf Grundlage von Standardvertragsklauseln (Standard Contractual Clauses – SCC) gemäß Art. 46 Abs. 2 lit. c DSGVO, die der Anbieter mit dem jeweiligen KI-Modellanbieter abgeschlossen hat. Der Nutzer kann auf Anfrage eine Kopie der abgeschlossenen SCC erhalten. Der Nutzer ist als Verantwortlicher verpflichtet, eigenständig zu prüfen, ob die Übermittlung personenbezogener Daten an KI-Modelle in Drittländern mit seinen datenschutzrechtlichen Pflichten vereinbar ist. Der Anbieter empfiehlt, für sensible oder personenbezogene Daten ausschließlich EU-gehostete KI-Modelle zu verwenden. Die Auswahl des KI-Modells erfolgt aktiv durch den Nutzer, wobei die Kennzeichnung „EU" die Zuordnung transparent macht.

8.4 Der Anbieter führt regelmäßige Backups der Nutzerdaten durch. Dennoch empfiehlt der Anbieter dem Nutzer, regelmäßig eigene Sicherungskopien seiner wichtigen Daten zu erstellen.

8.5 Nach Ablauf der im Vertrag festgelegten Aufbewahrungsfrist (Historie) werden Daten, Chats und Dokumente automatisch gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

8.6 Die Brainy-Anwendung stellt eine Infrastruktur zur Verfügung, die der Nutzer nach eigener Entscheidung konfiguriert und einsetzt. Art, Umfang und Zweck der Verarbeitung personenbezogener Daten über KI-Agenten werden ausschließlich durch den Nutzer bestimmt. Der Anbieter bestimmt lediglich die technischen Mittel der Plattform und trifft keine eigenständigen Entscheidungen über Verarbeitungszwecke. Der Anbieter handelt daher als Auftragsverarbeiter gemäß Art. 28 DSGVO. Soweit eine Datenschutzaufsichtsbehörde im Einzelfall eine gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO feststellen sollte, verpflichten sich die Parteien, unverzüglich eine Vereinbarung gemäß Art. 26 DSGVO zu schließen.

8.7 Der Nutzer wird darauf hingewiesen, dass die Nutzung von Agentic AI Funktionen mit Zugriff auf personenbezogene Daten in Drittdiensten eine Datenschutz-Folgenabschätzung (DPIA) gemäß Art. 35 DSGVO erforderlich machen kann. Die Prüfung der Erforderlichkeit und die Durchführung einer DPIA obliegen dem Nutzer als Verantwortlichem. Der Anbieter unterstützt den Nutzer auf Anfrage durch Bereitstellung der notwendigen technischen Informationen.

8.8 **Datenschutz bei Agentic AI und Konnektoren**: Soweit KI-Agenten über Konnektoren auf Daten in Drittdiensten zugreifen, gilt Folgendes:

- Der Nutzer ist als Verantwortlicher im Sinne der DSGVO für die Rechtmäßigkeit des durch KI-Agenten erfolgenden Datenzugriffs auf Drittdienste verantwortlich. Der Anbieter handelt insoweit als Auftragsverarbeiter.
- Der Nutzer stellt sicher, dass der Einsatz von KI-Agenten für den Zugriff auf personenbezogene Daten in Drittdiensten einer ausreichenden Rechtsgrundlage im Sinne der DSGVO entspricht.
- Die über Konnektoren zugegriffenen Daten (z.B. E-Mail-Inhalte, Dateiinhalte) werden an KI-Modelle zur Verarbeitung weitergeleitet. Der Nutzer hat die Pflicht sicherzustellen, dass diese Daten nur an KI-Modelle mit angemessenem Schutzniveau weitergeleitet werden.
- Für die Verarbeitung von Daten über Konnektoren durch Nango Inc. (als Infrastrukturanbieter) werden entsprechende datenschutzrechtliche Vereinbarungen vorgehalten. Näheres regelt der Auftragsverarbeitungsvertrag (AVV).

8.9 Bei Fragen zum Datenschutz kann der Nutzer sich an den Datenschutzbeauftragten des Anbieters unter datenschutz@latoo.at wenden.

9. Gewährleistung und Haftung

9.1 Der Anbieter gewährleistet, dass die Anwendung im Wesentlichen die beschriebenen Funktionen erfüllt. Eine Gewähr für die Richtigkeit, Vollständigkeit oder bestimmte Qualität, der durch KI-Modelle erzeugten Inhalte wird nicht übernommen.

9.2 Auftretende Mängel der Anwendung sind vom Nutzer unverzüglich nach Entdeckung zu melden. Der Anbieter wird gemeldete Mängel innerhalb angemessener Frist beheben.

9.3 Der Anbieter haftet unbeschränkt für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit sowie für alle sonstigen Schäden, die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung des Anbieters, seiner gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen.

9.4 Bei leichter Fahrlässigkeit haftet der Anbieter nur bei der Verletzung von wesentlichen Vertragspflichten (Kardinalpflichten), deren Erfüllung die ordnungsgemäße Durchführung des

Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Nutzer regelmäßig vertrauen darf. In diesen Fällen ist die Haftung auf den Ersatz des vertragstypischen, vorhersehbaren Schadens begrenzt. Im Übrigen ist die Haftung für leichte Fahrlässigkeit ausgeschlossen. Dieser Ausschluss gilt nicht für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit. Die Haftung des Anbieters bei Vorliegen höherer Gewalt richtet sich nach § 13. Soweit ein Force-Majeure-Ereignis vorliegt, ist die Haftung für leichte und grobe Fahrlässigkeit nach Maßgabe von § 13 ausgeschlossen bzw. eingeschränkt.

9.5 Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

9.6 Die vorstehende Haftungsbeschränkung gilt gleichermaßen bei der Verursachung von Schäden durch gesetzliche Vertreter, leitende Angestellte oder sonstige Erfüllungsgehilfen des Anbieters.

9.7 Der Anbieter übernimmt keine Haftung für Schäden oder Rechtsverletzungen, die durch die Nutzung von KI-Modellen außerhalb der EU (gekennzeichnet mit „Weltweit“) entstehen.

9.8 Besondere Haftungsregelungen für Agentic AI Funktionen und Konnektoren:

9.8.1 Der **Haftungsausschluss für die Qualität KI-generierter Ergebnisse** (§ 9.1) gilt insbesondere auch für Entscheidungen und Handlungen, die KI-Agenten im Rahmen von Agentic AI Funktionen auf Basis KI-generierter Auswertungen eigenständig treffen und ausführen. Der Anbieter haftet nicht für Aktionen, die ein KI-Agent aufgrund unvorhersehbaren Verhaltens des zugrunde liegenden KI-Modells ausführt, soweit diese Aktionen im Rahmen der dem Agenten erteilten technischen Berechtigungen (Konnektoren, Tools) liegen. Der Nutzer ist verpflichtet, die technischen Berechtigungen so eng wie möglich zu halten (Least Privilege), um die Auswirkungen unerwarteten Agentenverhaltens zu begrenzen.

9.8.2 **Grundsatz der Nutzerverantwortung**: KI-Agenten handeln auf Basis der durch den Nutzer vorgenommenen Konfiguration und in dessen Namen. Alle durch einen KI-Agenten ausgeführten Autonomen Aktionen gelten rechtlich als durch den Nutzer veranlasst. Der Nutzer trägt die volle Verantwortung für die Folgen von Aktionen, die KI-Agenten in Drittdiensten ausführen.

9.8.3 **Haftungsausschluss bei Fehlkonfiguration**: Der Anbieter übernimmt keine Haftung für Schäden, die durch eine fehlerhafte, unvollständige oder unsachgemäße Konfiguration von KI-Agenten oder Konnektoren durch den Nutzer entstehen. Dies umfasst insbesondere:

- Schäden durch zu weit gefasste Zugriffsberechtigungen für KI-Agenten in Drittdiensten
- Schäden durch das unbeabsichtigte Löschen, Ändern oder Versenden von Daten durch KI-Agenten aufgrund fehlerhafter Konfiguration
- Schäden durch die Anbindung unsicherer oder nicht autorisierter Drittdienste
- Schäden durch das Fehlen geeigneter menschlicher Aufsicht und Kontrollmechanismen

9.8.4 **Haftungsausschluss bei Prompt Injection**:
Der Anbieter übernimmt keine Haftung für Schäden, die durch Prompt Injection-Angriffe entstehen. Dies umfasst insbesondere Schäden, die dadurch entstehen, dass schadhafte Inhalte in externen Daten (z.B. E-Mails, Dokumente, Webseiten), auf die ein KI-Agent zugreift, den Agenten zu unbeabsichtigten oder schädlichen Aktionen veranlassen. Der Nutzer ist verpflichtet, geeignete Schutzmaßnahmen gegen Prompt Injection zu implementieren (vgl. § 6.8.2). Im Falle eines Prompt Injection-Angriffs haftet ausschließlich der Angreifer; der Anbieter haftet nur dann, wenn er die in der AVV (Ziff. 4.4.2) beschriebenen Schutzmaßnahmen nicht implementiert hat.

9.8.5 **Haftungsausschluss bei Drittdiensten**:
Der Anbieter übernimmt keine Haftung für:

- Ausfälle, Fehler oder Sicherheitsvorfälle bei Drittdiensten, die über Konnektoren verbunden sind
- Änderungen der API oder Funktionalität von Drittdiensten, die zu einer Beeinträchtigung oder einem Ausfall von Konnektoren führen
- Datenverlust oder -beschädigung in Drittdiensten, der durch Aktionen von KI-Agenten verursacht wurde, soweit diese auf einer ordnungsgemäßen Konfiguration und im Rahmen der erteilten Zugriffsberechtigungen beruhen
- Sicherheitsvorfälle bei Drittdiensten, die nicht in der Sphäre des Anbieters liegen

9.8.6 Haftungsausschluss bei Nango-Infrastruktur:
Der Anbieter übernimmt keine Haftung für Sicherheitsvorfälle, Ausfälle oder Datenverluste, die auf Sicherheitslücken oder Fehler in der Nango-Infrastruktur zurückzuführen sind, soweit der Anbieter diese nicht zu vertreten hat und angemessene Vorkehrungen getroffen hat. Der Anbieter verpflichtet sich, mit Nango Inc. eine geeignete datenschutzrechtliche Vereinbarung zu unterhalten und sicherheitsrelevante Vorfälle bei Nango unverzüglich an den Nutzer zu kommunizieren.

9.8.7 **Freistellung bei KI-Agenten-Aktionen in Drittdiensten**:
Der Nutzer stellt den Anbieter von allen Ansprüchen Dritter frei, die aufgrund von Aktionen entstehen, die KI-Agenten im Namen des Nutzers in Drittdiensten ausführen, insbesondere bei Schäden durch:

- fehlerhafte Konfiguration von KI-Agenten oder Konnektoren durch den Nutzer
- Verletzung von Rechten Dritter durch Aktionen des KI-Agenten (z.B. unbefugter Datenzugriff, unerwünschte E-Mail-Versendung)
- Verstöße gegen Nutzungsbedingungen von Drittdiensten durch den Nutzer oder den KI-Agenten
- Datenschutzverstöße, die auf einer rechtswidrigen Konfiguration des KI-Agenten durch den Nutzer beruhen

9.8.8. **Haftungsausschluss bei Kunden-MCP-Servern**
Der Anbieter übernimmt keine Haftung für Schäden, die durch den Betrieb, Fehler, Sicherheitslücken oder die unsachgemäße Implementierung von Kunden-MCP-Servern entstehen. Dies umfasst insbesondere:

- Schäden durch manipulative oder fehlerhafte Rückgabewerte des Kunden-MCP-Servers, die einen KI-Agenten zu unbeabsichtigten oder schädlichen Aktionen veranlassen
- Schäden durch unbefugten Datenzugriff auf Systeme, die über den Kunden-MCP-Server angebunden sind
- Schäden durch Prompt Injection-Angriffe, die über den Kunden-MCP-Server in den Agenten-Workflow eingeschleust werden
- Schäden durch die Integration von Drittanbieter-MCP-Servern, die Sicherheitslücken aufweisen oder schädliches Verhalten zeigen
- Datenschutzverstöße, die durch die über den Kunden-MCP-Server angebundenen Drittsysteme oder durch den Kunden-MCP-Server selbst verursacht werden

Der Nutzer stellt den Anbieter von allen Ansprüchen Dritter frei, die im Zusammenhang mit dem Betrieb oder der Integration von Kunden-MCP-Servern entstehen, insbesondere bei Ansprüchen wegen Datenschutzverstößen, Verletzung von Nutzungsbedingungen angebundener Drittsysteme oder Schäden durch sicherheitswidrige MCP-Server-Implementierungen.

9.8.9. **Haftung bei Anbieter-MCP-Servern**

Der Anbieter haftet bei Anbieter-MCP-Servern wie für sonstige Konnektor-Infrastruktur gemäß den Regelungen in §§ 9.3 und 9.4.

9.9 **Allgemeine Haftungshöchstgrenze**

9.9.1 Haftungsobergrenze für Auftragsverarbeitung und Vertragserfüllung: Soweit die Haftung des Anbieters nach dieser AGB der Höhe nach beschränkbar ist (insbesondere bei leichter Fahrlässigkeit im Sinne von §9.4), ist die Gesamthaftung des Anbieters je Schadensereignis und je Vertragsjahr auf das Zweifache (2-fache) des vom Kunden im betreffenden Vertragsjahr tatsächlich bezahlten Entgelts für das Grundabonnement (Brainy Agent Jahresabo) begrenzt.

9.9.2 Nicht von der Haftungsobergrenze erfasst: Die Haftungsbegrenzung nach §9.9.1 gilt ausdrücklich NICHT für folgende variable oder gesondert vereinbarte Leistungen:

- Coin-Käufe und daraus resultierende Verbrauchskosten (variable KI-Nutzungsentgelte)
- Schulungen, Workshops oder sonstige Trainingsleistungen
- Individuelle Integrationsleistungen und Implementierungsprojekte
- Connector-Einrichtungsgebühren und sonstige einmalige Setup-Leistungen
- Sonstige gesondert in Rechnung gestellte Sonderleistungen außerhalb des Grundabonnements

Für die vorstehenden Leistungen verbleibt es bei den allgemeinen gesetzlichen Haftungsregeln nach Maßgabe von §9.3 bis §9.6 dieser AGB.

9.9.3 **Berechnungsgrundlage Grundabonnement**:
Als Berechnungsgrundlage gilt das netto-jährliche Abonnemententgelt des vom Kunden gebuchten Brainy Agent-Pakets (Grundabonnement). Bei Monatsabonnements errechnet sich das Jahresentgelt als das Zwölffache (12-fache) der zum Zeitpunkt des Schadensereignisses geltenden monatlichen Netto-Paketgebühr. Nicht eingerechnet werden Coins, Zusatzmodule, Trainings, Integrationsleistungen oder sonstige variable Vergütungsbestandteile.

9.9.4 **Kumulationsregel**: Mehrere Schadensereignisse innerhalb eines Vertragsjahres werden für die Berechnung der Gesamtobergrenze zusammengezählt. Sobald das Zweifache des Jahres-Grundabonnements erreicht ist, entfällt eine weitere Haftung des Anbieters für leicht fahrlässig verursachte Schäden in diesem Vertragsjahr.

9.9.5 **Unberührtheit gesetzlicher Haftungsansprüche**: Die vorstehenden Haftungsgrenzen gelten nicht für Ansprüche aus der Verletzung des Lebens, des Körpers oder der Gesundheit, für vorsätzlich oder grob fahrlässig verursachte Schäden sowie für Ansprüche nach dem Produkthaftungsgesetz. Für diese Ansprüche haftet der Anbieter unbeschränkt gemäß §9.3.

10. Laufzeit und Kündigung

10.1 Die Vertragslaufzeit entspricht dem im jeweiligen Vertrag mit dem Nutzer genannten Abonnement-Zeitraum.

a. Monatsabonnements verlängern sich automatisch um jeweils einen (1) weiteren Monat, sofern der Vertrag nicht von einer Partei mit einer Frist von 14 Tagen vor Ablauf des jeweiligen Monatszeitraums gekündigt wird.
b. Jahresabonnements und sonstige Abonnements mit längerer Laufzeit verlängern sich automatisch um jeweils zwölf (12) weitere Monate, sofern der Vertrag nicht von einer Partei mit einer Frist von zwei (2) Monaten vor Ablauf der jeweils laufenden Vertragslaufzeit gekündigt wird.

10.2 Der Anbieter ist berechtigt, die Vergütung für die Paketgebühr für Folgezeiträume anzupassen. Eine Preisanpassung wird dem Nutzer mindestens 60 Tage vor Beginn des neuen Vertragszeitraums mitgeteilt. Widerspricht der Nutzer der Preisanpassung binnen 30 Tagen, steht beiden Parteien ein Sonderkündigungsrecht zum Ende des laufenden Vertragszeitraums zu.

10.3 Die Kündigung bedarf zu ihrer Wirksamkeit der Schriftform. Das Sonderkündigungsrecht bei langanhaltender höherer Gewalt gemäß § 13.7 bleibt unberührt.

10.4 Eine ordentliche Kündigung vor Ablauf der vereinbarten Mindestvertragslaufzeit ist ausgeschlossen. Das Kündigungsrecht zum Ende der Vertragslaufzeit gemäß Pkt. 10.1 sowie das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleiben unberührt.

Ein wichtiger Grund liegt insbesondere vor, wenn:

- der Nutzer trotz Mahnung und Nachfristsetzung mit Zahlungen in Verzug ist
- der Nutzer schwerwiegend oder wiederholt gegen seine Pflichten aus diesen AGB verstößt

10.5 Falls über das Vermögen des Nutzers ein Insolvenzverfahren eröffnet wird oder ein Antrag auf Einleitung eines Insolvenzverfahrens mangels hinreichenden Vermögens abgewiesen wird, ist der Anbieter berechtigt, ohne Setzung einer Nachfrist vom Vertrag zurückzutreten.

10.6 Nach Beendigung des Vertrags werden die Daten des Nutzers für 30 Tage zum Export bereitgestellt und anschließend gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Mit Beendigung des Vertrags werden auch alle aktiven Konnektoren binnen 72 Stunden deaktiviert. Der Nutzer ist dafür verantwortlich, die Zugriffsberechtigungen für Drittdienste nach Vertragsende selbst zu widerrufen.

11. Support und Wartung

11.1 Der Anbieter ist bestrebt, Anfragen und Probleme der Kunden zu klären. Unter office@latoo.at können Anfragen gestellt werden. Latoo.labs ist nicht verpflichtet, innerhalb von bestimmten Fristen zu antworten.

11.2 Wartungsarbeiten werden vorrangig außerhalb der üblichen Geschäftszeiten durchgeführt und nach Möglichkeit rechtzeitig angekündigt. Eine Ankündigungspflicht besteht außerhalb der üblichen Bürozeiten (Mo-Fr 7h bis 19h) nicht.

11.3 Sicherheitsvorfälle im Zusammenhang mit Agentic AI Funktionen oder Konnektoren soll der Nutzer unverzüglich unter security@latoo.at melden. Der Anbieter wird sicherheitsrelevante Vorfälle mit höchster Priorität behandeln.

12. Eigentum und Nutzungsrechte an verarbeiteten und generierten Daten

12.1 **Eigentum des Kunden**: Sämtliche vom Kunden eingegebenen Daten (Auftragsdaten, Dokumente, Spracheingaben, Konfigurationen) sowie alle durch die Brainy-Anwendung generierten Ausgaben, Protokolle, Transkriptionen, Dokumente und sonstigen Ergebnisse stehen im alleinigen Verfügungsrecht und wirtschaftlichen Eigentum des Kunden. Der Anbieter erwirbt durch die Verarbeitung keinerlei Eigentumsrechte an diesen Daten oder Ergebnissen.

12.2 **Verarbeitungsverbot für eigene Zwecke**: Der Anbieter darf Auftragsdaten nicht für andere Zwecke außerhalb der konkreten Leistungserbringung gemäß dieser AGB verwenden. Insbesondere ist es dem Anbieter ausdrücklich untersagt:

- Kundendaten zum Training oder zur Verbesserung eigener oder Drittanbieter-KI-Modelle zu verwenden
- Auftragsdaten für eigene Produktentwicklung oder Marktforschung zu nutzen
- Auftragsdaten an Dritte zu verkaufen, zu lizenzieren oder anderweitig zu übermitteln (außer im Rahmen der vertraglich genehmigten Unterauftragsverarbeitung)

12.3 **Klarstellung Konto- und Betriebsdaten**: Konto- und Vertragsdaten (z.B. E-Mail, Firmendaten, Zahlungsinformationen) sowie anonymisierte Betriebs- und Telemetriedaten (z.B. Systemlogs, Performance-Metriken ohne Personenbezug) sind keine Auftragsdaten im Sinne von §12.1. Für diese Daten gelten die Bestimmungen des Anbieters als Verantwortlicher gemäß Datenschutzerklärung.

12.4 **Datenrückgabe und Export**: Der Anbieter stellt dem Kunden auf Anfrage einen vollständigen Export aller Auftragsdaten in einem gängigen, maschinenlesbaren Format (JSON oder CSV) zur Verfügung. Der Export wird innerhalb von 30 Tagen nach schriftlicher Anforderung bereitgestellt.

12.5 **Löschung nach Vertragsende**: Nach Beendigung des Vertragsverhältnisses werden Auftragsdaten innerhalb von 30 Tagen datenschutzkonform gelöscht, sofern der Kunde nicht zuvor einen Export angefordert hat. Für Backup-Systeme gilt: Eine selektive Löschung in laufenden Sicherungen erfolgt nicht; Auftragsdaten werden mit Ablauf der regulären Backup-Rotationsfristen (spätestens 90 Tage nach Vertragsende) auch aus Sicherungen gelöscht.

13. Höhere Gewalt (Force Majeure)

13.1 Höhere Gewalt im Sinne dieser AGB bezeichnet außergewöhnliche, unvorhersehbare und vom Anbieter nicht beherrschbare Ereignisse, die trotz Anwendung zumutbarer Sorgfalt nicht verhindert oder in ihren Auswirkungen nicht abgewendet werden können. Hierzu zählen insbesondere:

a) Naturkatastrophen, Epidemien, Pandemien, Erdbeben, Überschwemmungen, Unwetter oder vergleichbare Naturereignisse
b) Krieg, Terroranschläge, Bürgerunruhen, Sabotage oder vergleichbare sicherheitsrelevante Ereignisse
c) Behördliche Anordnungen, Gesetzesänderungen, Embargos, Sanktionen oder sonstige hoheitliche Maßnahmen, die die Leistungserbringung unmittelbar beeinträchtigen
d) Großflächige Ausfälle öffentlicher Telekommunikationsnetze, des Internets oder der Energieversorgung, die nicht in der Sphäre des Anbieters liegen
e) Cyberangriffe, Distributed-Denial-of-Service-Angriffe (DDoS) oder vergleichbare Angriffe auf die Infrastruktur des Anbieters oder seiner wesentlichen Unterauftragnehmer, soweit der Anbieter dem Stand der Technik entsprechende Schutzmaßnahmen implementiert hat und diese den Angriff nicht verhindern konnten
f) Ausfall, wesentliche Leistungsstörung oder Einstellung des Dienstes eines kritischen Drittanbieters, insbesondere von Cloud-Infrastruktur-Anbietern (z.B. Hosting-Provider), KI-Modell-Anbietern (z.B. OpenAI, Anthropic, Mistral) oder der Konnektor-Infrastruktur (Nango Inc.), soweit der Anbieter keinen zumutbaren Alternativanbieter innerhalb angemessener Frist einsetzen kann
g) Streiks, Aussperrungen oder vergleichbare Arbeitskampfmaßnahmen, auch bei Unterauftragnehmern des Anbieters

13.2 **Rechtsfolgen bei vorübergehender Störung**

Wird der Anbieter durch ein Ereignis höherer Gewalt an der Erfüllung seiner vertraglichen Pflichten gehindert, so ruhen die betroffenen Leistungspflichten für die Dauer des Ereignisses und einer angemessenen Anlaufzeit danach. Der Anbieter gerät insoweit nicht in Verzug.

Schadensersatzansprüche des Nutzers wegen Nichterfüllung oder Schlechterfüllung sind für die Dauer des Force-Majeure-Ereignisses ausgeschlossen, soweit die Leistungsstörung unmittelbar und nachweislich auf das Ereignis zurückzuführen ist.

13.3 **Informationspflicht**

Der Anbieter wird den Nutzer unverzüglich nach Eintritt eines Force-Majeure-Ereignisses über die Art des Ereignisses, die voraussichtliche Dauer der Beeinträchtigung sowie die betroffenen Leistungen informieren. Ebenso wird der Anbieter den Nutzer unverzüglich über das Ende des Ereignisses und die Wiederaufnahme der betroffenen Leistungen informieren. Die Information erfolgt über die in der Anwendung hinterlegte E-Mail-Adresse des Administrators oder, bei Nichtverfügbarkeit der Anwendung, über die bei der Registrierung angegebene Kontaktadresse.

13.4 **Pflicht zur Schadensbegrenzung**

Der Anbieter ist auch während eines Force-Majeure-Ereignisses verpflichtet, alle zumutbaren Maßnahmen zu ergreifen, um die Auswirkungen des Ereignisses auf den Nutzer so gering wie möglich zu halten. Dies umfasst insbesondere:

a) den Einsatz alternativer Infrastrukturen oder Dienstleister, soweit dies technisch und wirtschaftlich zumutbar ist
b) die vorrangige Wiederherstellung der Kernfunktionalität der Anwendung vor erweiterten Funktionen
c) die sichere Beendigung oder Unterbrechung laufender Agenten-Workflows, um unkontrollierte Aktionen in Drittdiensten während des Ausfalls zu verhindern

13.5 **Besondere Regelungen für Agentic AI Funktionen**

Der Nutzer wird ausdrücklich darauf hingewiesen, dass ein Force-Majeure-Ereignis dazu führen kann, dass laufende KI-Agenten-Workflows unterbrochen werden, ohne dass eine ordnungsgemäße Beendigung oder Rückmeldung an den Nutzer möglich ist. Insbesondere kann es vorkommen, dass:

a) KI-Agenten während eines mehrstufigen Workflows gestoppt werden und der Workflow in einem inkonsistenten Zustand verbleibt (z.B. Teildaten verarbeitet, E-Mails teilweise versendet)
b) Konnektoren zu Drittdiensten unterbrochen werden und die Synchronisation von Daten zwischen Brainy und den Drittdiensten temporär gestört ist
c) Über MCP-Server angebundene Systeme nicht erreichbar sind und hieraus Folgewirkungen in den angebundenen Systemen entstehen

Der Anbieter übernimmt keine Haftung für Schäden, die aus der durch höhere Gewalt verursachten Unterbrechung von Agenten-Workflows, Konnektoren oder MCP-Server-Verbindungen entstehen, insbesondere nicht für inkonsistente Zustände in Drittdiensten oder unvollständig ausgeführte Aktionen. Der Nutzer ist verpflichtet, nach dem Ende eines Force-Majeure-Ereignisses die Ergebnisse unterbrochener Agenten-Workflows eigenständig zu überprüfen und gegebenenfalls korrigierende Maßnahmen in den betroffenen Drittdiensten vorzunehmen.

13.6 **Anpassung der Vergütung**

Dauert ein Force-Majeure-Ereignis länger als 7 aufeinanderfolgende Kalendertage an, so hat der Nutzer für den Zeitraum der vollständigen Nichtverfügbarkeit der Anwendung Anspruch auf eine anteilige Gutschrift der monatlichen Paketgebühr (berechnet auf Tagesbasis ab dem 8. Tag der Nichtverfügbarkeit). Die Gutschrift wird mit der nächsten regulären Rechnung verrechnet. Ein Anspruch auf Erstattung von Coins, die vor Eintritt des Ereignisses bereits verbraucht wurden, besteht

nicht. Coins, die aufgrund des Force-Majeure-Ereignisses nicht genutzt werden konnten, verfallen nicht vorzeitig; die Gültigkeitsdauer, der im betroffenen Abrechnungszeitraum zur Verfügung stehenden Coins verlängert sich um die Dauer des Ereignisses, maximal jedoch um 30 Tage.

13.7 **Sonderkündigungsrecht bei langanhaltender Störung**

Dauert ein Force-Majeure-Ereignis länger als 60 aufeinanderfolgende Kalendertage an oder ist absehbar, dass es mindestens 60 Tage andauern wird, so sind beide Parteien berechtigt, den Vertrag mit einer Frist von 14 Tagen zum Monatsende außerordentlich zu kündigen. In diesem Fall erstattet der Anbieter dem Nutzer die bereits im Voraus bezahlte Vergütung für den Zeitraum nach Wirksamwerden der Kündigung anteilig zurück. Weitergehende Schadensersatzansprüche des Nutzers aus der Kündigung sind ausgeschlossen. Das Recht des Nutzers, innerhalb von 30 Tagen nach Vertragsbeendigung einen Datenexport anzufordern (vgl. § 12.4), bleibt von der Kündigung unberührt, soweit dies technisch möglich ist.

13.8 **Keine Berufung bei Verschulden**

Die Berufung auf höhere Gewalt ist ausgeschlossen, soweit der Anbieter das Ereignis schuldhaft herbeigeführt hat oder soweit der Anbieter zumutbare und branchenübliche Vorkehrungen gegen das Eintreten des Ereignisses unterlassen hat. Insbesondere kann sich der Anbieter nicht auf den Ausfall eines KI-Modell-Anbieters oder Infrastrukturdienstleisters berufen, wenn der Ausfall auf einem vertragswidrigen Verhalten des Anbieters gegenüber diesem Dienstleister beruht.

14. AGB-Änderungen

Der Anbieter wird den Nutzer über Änderungen der AGB, des AVV oder der AI Act Compliance Notice beim nächsten Login informieren. Die geänderten Bestimmungen werden dem Nutzer vollständig angezeigt. Eine weitere Nutzung der Anwendung ist nur nach aktiver Zustimmung zu den geänderten Bestimmungen durch Anklicken einer entsprechenden Schaltfläche („Ich stimme den neuen AGB / AVV zu") möglich.

Der Anbieter ist bestrebt, wesentliche Änderungen mindestens 14 Tage vor Inkrafttreten per E-Mail an die hinterlegte Administratoren-Adresse anzukündigen. Eine Verpflichtung zur Vorankündigung besteht nicht bei Änderungen, die zur Einhaltung zwingender gesetzlicher oder behördlicher Vorgaben kurzfristig erforderlich sind.

Verweigert der Nutzer die Zustimmung, gilt dies als außerordentliche Kündigung des Nutzungsvertrages durch den Nutzer zum Zeitpunkt der Verweigerung. Regulatorisch bedingte AGB-Änderungen (insbesondere AI-Act-Compliance, neue Bestimmungen im Rahmen von Agentic AI) lösen kein Recht auf anteilige Erstattung bereits bezahlter Gebühren oder Schadensersatz aus.

Nach Zustimmung sind die AGB und der AVV jederzeit im Profil des Benutzers einsehbar.

15. Schlussbestimmungen

15.1 Auf diese Nutzungsbedingungen findet österreichisches Recht Anwendung. Die Anwendung des UN-Kaufrechts (CISG) sowie der Kollisionsregelungen des internationalen Privatrechts ist ausgeschlossen.

15.2 Ausschließlich zuständig für alle sich aus oder im Zusammenhang mit der Nutzung der Anwendung oder mit den gegenständlichen Nutzungsbedingungen zwischen dem Anbieter und dem Nutzer ergebenden Streitigkeiten ist das sachlich zuständige Gericht am Sitz des Anbieters, soweit nicht ein anderes Gericht aufgrund zwingender gesetzlicher Bestimmungen zuständig ist.

15.3 Änderungen und Ergänzungen dieser AGB bedürfen der Textform. Dies gilt auch für die Änderung dieser Formklausel.

15.4 Sollten einzelne Bestimmungen dieser AGB unwirksam sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hiervon nicht berührt. Anstelle der unwirksamen Bestimmung gilt diejenige wirksame Bestimmung als vereinbart, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.