

Vereinbarung zur Auftragsverarbeitung

Version 3.1 · Gültig ab 1. September 2026 · Artikel 28 DSGVO · Anlage zu den Mimirio Software- und Servicebedingungen Version 3.1

1. Parteien, Gegenstand und Rollen

- 1.1 Diese Vereinbarung zur Auftragsverarbeitung („Vereinbarung“) wird geschlossen zwischen dem nachstehend genannten Kunden als Verantwortlichem („Kunde“) und der Mimirio FlexCo, Schönbrunner Straße 63/30, 1050 Wien, Österreich, FN 640289, als Auftragsverarbeiter („Mimirio“).

Verantwortlicher (Kunde)

Anschrift

Firmenbuch- bzw.
Registernummer

Ansprechstelle für
Datenschutz

Meldeadresse für
Datenschutzvorfälle

- 1.2 Ansprechstelle für Datenschutz bei Mimirio: security@mimirio.com. Meldungen und Anfragen aus dieser Vereinbarung können an diese Adresse gerichtet werden; Supportanfragen an den im Order Form vereinbarten Supportkanal.
- 1.3 Gegenstand der Verarbeitung ist die Erbringung der im Order Form und in den Mimirio Software- und Servicebedingungen vereinbarten Leistungen: Bereitstellung und Betrieb der Mimirio-Plattform einschließlich des KI-Modellbetriebs, Anbindung der vom Kunden ausgewählten Quellsysteme, Support und Fehleranalyse. Art, Zweck und Umfang der Verarbeitung, die Kategorien betroffener Personen und personenbezogener Daten sowie die Aufbewahrungsfristen ergeben sich aus Anlage A.
- 1.4 Der Kunde ist Verantwortlicher im Sinne des Art 4 Z 7 DSGVO, Mimirio ist Auftragsverarbeiter im Sinne des Art 4 Z 8 DSGVO. Der Betrieb der Infrastruktur oder die Verfügung über administrative Zugänge macht Mimirio nicht zum Verantwortlichen.
- 1.5 Diese Vereinbarung gilt unabhängig vom Betriebsmodell: für den von Mimirio betriebenen Cloud-Dienst ebenso wie für eine Installation, die der Kunde selbst oder ein von ihm beauftragter Dritter betreibt. Auch bei einer selbst betriebenen Installation erhält Mimirio zur Bereitstellung, Aktualisierung, Wartung, Support und Fehleranalyse Zugriff auf die Installation und damit auf die darin verarbeiteten personenbezogenen Daten; dieser Zugriff ist Auftragsverarbeitung und von dieser Vereinbarung erfasst. Welches Betriebsmodell vereinbart ist und welche Komponenten wer betreibt, ergibt sich aus dem Order Form (Anhang A bzw Anhang B der Bedingungen).
- 1.6 Diese Vereinbarung geht dem Order Form und den Bedingungen in Bezug auf die Verarbeitung personenbezogener Daten vor. Im Übrigen gelten das Order Form und die Bedingungen unverändert. Begriffe dieser Vereinbarung sind entsprechend ihrer Definition in der DSGVO zu verstehen.

2. Dauer

- 2.1 Diese Vereinbarung tritt mit Unterfertigung durch beide Parteien in Kraft, jedenfalls vor Beginn der Verarbeitung personenbezogener Daten, und läuft für die Dauer des Vertragsverhältnisses.

- 2.2 Sie gilt auch für Verarbeitungen personenbezogener Daten, die Mimirio bereits vor Abschluss dieser Vereinbarung im Auftrag des Kunden durchgeführt hat.
- 2.3 Pflichten, die über das Ende des Vertragsverhältnisses hinausreichen — insbesondere Vertraulichkeit, Löschung und Nachweisführung nach Punkt 13 — bleiben bis zu ihrer Erfüllung aufrecht.

3. Weisungen

- 3.1 Mimirio verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden. Diese Vereinbarung, das Order Form, die Bedingungen und die vom Kunden vorgenommene Konfiguration der Plattform bilden die anfänglichen Weisungen.
- 3.2 Einzelweisungen erteilt der Kunde schriftlich oder per E-Mail über die in Punkt 1 genannten Ansprechstellen. Mimirio setzt sie im Rahmen des vereinbarten Leistungsumfangs um; darüber hinausgehender Aufwand wird gesondert vereinbart.
- 3.3 Eine Verarbeitung für eigene Zwecke von Mimirio erfolgt nicht. Erhält Mimirio eine behördliche oder gerichtliche Anordnung, Daten des Kunden herauszugeben, informiert Mimirio den Kunden — soweit gesetzlich zulässig — unverzüglich und verweist die anordnende Stelle an den Kunden.
- 3.4 Ist Mimirio der Ansicht, dass eine Weisung gegen datenschutzrechtliche Bestimmungen der Union oder der Mitgliedstaaten verstößt, informiert Mimirio den Kunden unverzüglich und darf die Umsetzung dieser Weisung bis zur Klärung aussetzen.

4. Vertraulichkeit

- 4.1 Mimirio erklärt rechtsverbindlich, alle mit der Verarbeitung befassten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet zu haben oder sicherzustellen, dass sie einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht nach Beendigung der Tätigkeit und nach Ausscheiden fort.
- 4.2 Zugriff auf personenbezogene Daten des Kunden erhalten nur Personen, die ihn zur Erbringung der vereinbarten Leistungen benötigen, im erforderlichen Umfang und nachvollziehbar protokolliert.
- 4.3 Eine Weitergabe an Dritte erfolgt nur nach dieser Vereinbarung, insbesondere an die in Anlage C genannten Unterauftragsverarbeiter, oder soweit gesetzlich verpflichtend.

5. Sicherheit der Verarbeitung

- 5.1 Mimirio hat die technischen und organisatorischen Maßnahmen nach Art 32 DSGVO getroffen. Sie sind in Anlage B beschrieben und dokumentiert.
- 5.2 Mimirio darf die Maßnahmen weiterentwickeln, insbesondere technischen Fortschritt nachvollziehen. Das vereinbarte Schutzniveau darf dadurch nicht unterschritten werden. Wesentliche Änderungen werden dokumentiert und dem Kunden auf Anfrage mitgeteilt.
- 5.3 Die Verantwortung für Sicherheitsmaßnahmen folgt der Betriebsverantwortung: Mimirio verantwortet die von Mimirio betriebenen Komponenten und die eigenen Zugangswege, der Kunde verantwortet Identitäten, Berechtigungen, die angebundenen Quellsysteme und eine allenfalls von ihm betriebene Infrastruktur (Anhang B der Bedingungen).

6. Ort der Verarbeitung

- 6.1 Die Verarbeitung personenbezogener Daten erfolgt ausschließlich innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums. Die konkrete Region ergibt sich aus dem Order Form.
- 6.2 Eine Verarbeitung in einem Drittland — einschließlich eines Zugriffs zu Support- oder Wartungszwecken — findet nicht ohne vorherige Vereinbarung mit dem Kunden und ohne Vorliegen einer Grundlage nach Art 44 ff DSGVO statt.
- 6.3 Auch Zugriffe von Mimirio auf die Plattform erfolgen aus der EU bzw dem EWR und über die im Order Form vereinbarte Zugangsmethode.

7. KI-spezifische Zusagen

- 7.1 Mimirio garantiert ausdrücklich, dass personenbezogene Daten des Kunden nicht zum Training oder zum Fine-Tuning von KI-Modellen verwendet werden. Diese Zusage gilt ebenso für die in Anlage C genannten Unterauftragsverarbeiter.
- 7.2 Eingaben (Prompts), Konversationen, Inhalte und daraus erzeugte Ausgaben verarbeitet Mimirio ausschließlich zur Erbringung der vereinbarten Leistungen. Modelldienste werden in einer Konfiguration eingesetzt, in der Eingaben und Ausgaben nicht zum Training verwendet und nicht über die zur Leistungserbringung erforderliche Dauer gespeichert werden.
- 7.3 Mimirio trifft keine automatisierten Entscheidungen über betroffene Personen. Ausgaben der Software sind Vorschläge; die Verwendung und eine allfällige Entscheidung verantwortet der Kunde. Art 22 DSGVO ist vom Kunden als Verantwortlichem zu beachten.
- 7.4 Nutzungs- und Telemetriedaten verarbeitet Mimirio zur Leistungserbringung, zur Sicherheit des Dienstes, zur Kapazitätsplanung und zur Fehlerbehebung. Eine Nutzung für eigene Zwecke von Mimirio, etwa zur Produktverbesserung, erfolgt ausschließlich in anonymisierter Form ohne Personenbezug. Zur Abrechnung des Verbrauchs nach Punkt 7.11 der Bedingungen werden Nutzungsdaten je Installation zusammengefasst; Rechnungen und Verbrauchsnachweise enthalten keine Angaben zu einzelnen Nutzern.

8. Unterstützung bei Betroffenenrechten

- 8.1 Mimirio unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen dabei, die Rechte betroffener Personen nach Kapitel III DSGVO (Information, Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen zu erfüllen, und stellt dem Kunden die dafür erforderlichen Informationen und Funktionen zur Verfügung.
- 8.2 Richtet eine betroffene Person einen Antrag unmittelbar an Mimirio, leitet Mimirio ihn unverzüglich an den Kunden weiter, teilt dies der betroffenen Person mit und beantwortet den Antrag nicht selbst.
- 8.3 Berichtigung, Löschung oder Einschränkung der Verarbeitung nimmt Mimirio nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Kunden vor. Davon unberührt bleiben Funktionen, die der Kunde oder seine Nutzer in der Software selbst ausführen.

9. Verletzungen des Schutzes personenbezogener Daten

- 9.1 Mimirio teilt dem Kunden eine Verletzung des Schutzes personenbezogener Daten ohne unangemessene Verzögerung mit, jedenfalls innerhalb von 48 Stunden ab Kenntnis, an die in Punkt 1 genannte Meldeadresse. Ist die Bewertung innerhalb dieser Frist noch nicht abgeschlossen, genügt eine erste Mitteilung innerhalb von 48 Stunden mit den zu diesem Zeitpunkt verfügbaren Informationen; die weiteren Informationen werden unverzüglich nachgereicht. Begründete Verdachtsfälle sind ebenfalls mitzuteilen.
- 9.2 Die Mitteilung enthält, soweit verfügbar:
 - eine Beschreibung der Art der Verletzung sowie der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze,
 - den Namen und die Kontaktdaten der Anlaufstelle bei Mimirio,
 - eine Beschreibung der wahrscheinlichen Folgen,
 - eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und zur Abmilderung möglicher nachteiliger Auswirkungen.
- 9.3 Stehen nicht alle Angaben innerhalb der Frist zur Verfügung, erfolgt die Mitteilung mit den vorhandenen Informationen; die weiteren Angaben werden unverzüglich nachgereicht. Die Frist wird durch fehlende Detailinformationen nicht verlängert.
- 9.4 Mimirio unterstützt den Kunden bei der Einhaltung der Art 32 bis 36 DSGVO, insbesondere bei Meldungen an die Aufsichtsbehörde, bei der Benachrichtigung betroffener Personen und bei einer Datenschutz-Folgenabschätzung, und dokumentiert Vorfälle einschließlich der getroffenen Maßnahmen. Eine Meldung im Namen des Kunden erfolgt nur auf dessen Weisung.

- 9.5 Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen der Leistungserbringung, Verstöße gegen diese Vereinbarung sowie Kontrollen oder Maßnahmen von Aufsichtsbehörden, soweit sie einen Bezug zur Verarbeitung für den Kunden aufweisen.

10. Nachweise und Überprüfung

- 10.1 Mimirio stellt dem Kunden die Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art 28 DSGVO erforderlich sind, insbesondere:
- die Dokumentation der technischen und organisatorischen Maßnahmen (Anlage B) in ihrer jeweils aktuellen Fassung,
 - das Verzeichnis der Verarbeitungstätigkeiten nach Art 30 Abs 2 DSGVO, soweit es die Verarbeitung für den Kunden betrifft,
 - aktuelle Zertifikate und Prüfberichte der eingesetzten Hosting- und Modellanbieter,
 - die Beantwortung angemessener Datenschutz- und Sicherheitsfragebögen des Kunden.
- 10.2 Reichen diese Nachweise im Einzelfall nicht aus, ist der Kunde berechtigt, die Einhaltung dieser Vereinbarung selbst oder durch beauftragte, zur Vertraulichkeit verpflichtete Dritte zu überprüfen, die nicht in Wettbewerb zu Mimirio stehen. Solche Überprüfungen erfolgen in angemessenem Umfang, mit angemessener Vorankündigung — in der Regel 14 Tage —, zu üblichen Geschäftszeiten, ohne vermeidbare Störung des Geschäftsbetriebs und in der Regel einmal jährlich. Anlassbezogen, insbesondere nach einer Verletzung des Schutzes personenbezogener Daten oder auf Anordnung einer Aufsichtsbehörde, ist eine Überprüfung auch darüber hinaus zulässig.
- 10.3 Mimirio erteilt die erforderlichen Auskünfte, demonstriert Abläufe und ermöglicht den erforderlichen Einblick. Ausgenommen bleiben Daten anderer Kunden, Quellcode und sonstige Betriebs- und Geschäftsgeheimnisse; für Rechenzentren richtet sich eine Überprüfung nach den Möglichkeiten und Nachweisen des jeweiligen Anbieters.
- 10.4 Den eigenen Aufwand einer Überprüfung trägt jede Partei selbst; der Kunde trägt jedoch die angemessenen Kosten einer Unterstützung durch Mimirio, die über die Nachweise nach Punkt 10.1 hinausgeht, sowie die Kosten einer Überprüfung, die ohne besonderen Anlass mehr als einmal in zwölf Monaten durchgeführt wird. Punkt 9.9 der Bedingungen gilt für diese Kosten.

11. Unterauftragsverarbeiter

- 11.1 Der Kunde stimmt der Beauftragung der in Anlage C genannten Unterauftragsverarbeiter zu. Anlage C nennt alle möglichen Unterauftragsverarbeiter; welche davon für das Deployment des Kunden tatsächlich eingesetzt werden, ergibt sich aus Anlage C in Verbindung mit dem Order Form.
- 11.2 Mimirio informiert den Kunden über die beabsichtigte Hinzuziehung eines weiteren oder den Austausch eines bestehenden Unterauftragsverarbeiters mindestens 30 Tage vorab unter Angabe der Leistung, des Sitzes und des Ortes der Verarbeitung.
- 11.3 Der Kunde kann der Änderung innerhalb von 14 Tagen nach der Mitteilung aus nachvollziehbaren datenschutzrechtlichen Gründen widersprechen. Die Parteien suchen in diesem Fall eine einvernehmliche Lösung. Kommt eine solche nicht zustande, kann der Kunde die betroffene Leistung zum Zeitpunkt der Änderung kündigen, ohne dass Kosten für die verfrühte Beendigung anfallen; bis dahin bereits erbrachte Leistungen bleiben zu vergüten.
- 11.4 Mimirio schließt mit jedem Unterauftragsverarbeiter eine Vereinbarung nach Art 28 Abs 4 DSGVO, die dieselben Pflichten vorsieht, die Mimirio nach dieser Vereinbarung obliegen. Erfüllt ein Unterauftragsverarbeiter seine Datenschutzpflichten nicht, haftet Mimirio dem Kunden gegenüber wie für eigenes Handeln.
- 11.5 Leistungen, bei denen kein Zugriff auf personenbezogene Daten des Kunden erfolgt — etwa Telekommunikation, Postdienste oder Reinigung —, sind keine Auftragsverarbeitung. Ist ein Zugriff nicht auszuschließen, verpflichtet Mimirio den Dienstleister zur Vertraulichkeit und kontrolliert die Einhaltung.

12. Pflichten des Verantwortlichen

- 12.1 Der Kunde verantwortet die Rechtmäßigkeit der Verarbeitung, insbesondere das Vorliegen einer Rechtsgrundlage, die Erfüllung der Informationspflichten und allenfalls erforderliche Einwilligungen. Er entscheidet, welche Quellsysteme angebunden, welche Inhalte verarbeitet und welche Berechtigungen vergeben werden.
- 12.2 Besondere Kategorien personenbezogener Daten nach Art 9 DSGVO und Daten nach Art 10 DSGVO sind nicht Gegenstand dieser Vereinbarung, sofern sie nicht ausdrücklich vereinbart und allenfalls erforderliche zusätzliche Maßnahmen festgelegt wurden. Der Kunde informiert Mimirio vor Anbindung einer Quelle, die solche Daten enthält.
- 12.3 Der Kunde führt sein eigenes Verzeichnis der Verarbeitungstätigkeiten und erforderlichenfalls eine Datenschutz-Folgenabschätzung; Mimirio unterstützt ihn dabei nach Punkt 9.4.
- 12.4 Der Kunde verwaltet seine Nutzerkonten und Berechtigungen und deaktiviert die Konten ausgeschiedener Nutzer unverzüglich.
- 12.5 Wird Mimirio von Dritten oder Behörden in Anspruch genommen, weil eine Weisung des Kunden, eine fehlende Rechtsgrundlage oder eine Verletzung der Pflichten des Kunden nach diesem Punkt 12 dafür ursächlich war, hält der Kunde Mimirio schad- und klaglos. Das gilt nicht, soweit Mimirio die Rechtsverletzung selbst zu vertreten hat.

13. Löschung und Rückgabe

- 13.1 Nach Beendigung des Vertragsverhältnisses gibt Mimirio die personenbezogenen Daten nach Wahl des Kunden heraus oder löscht sie. Für die Herausgabe gilt Anhang C der Bedingungen (Datenexport) mit den dort genannten Formaten und Ausnahmen.
- 13.2 Die Daten bleiben mindestens 30 Kalendertage nach Beendigung zum Abruf verfügbar und werden anschließend innerhalb weiterer 30 Tage gelöscht, einschließlich der Kopien in den Backupzyklen nach Ablauf des jeweiligen Zyklus. Eine abweichende Frist bedarf einer Vereinbarung in Textform.
- 13.3 Die Aufbewahrungsfristen für die einzelnen Datenkategorien während des laufenden Vertragsverhältnisses ergeben sich aus Anlage A.
- 13.4 Gesetzlich erforderliche Kopien bleiben geschützt gespeichert und werden zu keinem anderen Zweck verwendet.
- 13.5 Mimirio bestätigt die Löschung auf Anfrage in Textform.

14. Haftung

- 14.1 Punkt 10 der Bedingungen gilt für diese Vereinbarung uneingeschränkt, einschließlich der dort geregelten Haftungsbeschränkung und Haftungsausschlüsse. Ansprüche zwischen den Parteien aus oder im Zusammenhang mit dieser Vereinbarung — einschließlich des Rückgriffs und der Haftungsverteilung nach Art 82 Abs 5 DSGVO, verhängter Geldbußen sowie der Kosten für Benachrichtigungen, Behebungsmaßnahmen, forensische Untersuchungen oder Kreditüberwachung — werden auf die Haftungshöchstbeträge in Punkt 10 der Bedingungen angerechnet, sind durch diese beschränkt und unterliegen den dort geregelten Ausschlüssen wie jeder andere Anspruch. Die Haftung gegenüber betroffenen Personen nach Art 82 DSGVO, die Haftung für Personenschäden, die Haftung für Vorsatz sowie sonstige Haftung, die nach zwingendem Recht nicht beschränkt werden kann, bleiben unberührt.
- 14.2 Jede Partei trägt die Verantwortung für den ihr zugeordneten Verantwortungsbereich (Punkt 5.3). Der Einsatz eines Unterauftragsverarbeiters nimmt Mimirio die Verantwortung für die betroffene Leistung nicht ab.

15. Schlussbestimmungen

- 15.1 Mitteilungen, Weisungen und Änderungen dieser Vereinbarung bedürfen der Textform; E-Mail zwischen den benannten Ansprechstellen genügt, soweit nicht zwingendes Recht eine andere Form verlangt.

- 15.2 Erfordern Änderungen der Rechtslage oder Vorgaben einer Aufsichtsbehörde eine Anpassung dieser Vereinbarung, vereinbaren die Parteien die erforderlichen Anpassungen unverzüglich und nach Treu und Glauben.
- 15.3 Sind oder werden einzelne Bestimmungen dieser Vereinbarung unwirksam, bleiben die übrigen Bestimmungen gültig. Unwirksame Bestimmungen sind einvernehmlich durch solche zu ersetzen, die dem angestrebten Zweck möglichst nahekommen.
- 15.4 Es gilt österreichisches materielles Recht unter Ausschluss seiner Kollisionsnormen. Für Streitigkeiten aus dieser Vereinbarung sind die sachlich zuständigen Gerichte in Wien ausschließlich zuständig. Zwingende Bestimmungen der DSGVO und die Zuständigkeit der Aufsichtsbehörden bleiben unberührt.
- 15.5 Diese Vereinbarung liegt in einer deutschen und einer englischen Fassung vor. Maßgeblich ist die von den Parteien unterzeichnete Fassung. Werden beide Sprachfassungen für dieselbe Beauftragung unterzeichnet, ist die deutsche Fassung maßgeblich. Die Bedingungen werden in englischer Sprache abgeschlossen; maßgeblich ist der englische Wortlaut.
- 15.6 Die Anlagen A, B und C sind Bestandteil dieser Vereinbarung.

Der Verantwortliche (Kunde)**Mimirio FlexCo**

Ort, Datum

Ort, Datum

Name, Funktion

Name, Funktion

Anlage A — Einzelheiten der Verarbeitung

A1. Zweck der Verarbeitung

- A1.1 Mimirio verarbeitet personenbezogene Daten, um die vereinbarten Leistungen zu erbringen: Bereitstellung und Betrieb der Mimirio-Plattform, Betrieb des KI-Modelldienstes, Anbindung und Indexierung der vom Kunden ausgewählten Quellen, Beantwortung von Anfragen der Nutzer und Erzeugung von Ausgaben, Support und Fehleranalyse sowie Sicherstellung von Sicherheit, Stabilität und Kapazität des Dienstes.
- A1.2 Die Verarbeitung erfolgt auf Grundlage einer strikten Need-to-know-Basis und datenschutzfreundlicher Voreinstellungen: Umfang der zugänglichen Daten, Dauer und Eingriffstiefe werden auf das für den jeweiligen Zweck Erforderliche beschränkt.

A2. Kategorien betroffener Personen

- A2.1 Beschäftigte und Auftragnehmer des Kunden, die die Software nutzen oder verwalten, sowie die vom Kunden benannten Ansprechpersonen.
- A2.2 Personen, deren personenbezogene Daten in den vom Kunden angebotenen oder hochgeladenen Inhalten enthalten sind — etwa als Verfasser, Bearbeiter, Empfänger oder als in einem Dokument genannte Person. Welche das sind, bestimmt der Kunde durch die Auswahl der Quellen und Inhalte.

A3. Kategorien personenbezogener Daten

Kategorie	Beschreibung
Kontodaten	Name, E-Mail-Adresse, Konto-UUID, Rolle und Berechtigungen. Keine Passwörter — die Authentifizierung erfolgt über das Identitätssystem des Kunden.
Inhalts- und Wissensdaten	Inhalte und Metadaten der angebotenen Quellen und der hochgeladenen Dateien (Inhalt, Autor, letzte Bearbeitung, Erstellungs- und Änderungsdatum, Ablageort, Berechtigungsinformationen). Der Umfang bestimmt sich durch die vom Kunden aktivierten Integrationen.
Eingaben und Ausgaben	Texteingaben (Prompts), Konversationen und die korrespondierenden Antworten und Erzeugnisse, einschließlich erzeugter Dokumente.
Nutzungs- und Telemetriedaten	Verbrauch, Tokens, Qualitäts- und Genauigkeitswerte, Metadaten der Anfragen, Zeitstempel und technische Kennungen.
Protokolldaten	Zugriffs-, Sicherheits- und Fehlerprotokolle.
Supportdaten	Anfragen, Korrespondenz und die vom Kunden übermittelten Diagnoseinformationen.

- A3.1 Besondere Kategorien personenbezogener Daten nach Art 9 DSGVO sind nicht Gegenstand der Verarbeitung, sofern nicht nach Punkt 12.2 ausdrücklich vereinbart.

A4. Art der Verarbeitungstätigkeiten

- Erheben aus den angebotenen Quellen, Speichern und Organisieren,
- Indexieren und Verknüpfen zur Auffindbarkeit innerhalb der Berechtigungen des Nutzers,
- Abfragen, Auswerten und Erzeugen von Ausgaben,
- Protokollieren, Sichern (Backup) und Wiederherstellen,
- Analysieren zu Zwecken der Fehlerbehebung und Sicherheit auf Need-to-know-Basis,
- Löschen und Herausgeben nach Punkt 13.

A5. Aufbewahrung

Kategorie	Aufbewahrung
Kontodaten	Für die Dauer des Vertragsverhältnisses; Löschung nach Punkt 13.

Kategorie	Aufbewahrung
Inhalts- und Wissensdaten	Für die Dauer der Anbindung der jeweiligen Quelle; nach Trennung der Quelle werden die Kopien und Indexeinträge entfernt.
Eingaben, Konversationen und Erzeugnisse	Bis zur Löschung durch den Nutzer oder den Kunden, sonst für die Dauer des Vertragsverhältnisses.
Nutzungs- und Telemetriedaten	12 Monate, danach Löschung oder Anonymisierung.
Protokolldaten	90 Tage, sofern nicht im Order Form eine längere Frist vereinbart oder gesetzlich erforderlich ist.
Backups	Gemäß der im Order Form vereinbarten Aufbewahrung, im Standard 30 Tage rollierend.
Supportdaten	24 Monate ab Abschluss der Anfrage.

A6. Ort der Verarbeitung

A6.1 Ausschließlich EU bzw EWR. Die konkrete Region und der Hosting-Anbieter ergeben sich aus dem Order Form; welche Unterauftragsverarbeiter dabei eingesetzt werden, ergibt sich aus Anlage C. Bei einer vom Kunden betriebenen Installation ist Ort der Verarbeitung die vom Kunden gewählte Umgebung; die Zugriffe von Mimirio erfolgen aus der EU bzw dem EWR.

Anlage B — Technische und organisatorische Maßnahmen

B1. Grundlagen und Verantwortungsabgrenzung

- B1.1 Die Mimirio-Plattform wird in zwei Betriebsmodellen bereitgestellt: als von Mimirio betriebener Cloud-Dienst und als Installation, die der Kunde selbst oder ein von ihm beauftragter Dritter betreibt (Punkt 1.5). Die Maßnahmen ergeben sich daher aus mehreren Ebenen:
- Rechenzentrum, physische Sicherheit und Plattformdienste: beim Cloud-Dienst der Infrastrukturanbieter nach Anlage C, bei einer selbst betriebenen Installation der Kunde bzw der von ihm beauftragte Anbieter.
 - Anwendung, Voreinstellungen, Entwicklungs- und Freigabeprozesse: Mimirio, in beiden Betriebsmodellen.
 - Zugangswege von Mimirio für Bereitstellung, Wartung und Support: Mimirio, in beiden Betriebsmodellen, über die im Order Form vereinbarte Zugangsmethode.
 - Identitäten, Berechtigungen und die angebundenen Quellsysteme: der Kunde (Punkt 5.3).
- B1.2 Bei einer vom Kunden betriebenen Installation gelten die nachstehenden Maßnahmen für die Anwendung, ihre Voreinstellungen, die Entwicklungs- und Freigabeprozesse sowie für die Zugriffe von Mimirio. Maßnahmen, die die Infrastruktur betreffen — insbesondere die physische Sicherheit (Punkt B3.5) sowie Sicherung, Betriebsüberwachung und Wiederherstellbarkeit (Punkt B5) — verantwortet insoweit der Kunde; Mimirio unterstützt im vereinbarten Leistungsumfang und stellt die dafür erforderlichen Informationen bereit.
- B1.3 Beim Cloud-Dienst wird die Plattform auf Infrastruktur der in Anlage C in Verbindung mit dem Order Form genannten Anbieter betrieben. Welche Zertifizierungen und Prüfberichte — etwa ISO/IEC 27001, ISO/IEC 27017 oder SOC 2 — vorliegen, richtet sich nach dem im Order Form gewählten Infrastrukturanbieter und ergibt sich aus Anlage C. Die aktuellen Nachweise stellt Mimirio auf Anfrage bereit. Bei einer vom Kunden betriebenen Installation richten sich diese Nachweise nach der Umgebung des Kunden. Mimirio richtet das eigene Informationssicherheitsmanagement an diesen Standards aus, verfügt derzeit jedoch über keine eigene Zertifizierung.

B2. Pseudonymisierung und Verschlüsselung

- Übertragung ausschließlich verschlüsselt (TLS 1.2 oder höher), auch zwischen den Komponenten der Plattform und zu den angebundenen Quellsystemen.
- Verschlüsselung im Ruhezustand für Datenbanken, Objektspeicher und Backups mit den Verfahren des jeweiligen Infrastrukturanbieters, in der Regel AES-256, soweit der jeweilige Dienst dies unterstützt. Bei einer vom Kunden betriebenen Installation richtet sich die Verschlüsselung im Ruhezustand nach der Umgebung des Kunden (Punkt B1.2).
- Zugangsdaten und Schlüssel liegen in Konfigurationsdateien auf dem jeweiligen Host. Der Zugriff darauf ist auf die betriebsnotwendigen System- und Administrationskonten beschränkt; es gelten die Verschlüsselung im Ruhezustand nach Punkt B2 und die Zugangskontrollen nach Punkt B3.
- Wo es für den Zweck möglich ist, werden Auswertungen auf pseudonymisierten oder aggregierten Daten durchgeführt; identifizierende Merkmale werden getrennt gehalten.

B3. Vertraulichkeit

- B3.1 **Zugangskontrolle.** Authentifizierung über das Identitätssystem des Kunden bzw Microsoft Entra ID, Mehr-Faktor-Authentifizierung für alle administrativen Zugänge, benannte persönliche Konten ohne gemeinsam genutzte Zugangsdaten, Passwort- und Sperrrichtlinien.
- B3.2 **Zugriffskontrolle.** Rollenbasierte Berechtigungen nach dem Prinzip der geringsten Rechte, Standardberechtigungsprofile auf Need-to-know-Basis, ein definierter Prozess für die Vergabe und Entziehung von Rechten und eine periodische Überprüfung insbesondere administrativer Konten.
- B3.3 **Mandantentrennung.** Die Daten jedes Kunden werden logisch getrennt gehalten und über die Kennung der Installation isoliert; Abfragen respektieren die Berechtigungen des jeweiligen Nutzers im Quellsystem.
- B3.4 **Supportzugriff.** Zugriff auf Kundendaten zu Support- und Fehlerbehebungs Zwecken nur anlassbezogen, im erforderlichen Umfang, protokolliert und über die im Order Form vereinbarte Zugangsmethode.

- B3.5 **Physische Sicherheit.** Rechenzentren des Infrastrukturanbieters mit Zutrittskontrolle, Überwachung und Besucherbegleitung. In den Räumlichkeiten von Mimirio: verschlossene Zugänge, Begleitung von Besuchern und eine Clear-Desk-/Clear-Screen-Regel; Kundendaten werden nicht auf Endgeräten gespeichert.
- B3.6 **Personal.** Vertraulichkeitsverpflichtung vor Aufnahme der Tätigkeit, Datenschutz- und Sicherheitsschulungen, definierte Prozesse bei Eintritt, Wechsel und Ausscheiden einschließlich des unverzüglichen Entzugs der Zugänge.

B4. Integrität

- B4.1 **Eingabekontrolle.** Protokollierung der Anmeldungen, administrativen Änderungen und Zugriffe auf Kundendaten mit Zeitstempel und handelndem Konto.
- B4.2 **Änderungskontrolle.** Versionskontrolle, verpflichtendes Code-Review, geschützte Hauptzweige, automatisierte Tests, Infrastruktur als Code und getrennte Freigabeschritte für Produktivänderungen.
- B4.3 **Übertragungskontrolle.** Datenübertragungen erfolgen ausschließlich über verschlüsselte, authentifizierte Verbindungen; Exporte nur über die vorgesehenen Funktionen und an berechtigte Empfänger.

B5. Verfügbarkeit und Belastbarkeit

- B5.1 **Sicherung.** Beim Cloud-Dienst regelmäßige, verschlüsselte Backups mit der im Order Form vereinbarten Häufigkeit und Aufbewahrung, getrennt von den Produktivsystemen gespeichert; Wiederherstellungen werden erprobt. Umfang, Häufigkeit, Aufbewahrung und allfällige Wiederherstellungsziele ergeben sich ausschließlich aus dem Order Form. Bei einer vom Kunden betriebenen Installation obliegen Sicherung und Wiederherstellung dem Kunden, soweit im Order Form nichts anderes vereinbart ist.
- B5.2 **Betriebsüberwachung.** Überwachung von Verfügbarkeit, Auslastung und Sicherheitsereignissen mit Alarmierung; definierte Reaktionswege außerhalb der Geschäftszeiten für kritische Ereignisse.
- B5.3 **Schutz gegen Angriffe und Verlust.** Netzwerksegmentierung, Firewalls und Web-Application-Firewall, DDoS-Schutz des Anbieters, Härtung der Systeme sowie Malware-Schutz auf den Arbeitsplatzsystemen.
- B5.4 **Wiederherstellbarkeit.** Dokumentierte Wiederherstellungsverfahren; vereinbarte Wiederherstellungsziele ergeben sich aus dem Order Form.

B6. Zweckbindung und Trennung

- Personenbezogene Daten des Kunden werden nicht zum Training oder Fine-Tuning von KI-Modellen verwendet (Punkt 7.1).
- Produktions-, Test- und Entwicklungsumgebungen sind getrennt; in Test- und Entwicklungsumgebungen werden keine Produktivdaten des Kunden verwendet.
- Modelldienste werden so konfiguriert, dass Eingaben und Ausgaben nicht zum Training verwendet und nicht länger als für die Leistungserbringung erforderlich gespeichert werden.
- Daten unterschiedlicher Kunden werden getrennt verarbeitet; ein Zugriff über die Grenzen einer Installation hinweg ist ausgeschlossen.

B7. Überprüfung, Bewertung und Evaluierung

- B7.1 **Datenschutzmanagement.** Dokumentierte Verfahren, Verzeichnis der Verarbeitungstätigkeiten nach Art 30 Abs 2 DSGVO, benannte Ansprechstelle für Datenschutz (security@mimirio.com) und regelmäßige Schulungen.
- B7.2 **Schwachstellenmanagement.** Laufende Aktualisierung von Abhängigkeiten und Systemen, automatisierte Schwachstellen- und Abhängigkeitsprüfungen sowie priorisierte Behebung nach Schweregrad. Penetrationstests werden anlassbezogen und bei wesentlichen Änderungen durchgeführt.
- B7.3 **Vorfallsbehandlung.** Definierter Prozess für Erkennung, Bewertung, Eindämmung, Behebung und Dokumentation von Sicherheitsvorfällen, einschließlich der Meldewege nach Punkt 9.

- B7.4 **Voreinstellungen.** Datenschutzfreundliche Voreinstellungen; neue Funktionen, die zusätzliche Berechtigungen benötigen, werden nicht ohne Freigabe des Kunden aktiviert.
- B7.5 **Lieferantenmanagement.** Auswahl und Überprüfung der Unterauftragsverarbeiter nach Punkt 11, formalisiertes Auftragsmanagement und Vorabprüfung vor Beauftragung.

Anlage C — Unterauftragsverarbeiter

C1.1 Die folgende Tabelle nennt alle Unterauftragsverarbeiter, die Mimirio für Leistungen nach dieser Vereinbarung einsetzen kann. Es werden nicht bei jedem Deployment alle davon eingesetzt: welche tatsächlich zum Einsatz kommen, richtet sich nach dem im Order Form vereinbarten Betriebsmodell, Hosting-Anbieter und Modellanbieter. Die Spalte „Einsatz“ nennt die jeweilige Voraussetzung. Für eine vom Kunden selbst betriebene Installation setzt Mimirio keine Unterauftragsverarbeiter für Hosting, Speicherung und Modellbetrieb ein, soweit der Kunde diese Komponenten selbst bereitstellt.

Unterauftragsverarbeiter	Leistung	Einsatz	Ort der Verarbeitung	Zertifizierungen und Prüfberichte
Microsoft Ireland Operations Ltd. (Microsoft Azure)	Hosting und Speicherung der Plattform; Betrieb der Modelldienste über Azure AI Foundry	Wenn im Order Form als Hosting- bzw. Modellanbieter vereinbart (Standard beim Cloud-Dienst)	EU (Region gemäß Order Form)	ISO/IEC 27001, ISO/IEC 27017; SOC 1/2/3 (Microsoft Service Trust Portal)
Amazon Web Services EMEA SARL (AWS)	Hosting und Speicherung der Plattform; Betrieb der Modelldienste über Amazon Bedrock	Nur wenn im Order Form als Hosting- bzw. Modellanbieter vereinbart	EU (Region gemäß Order Form)	ISO/IEC 27001, ISO/IEC 27017; SOC 1/2/3 (AWS Artifact)
SNS – Saturn Networking Solutions GmbH	Hosting und Speicherung der Plattform in einem österreichischen Rechenzentrum	Nur wenn im Order Form als Hosting-Anbieter vereinbart	Österreich	ISO/IEC 27001 in Zertifizierung (laufend); weitere Nachweise auf Anfrage
Schwarz Digits GmbH & Co. KG (STACKIT)	Hosting und Speicherung der Plattform	Nur wenn im Order Form als Hosting-Anbieter vereinbart	Deutschland	ISO/IEC 27001 (auf Basis IT-Grundschutz), ISO/IEC 27017; BSI C5 Typ 2; ISAE 3000 (SOC 2), ISAE 3402
Microsoft Ireland Operations Ltd. (Microsoft 365)	Support- und Ticketkorrespondenz in der Umgebung von Mimirio	In jedem Betriebsmodell, sobald Supportkorrespondenz personenbezogene Daten enthält	EU	ISO/IEC 27001, ISO/IEC 27017; SOC 1/2/3 (Microsoft Service Trust Portal)

C1.2 Mit jedem eingesetzten Unterauftragsverarbeiter besteht eine Vereinbarung nach Art 28 Abs 4 DSGVO — bei Microsoft und AWS auf Grundlage des jeweiligen Data Processing Addendum. Die Nachweise der eingesetzten Anbieter (Punkt B1.3) stellt Mimirio auf Anfrage bereit. Modelldienste werden ausschließlich in einer Konfiguration ohne Training mit Kundendaten eingesetzt (Punkt 7).

C1.3 Änderungen dieser Liste richten sich nach Punkt 11. Weitere Dienstleister mit Zugriff auf personenbezogene Daten des Kunden werden nicht eingesetzt.

C1.4 Leistungen ohne Zugriff auf personenbezogene Daten des Kunden sind keine Auftragsverarbeitung (Punkt 11.5).