AI ACT Compliance Notice

Stand: 13. April 2026

Herausgeber:

Latoo.labs GmbH
Kraußstr. 16
4020 Linz
Österreich

FN 565855s

im Folgenden: "***AI-System-Anbieter (Provider)***" oder „**Anbieter**“ -

1. Anwendungsbereich und Zweck

1.1 Gegenstand

Dieses Dokument konkretisiert die Anforderungen der Verordnung (EU) 2024/1689 über Künstliche Intelligenz (AI Act) für die Bereitstellung und Nutzung der Brainy-Anwendung, einschließlich aller Agentic AI Funktionen, Konnektoren und MCP-Server-Integrationen.

1.2 Verhältnis zu anderen Vereinbarungen

Diese AI Act Compliance Notice ergänzt:

- Die Allgemeinen Geschäftsbedingungen (AGB) bzw. den Hauptvertrag
- Den Auftragsverarbeitungsvertrag (AVV) – soweit personenbezogene Daten verarbeitet werden

Bei Widersprüchen: In Fragen der AI-Act-Compliance hat dieses Dokument Vorrang vor allgemeinen Bestimmungen in AGB oder AVV. Diese Vorrangregel ist spiegelbildlich in § 4 der AGB verankert.

1.3 Anwendbarkeit

Diese Notice gilt unabhängig davon, ob:

- Personenbezogene Daten verarbeitet werden (der AI Act gilt auch für nicht-personenbezogene Daten)
- Eine AVV geschlossen wurde
- Der Kunde als Unternehmen, Behörde oder sonstige Einrichtung agiert
- Der Kunde ausschließlich klassische Assistenzfunktionen oder auch Agentic AI Funktionen nutzt

1.4 Begriffsgleichsetzung

Der in den AGB als „Nutzer" bezeichnete Vertragspartner ist im Sinne des AI Acts der „Betreiber" (Deployer) und im Sinne der DSGVO der „Verantwortliche". In dieser Compliance Notice wird einheitlich der Begriff „Betreiber" verwendet.

1.5 Versionierung und Aktualisierung

Diese AI Act Compliance Notice wird bei Bedarf aktualisiert, insbesondere bei:

- Änderungen des regulatorischen Rahmens (neue Durchführungsrechtsakte, Leitlinien, delegierte Rechtsakte)
- Wesentlichen Änderungen der Brainy-Anwendung, insbesondere bei Einführung neuer KI-Funktionen oder Änderung der eingesetzten KI-Modelle
- Neuen Erkenntnissen aus der Marktüberwachung oder behördlichen Leitlinien

Der Anbieter informiert den Betreiber über wesentliche Aktualisierungen. Die jeweils aktuelle Fassung ist im Profil des Benutzers abrufbar und wird dem Betreiber auf Anfrage zugesandt. Die Versionsnummer und das Datum der Fassung sind auf der ersten Seite ausgewiesen.

2. Definitionen und Rollenzuweisung

2.1 Rollenzuweisung im Sinne des AI Acts

2.1.1 Im Sinne des EU AI Acts sind:

- „AI-System-Anbieter" (Provider): Latoo.labs GmbH als Entwickler und Bereitsteller der Brainy-Anwendung, einschließlich der Agentic AI Infrastruktur, der Anbieter-MCP-Server und der Konnektor-Plattform
- „AI-System-Betreiber" (Deployer): Der Vertragspartner (in den AGB als „Nutzer" bezeichnet) als Verwender der Brainy-Anwendung für eigene Geschäftszwecke
- „Betroffene Personen": Natürliche Personen, deren Daten durch die KI-Systeme verarbeitet werden oder die mit KI-Agenten interagieren (z.B. Empfänger von durch KI-Agenten versendeten E-Mails)
- „GPAI-Modell-Anbieter": Die Anbieter der in § 5 genannten KI-Modelle (z.B. OpenAI, Anthropic, Google, Mistral AI), die General Purpose AI Models (GPAI) bereitstellen

2.1.2 Abgrenzung der Verantwortung:

Der Anbieter stellt die Brainy-Anwendung als Allzweck-KI-Werkzeug bereit. Art, Umfang und Zweck der konkreten Nutzung werden ausschließlich durch den Betreiber bestimmt. Der Betreiber entscheidet eigenständig über:

- Welche Daten in die Anwendung eingegeben werden
- Welche KI-Modelle für welche Anwendungsfälle eingesetzt werden
- Welche KI-Agenten konfiguriert und mit welchen Berechtigungen ausgestattet werden
- Welche Drittdienste über Konnektoren oder MCP-Server angebunden werden
- Welche autonomen Aktionen KI-Agenten in Drittdiensten ausführen dürfen

2.2 Risikoklassifizierung

2.2.1 Standard-Anwendungsfälle (begrenztes Risiko):

Die Brainy-Anwendung wird für die vorgesehenen Standard-Anwendungsfälle (Transkription, Dokumentenerstellung, Zusammenfassungen, Formulierungshilfen, Übersetzungen, Bildgenerierung, administrative Dokumentation) als KI-System mit begrenztem Risiko gemäß Art. 50 AI Act eingestuft. In diesem Rahmen treffen den Anbieter Transparenzpflichten gemäß Art. 50 AI Act.

2.2.2 Agentic AI Funktionen (erhöhtes Risikoprofil):

Die Agentic AI Funktionen der Brainy-Anwendung (KI-Agenten, Konnektoren, MCP-Server, automatisierte Workflows) haben ein grundsätzlich höheres Risikoprofil als die Standard-Assistenzfunktionen, da:

- KI-Agenten eigenständig Entscheidungen treffen und Aktionen außerhalb der Anwendung ausführen
- Autonome Aktionen in Drittdiensten reale und potenziell irreversible Folgen haben (z.B. Versenden von E-Mails, Löschen von Dateien)
- Automatisierte Workflows ohne unmittelbare menschliche Kontrolle ablaufen können
- Prompt Injection-Risiken bei der Verarbeitung externer Daten bestehen

Der Anbieter stuft die Agentic AI Funktionen bei bestimmungsgemäßer Verwendung (vgl. Anhang A) weiterhin als System mit begrenztem Risiko ein. Diese Einstufung setzt voraus, dass der Betreiber die in den AGB (§ 6.8) festgelegten Konfigurations-, Sicherheits- und Überwachungspflichten einhält und die Agentic AI Funktionen nicht für Hochrisiko-Anwendungsfälle einsetzt.

2.2.3 Hochrisiko-Anwendungsfälle:

Sollte der Betreiber eine Nutzung beabsichtigen, die das System in eine Hochrisiko-Anwendung gemäß Anhang III des AI Acts überführt (z.B. Einsatz im Personalwesen für Bewerberbewertung, im Bildungswesen für Prüfungsbewertung, in der Strafverfolgung), ist er verpflichtet, den Anbieter hierüber vorab schriftlich zu informieren. Der Anbieter behält sich vor, bei Hochrisiko-Nutzung zusätzliche technische oder organisatorische Maßnahmen zu verlangen oder die Nutzung einzuschränken.

2.2.4 Wechsel der Risikoklasse durch Betreiber:

Der Betreiber wird darauf hingewiesen, dass die Risikoklassifizierung von der konkreten Verwendung abhängt. Nutzt der Betreiber die Brainy-Anwendung – einschließlich der Agentic AI Funktionen – in einem Kontext, der in Anhang III des AI Acts aufgeführt ist, trägt er als Betreiber die Pflichten eines Hochrisiko-System-Betreibers gemäß Art. 26 AI Act, unabhängig von der Einstufung durch den Anbieter.

3. Pflichten des AI-System-Anbieters (Latoo.labs)

3.1 Allgemeine Anbieterpflichten

Der Anbieter verpflichtet sich zur Erfüllung folgender Pflichten:

- Bereitstellung technischer Dokumentation und Informationen über die KI-Systeme, einschließlich der Agentic AI Architektur, auf Anfrage des Betreibers – insbesondere für Konformitätsbewertungen, DPIAs oder FRIAs
- Sicherstellung der Cybersicherheit des KI-Systems gemäß dem Stand der Technik
- Information des Betreibers über wesentliche Änderungen am KI-System (insbesondere neue KI-Modelle, neue Agentenfähigkeiten, Änderungen an Konnektoren)
- Bereitstellung von Informationen für Konformitätsbewertungen, soweit angefordert
- Führung von Aufzeichnungen über schwerwiegende Vorfälle gemäß Art. 73 AI Act

3.2 Transparenzpflichten (Art. 50 AI Act)

3.2.1 Allgemeine Transparenz:

- Kennzeichnung KI-generierter Inhalte, soweit technisch möglich und vom Anbieter umsetzbar
- Information über die Funktionsweise der verwendeten KI-Modelle in der Produktdokumentation
- Bereitstellung verständlicher Nutzungsanleitungen
- Hinweise auf Grenzen und mögliche Risiken des KI-Systems
- Bereitstellung dieser AI Act Compliance Notice als zusammenfassendes Transparenzdokument

3.2.2 Transparenz bei Agentic AI Funktionen:

Der Anbieter stellt für die Agentic AI Funktionen folgende zusätzliche Transparenzmaßnahmen bereit:

- Klare Dokumentation der verfügbaren Agentenfähigkeiten und der durch Konnektoren/MCP-Server möglichen Aktionen
- Protokollierung aller von KI-Agenten ausgeführten Aktionen (Action Logging), die dem Betreiber über die Anwendung zugänglich ist
- In-App-Bestätigungen (vgl. AGB § 6.9), die den Nutzer über die spezifischen Risiken der Agentic AI Funktionen aufklären, bevor er diese erstmalig verwendet
- In-App-Bestätigungen bei der erstmaligen Aktivierung von MCP-Tools mit schreibender, löschender oder kommunizierender Funktion (AGB § 6.9.2 lit. d), die den Nutzer über die spezifischen Risiken des Tools – einschließlich des Prompt Injection-Risikos und der Irreversibilität bestimmter Aktionen – aufklären
- Bereitstellung von Konfigurationsmöglichkeiten zur Kennzeichnung KI-generierter Kommunikation (z.B. automatische Signatur-Ergänzung bei durch KI-Agenten versendeten E-Mails)

3.2.3 Hinweis zur Kennzeichnung bei autonomer Kommunikation:

Gemäß Art. 50 Abs. 1 AI Act müssen natürliche Personen darüber informiert werden, dass sie mit einem KI-System interagieren, es sei denn, dies ist aus den Umständen offensichtlich. Die konkrete Umsetzung dieser Kennzeichnungspflicht bei durch KI-Agenten automatisch versendeten Nachrichten, E-Mails oder Dokumenten obliegt dem Betreiber. Der Anbieter stellt hierfür technische Unterstützung bereit (z.B. konfigurierbare KI-Kennzeichnungsoptionen), kann die Verantwortung für die inhaltliche Umsetzung jedoch nicht übernehmen.

3.3 Pflichten im Zusammenhang mit GPAI-Modellen (Art. 53 AI Act)

Die Brainy-Anwendung setzt General Purpose AI Models (GPAI) von Drittanbietern ein (vgl. § 5). Im Rahmen der Lieferkette verpflichtet sich der Anbieter:

- Sicherzustellen, dass die GPAI-Modell-Anbieter die ihnen nach Art. 53 AI Act obliegenden Informationspflichten erfüllen, soweit dies im Rahmen der vertraglichen Beziehungen des Anbieters mit den GPAI-Anbietern durchsetzbar ist

- Technische Dokumentation und Modellinformationen der eingesetzten GPAI-Modelle dem Betreiber auf Anfrage in dem Umfang bereitzustellen, in dem sie vom GPAI-Modell-Anbieter zur Verfügung gestellt wurden
- Den Betreiber zu informieren, wenn ein GPAI-Modell-Anbieter als Anbieter eines GPAI-Modells mit systemischem Risiko (Art. 51 AI Act) eingestuft wird und dies Auswirkungen auf die Nutzung der Brainy-Anwendung haben kann

3.4 Pflichten bei Hochrisiko-Systemen

Sollte die Brainy-Anwendung oder ein Teil davon aufgrund einer behördlichen Entscheidung oder aufgrund der konkreten Nutzung durch den Betreiber als Hochrisiko-System eingestuft werden, verpflichtet sich der Anbieter zusätzlich zu:

- Implementierung eines Risikomanagement-Systems gemäß Art. 9 AI Act
- Gewährleistung angemessener Datenqualität gemäß Art. 10 AI Act
- Führung detaillierter Protokolle (Logging) gemäß Art. 12 AI Act
- Sicherstellung technischer Voraussetzungen für menschliche Aufsicht gemäß Art. 14 AI Act
- Gewährleistung von Genauigkeit, Robustheit und Cybersicherheit gemäß Art. 15 AI Act
- Erstellung und Pflege der technischen Dokumentation gemäß Art. 11 AI Act

3.5 Sicherheitsmaßnahmen des Anbieters für Agentic AI

Der Anbieter implementiert für die Agentic AI Funktionen folgende Sicherheitsmaßnahmen:

- Action Logging: Alle von KI-Agenten ausgeführten Aktionen werden protokolliert und dem Betreiber zugänglich gemacht
- Coin-Verbrauchskontrolle: Automatischer Stopp von Agenten-Workflows bei Erschöpfung des Coin-Kontingents
- Konnektor-Sicherheit: Verwaltung der Konnektor-Infrastruktur über einen spezialisierten Drittanbieter (Nango Inc.) mit entsprechenden Sicherheitsvereinbarungen
- Anbieter-MCP-Server: Implementierung und Betrieb der Anbieter-MCP-Server nach dem Stand der Technik mit Transportverschlüsselung, Authentifizierung und Zugriffskontrolle
- MCP-Tool Default-Off: Sämtliche MCP-Tools (Werkzeuge) eines MCP-Servers sind standardmäßig deaktiviert. Ein KI-Agent kann ein Tool erst nutzen, nachdem der Betreiber oder ein autorisierter Administrator das Tool explizit aktiviert hat. Jede Aktivierung und Deaktivierung wird revisionssicher protokolliert. Diese Maßnahme dient sowohl dem Datenschutz (Art. 25 Abs. 2 DSGVO) als auch der menschlichen Aufsicht (Art. 14 AI Act), da der Betreiber bewusst und granular entscheidet, welche Fähigkeiten einem KI-Agenten zur Verfügung stehen.

4. Pflichten des AI-System-Betreibers (Kunde)

Der Betreiber ist für die Einhaltung der ihn betreffenden Pflichten verantwortlich. Diese richten sich nach der Risikoklasse des konkreten Anwendungsfalls.

4.1 Pflichten bei Nutzung als System mit begrenztem Risiko (Standardfall)

Bei der regulären Nutzung ist der Betreiber insbesondere verpflichtet:

a) Das KI-System bestimmungsgemäß und gemäß der bereitgestellten Dokumentation zu verwenden (vgl. Anhang A)
b) Sicherzustellen, dass die Nutzer über ein ausreichendes Maß an KI-Kompetenz im Sinne von Art. 4 AI Act verfügen. Dies umfasst insbesondere das Verständnis der Funktionsweise von KI-Modellen, der Grenzen KI-generierter Inhalte sowie – bei Nutzung von Agentic AI Funktionen – der Funktionsweise autonomer KI-Agenten, der damit verbundenen Risiken und der Überwachungspflichten
c) Die in-App-Bestätigungen (AGB § 6.9) als Instrument zur Sicherstellung der KI-Kompetenz einzelner Nutzer zu nutzen
d) Personen, die mit dem KI-System interagieren, darüber zu informieren (Art. 50 Abs. 1 AI Act). Bei Agentic AI umfasst dies insbesondere die Kennzeichnung von durch KI-Agenten automatisch versendeten Nachrichten und E-Mails

4.2 Zusätzliche Pflichten bei Nutzung von Agentic AI Funktionen

Der Betreiber, der Agentic AI Funktionen aktiviert und nutzt, trägt über die allgemeinen Betreiberpflichten hinaus folgende AI-Act-relevante Verantwortung:

4.2.1 Menschliche Aufsicht:

Der Betreiber stellt sicher, dass KI-Agenten einer angemessenen menschlichen Aufsicht unterliegen. Die Intensität der Aufsicht richtet sich nach dem Risikopotenzial der konfigurierten Aktionen:

Risikoniveau	Beispielaktionen	Mindestanforderung an Aufsicht
Lesezugriff	E-Mails lesen, Dateien analysieren, Daten abrufen	Regelmäßige Prüfung der Protokolldateien
Schreibzugriff (intern)	Dateien in Unternehmens-Speicher erstellen/ändern, CRM-Einträge aktualisieren	Regelmäßige Prüfung; stichprobenartige Kontrolle der Ergebnisse
Schreibzugriff (extern)	E-Mails an Dritte versenden, Nachrichten in Kommunikationsplattformen posten	Genehmigungsworkflow oder zeitnahe Nachkontrolle empfohlen
Löschzugriff	Dateien löschen, Einträge entfernen	Genehmigungsworkflow dringend empfohlen
Automatisierte Trigger	Zeitgesteuerte oder ereignisbasierte Workflow-Ausführung	Regelmäßige Überwachung; Verbrauchskontrolle

Die granulare MCP-Tool-Steuerung (Default-Off) ist ein zusätzliches Instrument der menschlichen Aufsicht im Sinne von Art. 14 AI Act. Durch die gezielte Aktivierung einzelner Tools bestimmt der Betreiber den Aktionsrahmen des KI-Agenten vor dessen Einsatz. Der Anbieter empfiehlt:

- Für Tools mit Lesezugriff: Aktivierung nach Prüfung des Datenumfangs
- Für Tools mit Schreib-/Lösch-/Kommunikationszugriff: Aktivierung nur in Kombination mit Human-in-the-Loop-Genehmigungsworkflow
- Regelmäßige Überprüfung der aktivierten Tools und Deaktivierung nicht mehr benötigter Tools

Der Betreiber ist verpflichtet, die Konfiguration seiner KI-Agenten so auszugestalten, dass die menschliche Aufsicht den oben genannten Mindestanforderungen genügt. Die detaillierten Konfigurations- und Überwachungspflichten ergeben sich aus § 6.8 der AGB.

4.2.2 KI-Kompetenz für Agentic AI:

Die Nutzung von Agentic AI Funktionen erfordert ein erweitertes Maß an KI-Kompetenz im Sinne von Art. 4 AI Act. Der Betreiber stellt sicher, dass Personen, die KI-Agenten konfigurieren, über folgende Kenntnisse verfügen:

- Verständnis der Funktionsweise autonomer KI-Agenten und des Konzepts von Tool-Use
- Verständnis der granularen MCP-Tool-Steuerung (Default-Off-Prinzip, Risikokategorien lesend/schreibend/löschend/kommunizierend) und der Fähigkeit, Tool-Beschreibungen – insbesondere bei Kunden-MCP-Servern – eigenständig auf Richtigkeit und Vollständigkeit zu prüfen
- Verständnis des Prinzips der minimalen Rechtevergabe (Least Privilege) bei Konnektoren
- Kenntnis der Risiken von Prompt Injection und geeigneter Schutzmaßnahmen
- Fähigkeit zur Auswertung von Agenten-Protokollen
- Verständnis der Auswirkungen autonomer Aktionen auf verbundene Drittdienste

4.2.3 Transparenz gegenüber Betroffenen bei Agentic AI:

Der Betreiber ist verpflichtet, natürliche Personen, die von den Aktionen eines KI-Agenten betroffen sind, über die KI-Beteiligung zu informieren. Dies umfasst insbesondere:

- Empfänger von durch KI-Agenten automatisch erstellten oder versendeten E-Mails, Nachrichten oder Dokumenten
- Personen, deren Daten durch KI-Agenten in Drittdiensten verarbeitet, geändert oder gelöscht werden
- Personen, die mit KI-Agenten über Kommunikationsplattformen interagieren

Der Anbieter stellt hierfür technische Unterstützung bereit (vgl. § 3.2.2). Die inhaltliche und organisatorische Umsetzung der Informationspflicht obliegt dem Betreiber.

4.2.4 Risikobewertung bei Agentic AI:

Vor der Inbetriebnahme von KI-Agenten mit Schreibzugriff auf Drittdienste empfiehlt der Anbieter dem Betreiber die Durchführung einer internen Risikobewertung, die mindestens folgende Aspekte umfasst:

- Welche Daten kann der KI-Agent lesen und verarbeiten?
- Welche Aktionen kann der KI-Agent autonom ausführen?
- Welche Auswirkungen hätte eine fehlerhafte Aktion (z.B. falsche E-Mail, gelöschte Datei)?
- Sind die erteilten Berechtigungen auf das erforderliche Minimum beschränkt?
- Welche Kontrollmechanismen sind implementiert?
- Besteht ein Prompt Injection-Risiko durch externe Datenquellen?

4.3 Zusätzliche Pflichten bei Nutzung als Hochrisiko-System

Sollte der Anwendungsfall des Betreibers als Hochrisiko-System eingestuft werden, treffen ihn die weitergehenden gesetzlichen Pflichten des Art. 26 AI Act. Dazu zählen insbesondere:

a) Die Sicherstellung einer angemessenen menschlichen Aufsicht gemäß Art. 14 AI Act, die über die in § 4.2.1 genannten Mindestanforderungen hinausgehen kann

b) Die Überwachung des Systems und die Führung von Protokollen (Logging), soweit vom System technisch bereitgestellt

c) Die Durchführung einer Grundrechte-Folgenabschätzung (FRIA) vor der Inbetriebnahme, falls zutreffend (Art. 27 AI Act)

d) Die Erfüllung eventueller Registrierungspflichten in der EU-Datenbank (Art. 49 AI Act)

e) Die Information der Beschäftigtenvertretung über den Einsatz von Hochrisiko-KI-Systemen am Arbeitsplatz (Art. 26 Abs. 7 AI Act)

4.4 Datenschutz-Folgenabschätzung (DPIA)

Der Betreiber wird darauf hingewiesen, dass die Nutzung der Brainy-Anwendung – insbesondere der 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 Betreiber als Verantwortlichem im Sinne der DSGVO. Der Anbieter unterstützt den Betreiber auf Anfrage durch Bereitstellung der notwendigen technischen Informationen.

5. Eingesetzte KI-Modelle

5.1 EU-gehostete Modelle (empfohlen für sensible Daten)

Modell/Plattform	Anbieter	Hosting-Standort
Azure OpenAI (Regional / Data Zone)	Microsoft Ireland Operations Ltd.	EU (Schweden / Frankreich)
AWS Bedrock	Amazon EMEA SARL	EU/Luxemburg
Google Vertex AI	Google Ireland Limited	EU/Irland
Flux	BFL GmbH	EU/Deutschland

5.1a DSGVO-konforme Modelle mit teilweiser Drittlandverarbeitung

Modell/Plattform	Anbieter	Speicherung	Verarbeitung
Azure OpenAI	Microsoft Ireland Operations Ltd.	EU	Global (inkl. USA)

Bei diesen Modellen erfolgt die dauerhafte Speicherung in der EU. Die Inference-Verarbeitung kann auch außerhalb der EU stattfinden. Es bestehen EU-Standardvertragsklauseln, ein Transfer Impact

Assessment und zusätzliche technische Schutzmaßnahmen. Nutzung nur auf dokumentierte Weisung des Betreibers.

5.2 Nicht-EU-Modelle (nur auf ausdrückliche Anweisung des Betreibers)

Modell/Plattform	Anbieter	Hosting-Standort
OpenAI API	OpenAI, L.L.C.	USA
Anthropic API	Anthropic PBC	USA
Google AI (Gemini)	Google LLC	USA
xAI (Grok)	X.AI LLC	USA
Perplexity AI	Perplexity AI, Inc.	USA
Black Forest Labs	Black Forest Labs, Inc.	USA

5.3 Hinweise zur Modellauswahl

- Die Auswahl des KI-Modells obliegt dem Betreiber. In der Anwendung werden KI-Modelle in drei Kategorien gekennzeichnet: „EU" (vollständige Verarbeitung in der EU), „DSGVO" (Speicherung in der EU, Inference-Verarbeitung ggf. auch außerhalb der EU, mit EU-Standardvertragsklauseln und zusätzlichen Schutzmaßnahmen) und „Weltweit“ (derzeit Verarbeitung und Speicherung in den USA).
- Der Anbieter empfiehlt, für sensible oder personenbezogene Daten sowie für Agentic AI Anwendungen, bei denen potenziell sensible externe Daten verarbeitet werden, ausschließlich EU-gehostete KI-Modelle zu verwenden. Standardmäßig stehen dem Betreiber alle Modell-Kategorien zur Verfügung; der Betreiber kann die zulässigen Kategorien jederzeit mandantenweit einschränken (vgl. AGB § 4.5.4)
- Bei der Auswahl eines Nicht-EU-Modells wird der Nutzer über eine In-App-Bestätigung (AGB § 6.9.2) auf die damit verbundenen Risiken hingewiesen
- Für Drittlandtransfers an Nicht-EU-Modelle werden, soweit verfügbar, Standardvertragsklauseln (SCC) gemäß Art. 46 Abs. 2 lit. c DSGVO oder Angemessenheitsbeschlüsse gemäß Art. 45 DSGVO als Rechtsgrundlage herangezogen

5.4 GPAI-Eigenschaft der eingesetzten Modelle

Die in § 5.1 und § 5.2 genannten KI-Modelle sind als General Purpose AI Models (GPAI) im Sinne von Art. 51 ff. AI Act einzuordnen. Der Anbieter stellt sicher, dass die Informationen, die von den GPAI-Modell-Anbietern gemäß Art. 53 AI Act bereitgestellt werden, in die Produktdokumentation einfließen und dem Betreiber auf Anfrage zugänglich gemacht werden.

5.5 Änderungen an eingesetzten Modellen

Der Anbieter behält sich vor, die Liste der verfügbaren KI-Modelle zu erweitern, zu ändern oder einzelne Modelle zu entfernen. Wesentliche Änderungen (insbesondere das Entfernen von Modellen

oder der Wechsel des GPAI-Anbieters) werden dem Betreiber mindestens 14 Tage vor Umsetzung angekündigt, soweit dies nicht aus Sicherheitsgründen sofort erforderlich ist.

6. Verbotene KI-Praktiken (Art. 5 AI Act)

6.1 Absolutes Nutzungsverbot

Die Nutzung der Brainy-Anwendung – einschließlich aller Agentic AI Funktionen, Konnektoren und MCP-Server – für KI-Praktiken, die gemäß Art. 5 der Verordnung (EU) 2024/1689 verboten sind, ist ausdrücklich untersagt. Dies umfasst insbesondere:

a) **Unterschwellige Beeinflussung**: Den Einsatz der Anwendung oder ihrer KI-Agenten, um das Verhalten natürlicher Personen durch unterschwellige Techniken, die von diesen Personen nicht bewusst wahrgenommen werden können, wesentlich zu beeinflussen, sodass diesen Personen oder Dritten ein erheblicher Schaden zugefügt wird oder zugefügt werden könnte
b) **Ausnutzung von Schwächen**: Den Einsatz der Anwendung, um Schwächen natürlicher Personen aufgrund ihres Alters, einer Behinderung oder einer besonderen sozialen oder wirtschaftlichen Lage auszunutzen, mit dem Ziel, das Verhalten dieser Personen wesentlich zu beeinflussen
c) **Social Scoring**: Die Bewertung oder Klassifizierung natürlicher Personen auf der Grundlage ihres Sozialverhaltens oder persönlicher Eigenschaften, wenn die resultierende soziale Bewertung zu einer ungerechtfertigten oder unverhältnismäßigen Schlechterstellung führt
d) **Biometrische Echtzeit-Identifizierung**: Die Nutzung der Anwendung für die biometrische Echtzeit-Fernidentifizierung natürlicher Personen in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken
e) **Prädiktives Policing**: Die Bewertung oder Vorhersage des Risikos, dass eine natürliche Person eine Straftat begeht, ausschließlich auf der Grundlage von Profiling oder Persönlichkeitsmerkmalen
f) **Ungezieltes Auslesen von Gesichtsbildern**: Das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder aus Videoüberwachungsaufnahmen zur Erstellung oder Erweiterung von Gesichtserkennungsdatenbanken
g) **Biometrische Kategorisierung**: Die Verwendung von KI-Systemen zur biometrischen Kategorisierung, die einzelne natürliche Personen auf Grundlage ihrer biometrischen Daten kategorisiert, um deren Rasse, politische Meinungen, Gewerkschaftszugehörigkeit, religiöse oder weltanschauliche Überzeugungen, Sexualleben oder sexuelle Orientierung abzuleiten. Dies gilt nicht für rechtmäßig erworbene biometrische Datensätze, die im Bereich der Strafverfolgung gekennzeichnet werden.
h) **Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen**: Die Ableitung von Emotionen natürlicher Personen am Arbeitsplatz oder in Bildungseinrichtungen, es sei denn, dies ist aus medizinischen oder sicherheitstechnischen Gründen erforderlich

6.2 Besondere Relevanz bei Agentic AI

Der Betreiber wird darauf hingewiesen, dass die verbotenen Praktiken auch durch die mittelbare Nutzung über KI-Agenten verwirklicht werden können. Insbesondere ist es untersagt, KI-Agenten so zu konfigurieren, dass diese über Konnektoren oder MCP-Server auf Daten zugreifen und diese in einer Weise verarbeiten, die einer verbotenen Praktik entspricht.

---

7. Spezielle Bestimmungen nach Anwendungsbereich

7.1 Gesundheitswesen

Bei Nutzung im Gesundheitswesen gelten zusätzlich:

- Einhaltung der Medical Device Regulation (MDR), soweit anwendbar
- Besondere Sorgfalt bei Diagnose- oder Behandlungsentscheidungen
- Dokumentation der KI-Unterstützung in Patientenakten
- Aufklärung von Patienten über KI-Nutzung

WICHTIGE KLARSTELLUNG:

Die Brainy-Anwendung ist NICHT als Medizinprodukt gemäß Medical Device Regulation (MDR) zertifiziert. Eine Nutzung für medizinische Zweckbestimmungen (Diagnose, Therapie, Risikoeinschätzung von Patienten) ist NICHT zulässig und verstößt gegen die bestimmungsgemäße Verwendung. Dies gilt auch für den Einsatz von KI-Agenten im medizinischen Kontext.

Die Nutzung für rein administrative Dokumentation im Gesundheitswesen (z.B. Transkription von Gesprächen, Erstellung von Arztbriefen auf Basis diktierter Inhalte) ist zulässig, soweit keine medizinische Zweckbestimmung vorliegt.

7.2 Rechtswesen

Bei Nutzung im Rechtswesen gelten zusätzlich:

- Wahrung anwaltlicher Unabhängigkeit trotz KI-Unterstützung
- Kennzeichnung KI-unterstützter Dokumente, soweit beruflich erforderlich
- Besondere Sorgfalt bei rechtlichen Bewertungen und Empfehlungen
- Bei Nutzung von Agentic AI: Sicherstellung, dass KI-Agenten keine eigenständigen Rechtsberatungshandlungen vornehmen

7.3 Personalwesen

Bei Nutzung im Personalwesen gelten zusätzlich:

- Transparenz gegenüber Bewerbern und Mitarbeitern über KI-Nutzung
- Vermeidung diskriminierender KI-Entscheidungen
- Sicherstellung fairer Verfahren bei KI-Unterstützung
- Bei Nutzung von Agentic AI: Kein Einsatz von KI-Agenten für automatisierte Personalentscheidungen (Einstellung, Kündigung, Beförderung, Leistungsbewertung) ohne ausreichende menschliche Aufsicht und individuelle Prüfung. Der Einsatz von KI-Agenten im Personalwesen kann eine Hochrisiko-Einstufung gemäß Anhang III Nr. 4 AI Act begründen

7.4 Finanzwesen

Bei Nutzung im Finanzwesen gelten zusätzlich:

- Kein Einsatz von KI-Agenten für autonome Kreditwürdigkeitsprüfungen natürlicher Personen (Anhang III Nr. 5 lit. b AI Act – Hochrisiko)
- Besondere Sorgfalt bei KI-unterstützter Finanzanalyse und -berichterstattung
- Sicherstellung der Nachvollziehbarkeit KI-gestützter Entscheidungen

8. Meldung schwerwiegender Vorfälle

8.1 Definition schwerwiegender Vorfall

Ein schwerwiegender Vorfall im Sinne des Art. 73 AI Act liegt insbesondere vor bei:

Allgemeine Vorfälle:

- Systemausfall mit Datenverlust
- Unbefugtem Zugriff auf Kundendaten
- Fehlfunktionen mit Schadensrisiko
- Verletzung von Grundrechten durch das KI-System

Agentic-AI-spezifische Vorfälle:

- Unkontrollierte autonome Aktionen eines KI-Agenten, die zu erheblichen Schäden in Drittdiensten führen (z.B. Massenlöschung von Daten, unbeabsichtigter Massenversand von E-Mails)
- Erfolgreicher Prompt Injection-Angriff, der einen KI-Agenten zu unbeabsichtigten Handlungen mit erheblichen Auswirkungen veranlasst hat
- Sicherheitsvorfälle bei Konnektoren oder MCP-Servern, die zu unbefugtem Datenzugriff geführt haben
- KI-Agent führt Aktionen aus, die erheblich von seiner Konfiguration abweichen (halluzinierte Tool-Calls mit realen Auswirkungen)
- Verletzung von Grundrechten betroffener Personen durch autonome Agenten-Aktionen

8.2 Meldepflichten

Betreiber → Anbieter:

- Frist: Unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntniserlangung
- E-Mail: security@latoo.at
- Betreff: „AI ACT INCIDENT"
- Mindestinhalt der Meldung:
    - Beschreibung des Vorfalls
    - Betroffene Systeme, Daten und Personen (soweit bekannt)
    - Bei Agentic-AI-Vorfällen: betroffener Agent, ausgeführte Aktionen, betroffene Drittdienste
    - Bereits ergriffene Sofortmaßnahmen

Anbieter → zuständige Behörde:

- Frist: Binnen 15 Tagen nach Kenntniserlangung (Art. 73 Abs. 1 AI Act)
- Inhalt: Gemäß den Anforderungen des Art. 73 AI Act

Anbieter → Betreiber:

- Der Anbieter informiert den Betreiber unverzüglich über schwerwiegende Vorfälle, die das KI-System betreffen und die in der Sphäre des Anbieters aufgetreten sind

8.3 Zuständige Behörde

Zuständige Marktüberwachungsbehörde für den AI Act in Österreich: Die österreichische Datenschutzbehörde (voraussichtlich zuständig für die AI-Act-Marktüberwachung, vorbehaltlich der nationalen Umsetzungsgesetzgebung).

8.4 Zusammenarbeit mit Behörden

Bei Anfragen oder Prüfungen durch eine AI-Act-Marktüberwachungsbehörde arbeiten Anbieter und Betreiber zusammen und stellen der Behörde die angeforderten Informationen in der gesetzlich vorgeschriebenen Frist bereit. Beide Parteien informieren sich unverzüglich gegenseitig über behördliche Anfragen, die das jeweils andere Unternehmen betreffen könnten.

9. Koordination und Informationsaustausch

9.1 Pflichten des Anbieters

Der Anbieter verpflichtet sich:

- Den Betreiber über relevante AI-Act-Entwicklungen zu informieren, soweit diese die Nutzung der Brainy-Anwendung betreffen
- Technische Unterstützung bei Compliance-Maßnahmen zu leisten (z.B. Bereitstellung technischer Informationen für DPIAs oder FRIAs)
- Bei schwerwiegenden Vorfällen mit dem Betreiber zu kooperieren
- Aktualisierungen der Anwendung bereitzustellen, um die AI-Act-Compliance zu gewährleisten
- Diese AI Act Compliance Notice bei Bedarf zu aktualisieren (vgl. § 1.5)

9.2 Pflichten des Betreibers

Der Betreiber verpflichtet sich:

- Den Anbieter über beabsichtigte Hochrisiko-Nutzung vorab schriftlich zu informieren
- Schwerwiegende Vorfälle unverzüglich gemäß § 8.2 zu melden
- Bei Audits und behördlichen Kontrollen zu kooperieren
- Feedback über die Performance des KI-Systems zu geben, insbesondere bei wiederholt fehlerhaftem Verhalten von KI-Agenten
- Den Anbieter zu informieren, wenn die Nutzung von Agentic AI Funktionen eine Risikoklassenänderung begründen könnte

10. Haftung und Verantwortung

10.1 Anbieterhaftung

Der Anbieter haftet für:

- Ordnungsgemäße Entwicklung und Bereitstellung des KI-Systems, einschließlich der Agentic AI Infrastruktur und der Anbieter-MCP-Server
- Einhaltung der Anbieterpflichten nach AI Act gemäß § 3 dieser Notice

- Bereitstellung korrekter technischer Dokumentation
- Unverzügliche Information über Sicherheitsprobleme
- Implementierung der in § 3.5 genannten Sicherheitsmaßnahmen

Die Haftung des Anbieters richtet sich im Übrigen nach den Bestimmungen der AGB (§§ 9.3–9.9). Die AI-Act-Anbieterhaftung besteht zusätzlich zu den allgemeinen vertraglichen Haftungsregelungen.

10.2 Betreiberhaftung

Der Betreiber haftet für:

- Bestimmungsgemäße Nutzung des KI-Systems gemäß dieser Notice und der AGB
- Einhaltung der Betreiberpflichten nach AI Act gemäß § 4 dieser Notice
- Ordnungsgemäße Implementierung organisatorischer Maßnahmen, insbesondere der menschlichen Aufsicht bei Agentic AI
- Rechtswidrige Nutzung trotz ordnungsgemäßer Bereitstellung
- Nutzung des KI-Systems für verbotene Praktiken gemäß § 6 dieser Notice
- Konfiguration, Überwachung und Kontrolle von KI-Agenten gemäß AGB § 6.8
- Sicherheit und Betrieb von Kunden-MCP-Servern gemäß AGB § 6.8.6

10.3 Haftungsabgrenzung bei Agentic AI

Für die Haftungsabgrenzung bei Agentic AI Funktionen gilt der Grundsatz, dass alle durch einen KI-Agenten ausgeführten Autonomen Aktionen rechtlich als durch den Betreiber veranlasst gelten (AGB § 9.8.2). Der Betreiber trägt die Verantwortung für die Folgen von Aktionen, die KI-Agenten in Drittdiensten ausführen. Dies schließt die regulatorische Verantwortung nach dem AI Act ein. Die detaillierten Haftungsregelungen ergeben sich aus §§ 9.8 und 9.9 der AGB.

11. Kennzeichnung KI-generierter Inhalte

11.1 Grundsatz

Die Kennzeichnung, dass Inhalte durch eine KI erstellt oder unterstützt wurden, obliegt dem Betreiber.

11.2 Pflicht bei öffentlichen Publikationen

Bei öffentlichen Publikationen ist eine Kennzeichnung gemäß Art. 50 AI Act erforderlich. Der Betreiber hat sicherzustellen, dass KI-generierte oder KI-unterstützte Inhalte, die öffentlich zugänglich gemacht werden, als solche erkennbar sind.

11.3 Pflicht bei Agentic AI Kommunikation

Bei der Nutzung von Agentic AI Funktionen, die zu einer direkten Interaktion mit natürlichen Personen führen (z.B. automatisch versendete E-Mails, Nachrichten oder Dokumente), ist der Betreiber gemäß Art. 50 Abs. 1 AI Act verpflichtet, die Empfänger darüber zu informieren, dass sie mit einem KI-System interagieren oder der Inhalt KI-generiert ist, es sei denn, dies ist aus den Umständen offensichtlich.

Der Anbieter stellt hierfür Konfigurationsmöglichkeiten bereit (z.B. automatische Signatur-Ergänzung, KI-Kennzeichnungsoption in Agenten-Einstellungen). Die Aktivierung und inhaltliche Ausgestaltung der Kennzeichnung obliegt dem Betreiber.

11.4 Deep Fakes und synthetische Inhalte

Soweit die Brainy-Anwendung zur Erzeugung von Bild-, Audio- oder Videoinhalten eingesetzt wird, die den Anschein erwecken, authentisch zu sein (Deep Fakes im Sinne von Art. 50 Abs. 4 AI Act), ist der Betreiber verpflichtet, diese Inhalte als künstlich erzeugt oder manipuliert zu kennzeichnen. Der Anbieter stellt hierfür – soweit technisch möglich – Metadaten-Informationen bereit.

Anhang A: Bestimmungsgemäße Verwendung (Intended Use)

A.1 VORGESEHEN – Standard-Funktionen (begrenztes Risiko)

✅ Transkription von Audio/Video zu Dokumentationszwecken

✅ Erstellung von Text-Entwürfen (Briefe, E-Mails, Berichte)

✅ Zusammenfassungen und Protokolle

✅ Formulierungshilfen

✅ Übersetzungen

✅ Bildgenerierung für kreative Zwecke

✅ Administrative Dokumentation

✅ Erstellung von sprach-, text- und bildverarbeitenden Assistenten für Unternehmens-Workflows

A.2 VORGESEHEN – Agentic AI Funktionen (begrenztes Risiko, erhöhtes Risikoprofil)

✅ Automatisierte Erstellung und Versendung von E-Mails und Nachrichten auf Basis von Nutzerkonfiguration und mit implementierter menschlicher Aufsicht

✅ Automatisierte Lese- und Schreibzugriffe auf Dateispeicher des Betreibers (z.B. OneDrive, Google Drive, Dropbox)

✅ Automatisierte CRM- und ERP-Aktualisierungen auf Basis konfigurierter Workflows

✅ Workflow-Automatisierung auf Basis von Triggern und Zeitplänen für administrative und operative Geschäftsprozesse

✅ Integration externer Systeme über Anbieter-MCP-Server zur standardisierten Datenanbindung

✅ Integration kundeneigener Systeme über Kunden-MCP-Server unter Einhaltung der Sicherheitsanforderungen (AGB § 6.8.6)

✅ Datenanalyse und -aggregation aus mehreren Drittdiensten zur Entscheidungsunterstützung

✅ Automatisierte Dokumentenerstellung und -ablage auf Basis konfigurierter Vorlagen und Quellen

A.3 NICHT VORGESEHEN – Allgemein

❌ Medizinische Diagnose oder Therapieentscheidungen

❌ Automatisierte Personalentscheidungen (Einstellung/Kündigung/Beförderung) ohne menschliche Einzelfallprüfung

❌ Beweiswürdigung in Gerichtsverfahren

❌ Biometrische Identifikation

❌ Kreditwürdigkeitsprüfung natürlicher Personen

❌ Steuerung kritischer Infrastruktur

❌ Jede Nutzung, die eine verbotene Praktik gemäß Art. 5 AI Act darstellt (vgl. § 6 dieser Notice)

A.4 NICHT VORGESEHEN – Agentic AI

❌ Autonome Vertragsabschlüsse oder Abgabe rechtsverbindlicher Erklärungen ohne menschliche Freigabe

❌ Automatisierte Personalentscheidungen über KI-Agenten (Einstellung, Kündigung, Beförderung, Leistungsbewertung) ohne ausreichende menschliche Aufsicht und individuelle Prüfung

❌ Autonome Finanztransaktionen (Überweisungen, Bestellungen, Zahlungsfreigaben) ohne menschliche Genehmigung

❌ Unkontrollierter Zugriff auf kritische Unternehmensinfrastruktur über Konnektoren oder MCP-Server

❌ Vollständig autonome Entscheidungen mit erheblichen rechtlichen oder wirtschaftlichen Auswirkungen auf natürliche Personen ohne menschliche Aufsicht

❌ Einsatz von KI-Agenten zur systematischen Überwachung, Bewertung oder Profiling von Mitarbeitern, Kunden oder sonstigen natürlichen Personen

❌ Nutzung von KI-Agenten zur Manipulation oder Täuschung von Kommunikationspartnern (z.B. Vortäuschung menschlicher Kommunikation ohne Kennzeichnung)

❌ Einsatz von KI-Agenten zur Umgehung von Zugriffsbeschränkungen, Sicherheitsmaßnahmen oder Nutzungsbedingungen von Drittdiensten