RECHTLICHES

Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung von Daten im Auftrag nach Art. 28 DSGVO, mit den Anlagen zu Unterauftragnehmern, technischen und organisatorischen Maßnahmen und Datenarten.

Stand: 30. Oktober 2026

INHALT

Präambel
1. Gegenstand und Zweck der Verarbeitung
2. Allgemeines
3. Gegenstand des Auftrags
4. Rechte und Pflichten des Auftraggebers
5. Allgemeine Pflichten des Auftragnehmers
6. Datenschutzkoordinator des Auftragnehmers
7. Meldepflichten des Auftragnehmers
8. Mitwirkungspflichten des Auftragnehmers
9. Kontrollbefugnisse
10. Unterauftragsverhältnisse
11. Vertraulichkeitsverpflichtung
12. Wahrung von Betroffenenrechten
13. Technische und organisatorische Maßnahmen
14. Dauer des Auftrags
15. Folgen der Beendigung
16. Gerichtsstand
17. Schlussbestimmungen
Anlage 1: Unterauftragnehmer
Anlage 2: Technische und organisatorische Maßnahmen (TOM)
Anlage 3: Arten personenbezogener Daten

Präambel

Dieser Vertrag über die Verarbeitung von Daten im Auftrag (Auftragsverarbeitungsvertrag, „AVV“) gilt zwischen der Prodlane GmbH, Löhrstraße 15, 04105 Leipzig, Deutschland („Auftragnehmer“), und dem Kunden, der MAIA im Rahmen seiner beruflichen, geschäftlichen oder organisatorischen Tätigkeit nutzt („Auftraggeber“). Er ergänzt die Vereinbarung über die Nutzung von MAIA („Nutzungsvertrag“) und regelt die Verarbeitung personenbezogener Daten, die der Auftragnehmer dabei im Auftrag des Auftraggebers durchführt.

Der AVV wird durch ausdrückliche Einbeziehung in ein vom Auftraggeber angenommenes Angebot, eine Bestellung oder den Nutzungsvertrag vereinbart, auch durch elektronische Annahme für den Auftraggeber, etwa bei einer Online-Bestellung. Er kann auch gesondert unterzeichnet werden. Eine gesonderte Unterzeichnung ist bei anderweitiger wirksamer Einbeziehung nicht erforderlich.

Der AVV gilt ab seiner Vereinbarung für sämtliche im Auftrag des Auftraggebers durchgeführten Verarbeitungen im Rahmen der Nutzung von MAIA, einschließlich Test- und Pilotphasen. Er ist vor Beginn dieser Verarbeitungen zu vereinbaren.

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Im Rahmen dieses Auftrags stellt der Auftragnehmer dem Auftraggeber die cloud-basierte SaaS-Lösung „MAIA“ bereit. MAIA ermöglicht die Nutzung verschiedener Sprachmodelle (LLMs) in einer datenschutzkonformen Umgebung, insbesondere den Chat mit einem KI-Assistenten, die Analyse und Durchsuchung vom Auftraggeber bereitgestellter Dokumente, die Anbindung externer Datenquellen des Auftraggebers, die Erstellung von Dateien und die Ausführung von Workflows. Den Leistungsumfang im Einzelnen regelt die Leistungsbeschreibung.

2. Allgemeines

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

2.2 Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2.3 Unterliegt die Verarbeitung für den Auftraggeber dem schweizerischen Bundesgesetz über den Datenschutz (DSG), erfüllt der Auftragnehmer die Pflichten aus diesem Vertrag auch nach Maßgabe des DSG, insbesondere nach Art. 8 DSG (Datensicherheit), Art. 9 DSG (Bearbeitung durch Auftragsbearbeiter) und Art. 16 f. DSG (Bekanntgabe ins Ausland). Verweise auf die DSGVO umfassen in diesem Fall die entsprechenden Bestimmungen des DSG. Die Genehmigung von Unterauftragnehmern nach Ziff. 10 gilt als vorgängige Genehmigung im Sinne von Art. 9 Abs. 3 DSG.

3. Gegenstand des Auftrags

3.1 Der Gegenstand der Verarbeitung bezieht sich auf sämtliche personenbezogene Daten, die der Auftraggeber dem Auftragnehmer zur Verarbeitung übergibt, insbesondere mittels Chat-Schnittstelle, Dokumenten-Upload und integrierten Schnittstellen. Übergibt der Auftraggeber solche Daten auf einem anderen Weg, insbesondere per E-Mail, über Filesharing-Dienste oder postalisch, damit der Auftragnehmer sie verarbeitet, sind sie ebenfalls Gegenstand dieses Vertrages. Im Kontext der Schnittstellen-Integration erfasst dies sowohl die von MAIA bereitgestellten als auch die vom Auftraggeber eigenentwickelten und über die Programmierschnittstelle (API) angebundenen Integrationen. Als Integration wird hierbei jegliche technische Schnittstelle verstanden, die den bidirektionalen Datenaustausch zwischen MAIA und Drittsystemen ermöglicht. Integrationen, einschließlich über das Model Context Protocol (MCP) angebundener Server, greifen auf Drittsysteme mit den Berechtigungen zu, die der Auftraggeber oder seine Nutzer erteilen, insbesondere durch Anmeldung beim Drittsystem oder durch Zustimmung eines Administrators. Lese- und Schreibvorgänge in Drittsystemen erfolgen auf Weisung des Auftraggebers (Ziff. 4.3). Betreiber von Drittsystemen, die der Auftraggeber auf Grundlage eigener Verträge nutzt und an MAIA anbindet, sind keine Unterauftragnehmer des Auftragnehmers. Für die Verarbeitung in diesen Drittsystemen ist der Auftraggeber im Verhältnis zu deren Betreibern selbst verantwortlich. Die Verarbeitung der aus Drittsystemen abgerufenen Daten in MAIA unterliegt diesem Vertrag.

3.2 Unabhängig von den durch den Auftraggeber eingebrachten Inhalten werden bei Nutzung der MAIA-Plattform durch den Auftragnehmer stets bestimmte Arten personenbezogener Daten im Auftrag des Auftraggebers verarbeitet, die für die Bereitstellung, den Betrieb und die Sicherheit der Plattform technisch oder organisatorisch erforderlich sind (insbesondere Daten zur Einrichtung und Verwaltung von

Nutzerkonten, zur Authentifizierung sowie zur Protokollierung von Zugriffen und Vorgängen). Diese Datenarten sind in Anlage 3 (Arten personenbezogener Daten) beschrieben. Der Auftragnehmer ist berechtigt, diese Anlage bei Änderungen der Plattform oder ihrer technischen Erfordernisse zu aktualisieren. Über entsprechende Aktualisierungen informiert der Auftragnehmer den Auftraggeber stets unverzüglich.

3.3 Der Auftraggeber ist dafür verantwortlich, dass die Verarbeitung der von ihm übermittelten Daten rechtmäßig ist. Das gilt auch für besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO.

3.4 Personenbezogene Daten, die im Rahmen der Anbahnung, Abwicklung und Verwaltung der Geschäftsbeziehung zwischen den Parteien anfallen, verarbeitet der Auftragnehmer als eigener Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO und nicht im Auftrag des Auftraggebers. Dazu gehören insbesondere geschäftliche Kontaktdaten der Ansprechpartner, Korrespondenz zu Support, Abrechnung, Terminen und Vertragsverwaltung sowie Status- und Störungsmeldungen. Der Auftragnehmer informiert die betroffenen Personen nach Art. 13 DSGVO und benennt die Rechtsgrundlage in seinen Datenschutzhinweisen. Enthält eine solche Kommunikation personenbezogene Daten, die der Auftraggeber zur Verarbeitung übergibt, insbesondere als Anlage, eingebettetes Bildschirmfoto oder Auszug, unterliegen diese Daten Ziff. 3.1 und damit diesem Vertrag.

4. Rechte und Pflichten des Auftraggebers

4.1 Der Auftraggeber bleibt Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 5.5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

4.2 Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

4.3 Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen erfolgen in Textform (z. B. E-Mail) oder durch die Nutzung der Konfigurationsmöglichkeiten von MAIA. Wählt der Auftraggeber in MAIA Modelle, Integrationen oder Funktionen aus oder nimmt er sonstige Einstellungen vor, gilt dies als dokumentierte Weisung im Sinne von Art. 28 Abs. 3 lit. a DSGVO.

4.4 Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

4.5 Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt oder geändert werden, werden diese vom Auftraggeber dem Auftragnehmer in Textform mitgeteilt.

4.6 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

4.7 Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

5. Allgemeine Pflichten des Auftragnehmers

5.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen.

Ausgenommen hiervon sind gesetzliche Regelungen des Rechts der Union oder der Mitgliedstaaten, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich in Textform zugestimmt hat.

5.2 Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) oder in der Schweiz durchzuführen, darüber hinaus ist die Datenverarbeitung nur zulässig mit vorheriger Zustimmung des Auftraggebers und unter Beachtung der Voraussetzungen der Art. 44 ff. DSGVO. Für Personendaten, die dem DSG unterliegen, ist eine Bekanntgabe in einen Staat außerhalb der Schweiz, der EU und des EWR nur zulässig, wenn der Bundesrat einen angemessenen Schutz festgestellt hat (Art. 16 Abs. 1 DSG) oder geeignete Garantien nach Art. 16 Abs. 2 DSG bestehen, insbesondere Standardvertragsklauseln mit den vom EDÖB anerkannten Anpassungen, oder eine Ausnahme nach Art. 17 DSG vorliegt.

5.3 Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

5.4 Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

5.5 Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt.

5.6 Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

5.7 Der Auftragnehmer benennt hiermit dem Auftraggeber die Personen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind:

- Geschäftsführung der Prodlane GmbH, compliance@getmaia.ai

5.8 Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

6. Datenschutzkoordinator des Auftragnehmers

6.1 Der externe Datenschutzbeauftragte der Prodlane GmbH ist: heyData GmbH, Schützenstraße 5, 10117 Berlin, www.heydata.eu, datenschutz@heydata.eu

6.2 Der interne Datenschutzkoordinator der Prodlane GmbH ist die Geschäftsführung, compliance@getmaia.ai

6.3 Eine Änderung des Datenschutzkoordinators oder Benennung des Datenschutzbeauftragten ist dem Auftraggeber schriftlich anzuzeigen.

7. Meldepflichten des Auftragnehmers

7.1 Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

7.2 Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

7.3 Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen, soweit es sich um die Daten handelt die von diesem für den Auftraggeber verarbeitet werden. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten: a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze; b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

8. Mitwirkungspflichten des Auftragnehmers

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 12 dieses Vertrages.

8.2 Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit, soweit es die Daten die durch ihn verarbeitet werden, betrifft. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geei gneter Weise mitzuteilen.

8.3 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

9. Kontrollbefugnisse

9.1 Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer mit Abstimmung durch den Auftragnehmer jederzeit im erforderlichen und angemessenen Umfang zu kontrollieren.

9.2 Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

9.3 Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

9.4 Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

9.5 Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

10. Unterauftragsverhältnisse

10.1 Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in Anlage 1 (Unterauftragnehmer) zu diesem Vertrag angeben.

10.2 Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann.

10.3 Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt w orden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.

10.4 Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

10.5 Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

10.6 Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 9 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

10.7 Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-Systemen oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogene Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

10.8 Der Auftragnehmer ist berechtigt, weitere Unterauftragsverarbeiter einzusetzen oder bestehende zu ersetzen („allgemeine Genehmigung“ i.S.d. Art. 28 Abs. 2 DSGVO). Der Auftragnehmer informiert den Auftraggeber mindestens 14 Kalendertage vor dem beabsichtigten Einsatz oder Austausch per E-Mail und durch Aktualisierung der Liste in Anlage 1 (Unterauftragnehmer). Der Auftraggeber kann innerhalb von 14 Kalendertagen nach Zugang der Mitteilung aus angemessenen, datenschutzbezogenen Gründen Einspruch erheben. Rein wirtschaftliche oder technische Gründe genügen nicht.

10.9 Nach Eingang eines Einspruchs prüft der Auftragnehmer zumutbare Alternativen (z. B. alternative Verarbeitung, Deaktivierung betroffener Funktionen, anderer Unterauftragnehmer, andere Region), soweit technisch und wirtschaftlich vertretbar. Ist keine zumutbare Alternative verfügbar, ist das ausschließliche Rechtsmittel des Auftraggebers, die betroffene Leistung mit Wirkung zum Änderungsdatum ohne Vertragsstrafe zu kündigen. Bereits vorausbezahlte Entgelte für die betroffene Leistung werden zeitanteilig erstattet.

10.10 Ist der sofortige Austausch eines Unterauftragsverarbeiters zwingend erforderlich (z. B. zur Aufrechterhaltung der Sicherheit oder Verfügbarkeit), darf der Auftragnehmer den Austausch kurzfristig vornehmen und informiert den Auftraggeber unverzüglich. Die Rechte nach Absatz 10.8 und 10.9 gelten entsprechend.

11. Vertraulichkeitsverpflichtung

11.1 Die Parteien sind bei der Verarbeitung von Daten für den jeweiligen anderen Vertragspartner zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Die Parteien verpflichten sich, die gleichen Geheimnisschutzregeln zu beachten, wie der offenbarenden Partei obliegen. Die Parteien verpflichten sich dem jeweils anderen Vertragspartner etwaige besondere Geheimnisschutzregeln mitzuteilen.

11.2 Die Parteien sichern zu, dass ihnen die jeweils gesetzlich geltenden datenschutzrechtlichen Vorschriften bekannt sind und sie mit der Anwendung dieser vertraut sind. Die Parteien sichern ferner zu, dass sie die Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet haben. Die Parteien sichern weiter zu, dass sie insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet haben und diese über die Weisungen der jeweils anderen Partei informiert haben.

11.3 Die Verpflichtung der Beschäftigten nach Absatz 2 ist dem Auftraggeber auf Anfrage nachzuweisen.

12. Wahrung von Betroffenenrechten

12.1 Der Auftraggeber übernimmt trotz der Übertragung der Datenverarbeitung Verantwortung für die Betroffenenrechte. Der Auftragnehmer wird dennoch mitunter verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

12.2 Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung – durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

13. Technische und organisatorische Maßnahmen

13.1 Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

13.2 Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 2 (Technische und organisatorische Maßnahmen) zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

13.3 Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

14. Dauer des Auftrags

14.1 Der Vertrag beginnt mit Abschluss und wird auf unbestimmte Zeit geschlossen.

14.2 Eine ordentliche Kündigung dieses Vertrages ist ausgeschlossen, solange der Auftragnehmer im Rahmen des Nutzungsvertrags oder einer Erprobung personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Der Vertrag endet automatisch, sobald Nutzungsvertrag und Erprobung beendet sind. Seine Pflichten gelten fort, bis die Daten nach Ziff. 15 zurückgegeben oder gelöscht sind.

14.3 Die Parteien können den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß gegen die anzuwendenden Datenschutzvorschriften, gegen Pflichten aus diesem Vertrag oder ähnlichen Pflichten vorliegt, insbesondere kann der Auftraggeber kündigen, wenn der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert. Die Kündigung aus wichtigem Grund ist ausgeschlossen, wenn der Kündigungsgrund aus der Sphäre des Auftraggebers rührt. In diesen Fällen ist vielmehr der Auftragnehmer berechtigt im Sinne dieses Absatzes zu kündigen.

15. Folgen der Beendigung

15.1 Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Rückgabe oder Löschung erfolgt innerhalb von 30 Tagen nach Beendigung des Vertrages, soweit der Auftraggeber keine längere Aufbewahrung anweist oder ein längerer Abrufzeitraum gesetzlich vorgesehen ist, etwa beim Anbieterwechsel nach Kapitel VI der Verordnung (EU) 2023/2854 (Data Act). Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei sicherzustellen ist, dass die Daten gänzlich unbrauchbar gemacht werden. Die Vernichtung ist zu protokollieren. Kopien in

Sicherungssystemen werden im Rahmen der regulären Rotation spätestens 100 Tage nach der Löschung im Produktivsystem gelöscht. Bis dahin werden sie ausschließlich zur Wiederherstellung vorgehalten.

15.2 Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

16. Gerichtsstand

Es gilt deutsches Recht, einschließlich der DSGVO. Ausschließlicher Gerichtsstand bei Streitigkeiten aus diesem Vertrag ist Leipzig. Zwingende Bestimmungen des DSG bleiben unberührt.

17. Schlussbestimmungen

17.1 Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

17.2 Mündliche Nebenabreden sind bis zum Vertragsschluss zwischen den Parteien nachweislich nicht getroffen worden.

17.3 Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

17.4 Rechtlich verbindlich ist ausschließlich die deutsche Fassung dieses Vertrags. Eine englische Übersetzung dient ausschließlich Informationszwecken.

Anlage 1: Unterauftragnehmer

Übersicht der Unterauftragnehmer. Maßgeblich sind die ausführlichen Einträge darunter.

UNTERAUFTRAGNEHMER	LEISTUNGEN	VERARBEITUNGSORT	ÜBERMITTLUNGSMECHANISMUS
Hetzner Online GmbH	Cloud-Infrastruktur und Hosting der Plattform, einschließlich GPU-Inferenz	EU	Nicht erforderlich (Verarbeitung in der EU)
Microsoft Azure	Cloud-Infrastruktur und KI-Dienste, einschließlich LLMs	EU	Nicht erforderlich (Verarbeitung in der EU)
Amazon AWS	Cloud-Infrastruktur und KI-Dienste, einschließlich LLMs	EU	Nicht erforderlich (Verarbeitung in der EU)
Google Cloud	Cloud-Infrastruktur und KI-Dienste, einschließlich LLMs	EU	Nicht erforderlich (Verarbeitung in der EU)
AKI.IO GmbH	Bereitstellung von LLMs zur Nutzung in der Plattform	Deutschland	Nicht erforderlich (Verarbeitung in der EU)

UNTERAUFTRAGNEHMER	LEISTUNGEN	VERARBEITUNGSORT	ÜBERMITTLUNGSMECHANISMUS
PostHog	Produktanalyse auf Basis pseudonymisierter Nutzungs- und Ereignisdaten	EU	EU-US Data Privacy Framework; EU-Standardvertragsklauseln (Modul 2)

Hetzner Online GmbH

- **Anbieter:** Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland
- **Datenschutzkontakt:** data-protection@hetzner.com

Der Auftragnehmer bezieht von Hetzner eine umfangreiche Infrastruktur, bestehend aus mehreren Servern, Netzwerken und Load Balancing. In dieser Umgebung sind die Hauptserver aktiv, die sowohl die MAIA-Webanwendung bereitstellen als auch die Daten sicher speichern.

Die Hauptinfrastruktur befindet sich in der EU. Backups und Snapshots werden in ein zweites Rechenzentrum in der EU repliziert.

- **Verarbeitungsort:** EU
- **Übermittlungsmechanismus:** Nicht erforderlich (Verarbeitung in der EU)
- **DSGVO-Vereinbarungen:**
  - AVV: Hetzner: Vertrag zur Auftragsverarbeitung

Microsoft Azure

- **Anbieter:** Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland
- **Datenschutzkontakt (Europa):** Microsoft Ireland Operations Limited, z. Hd. Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland; Telefon: +353 1 706 3117; Kontaktformular

Microsoft Azure stellt dem Auftragnehmer GPT in einer datenschutzkonformen Umgebung bereit. Die GPT-Modelle werden als Deployments vom Typ DataZone EU genutzt, sodass Prompts und Ausgaben ausschließlich in der EU verarbeitet werden. Die verarbeiteten Daten werden nicht zum Training von KI-Modellen verwendet.

Zusätzlich stellt Microsoft dem Auftragnehmer dedizierte Server bereit, die speziell für den Betrieb von KI-Modellen ausgelegt sind. Diese Server werden in der EU betrieben und dienen ausschließlich der Vorverarbeitung von Dokumenten.

- **Verarbeitungsort:** EU (Azure-OpenAI-Deployments vom Typ DataZone EU)
- **Übermittlungsmechanismus:** Nicht erforderlich (Verarbeitung in der EU)
- **DSGVO-Vereinbarungen:**
  - Standardvertragsklauseln: Microsoft: Standardvertragsklauseln der Europäischen Union
  - AVV: Microsoft Products and Services Data Protection Addendum (DPA)

Amazon AWS

- **Anbieter:** Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg
- **Datenschutzkontakt (Europa):** Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg; Datenschutzbeauftragter: aws-EU-privacy@amazon.com

Amazon AWS stellt dem Auftragnehmer Large Language Models in einer datenschutzkonformen Umgebung bereit. Die zugehörigen Infrastrukturen werden ausschließlich in Europa betrieben.

Die verarbeiteten Daten werden nicht zum Training von KI-Modellen verwendet.

- **Verarbeitungsort:** EU (Amazon Bedrock EU Cross-Region Inference)
- **Übermittlungsmechanismus:** Nicht erforderlich (Verarbeitung in der EU)
- **DSGVO-Vereinbarungen:**
  - AVV: AWS Data Processing Addendum (DPA)

Google Cloud

- **Anbieter:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Dublin, Irland
- **Datenschutzkontakt:** Cloud Data Protection Team, Kontaktformular

Google Cloud stellt dem Auftragnehmer Large Language Models in einer datenschutzkonformen Umgebung bereit. Die zugehörigen Infrastrukturen werden ausschließlich in Europa betrieben.

Die verarbeiteten Daten werden nicht zum Training von KI-Modellen verwendet.

- **Verarbeitungsort:** EU
- **Übermittlungsmechanismus:** Nicht erforderlich (Verarbeitung in der EU)
- **DSGVO-Vereinbarungen:**
  - AVV: Google Cloud Data Processing Addendum

AKI.IO GmbH

- **Anbieter:** AKI.IO GmbH, Marienburger Str. 1, 10405 Berlin, Deutschland
- **Datenschutzkontakt:** privacy@aki.io

AKI.IO stellt dem Auftragnehmer Large Language Models in einer datenschutzkonformen Umgebung bereit. Die zugehörigen Infrastrukturen werden ausschließlich in Europa betrieben.

Die verarbeiteten Daten werden nicht zum Training von KI-Modellen verwendet.

- **Verarbeitungsort:** Deutschland, eigene GPU-Server in Co-Location-Rechenzentren
- **Übermittlungsmechanismus:** Nicht erforderlich (Verarbeitung in der EU)

PostHog

- **Anbieter:** PostHog Inc., 2261 Market Street #4008, San Francisco, CA 94114, USA
- **Datenschutzkontakt:** privacy@posthog.com

Der Auftragnehmer nutzt PostHog für die technische Analyse des Betriebs, von Fehlern und der Performance seiner Webanwendungen. PostHog ermöglicht datenschutzkonformes Tracking und Echtzeitanalysen. PostHog erhält keine Prompts, Modellausgaben oder Dokumentinhalte. Ereignisse werden pseudonymisiert: Sie sind mit einer internen Nutzer-ID verknüpft, nicht mit Namen oder E-Mail-Adressen.

Die erhobenen Daten werden ausschließlich für die technische Analyse des Betriebs, von Fehlern und der Performance der MAIA-Plattform verwendet.

Zur Einhaltung der DSGVO-Anforderungen nutzt der Auftragnehmer ausschließlich PostHog Cloud EU, die in der EU betrieben wird.

- **Verarbeitungsort:** EU
- **Übermittlungsmechanismus:** PostHog Inc. hat ihren Sitz in den USA: EU-US Data Privacy Framework (PostHog ist selbstzertifiziert); zusätzlich EU-Standardvertragsklauseln (Modul 2) im Rahmen des Auftragsverarbeitungsvertrags mit PostHog vom 6. Januar 2025

- DSGVO-Konformität:
  - PostHog Cloud EU
  - PostHog: DSGVO-Konformität

Anlage 2: Technische und organisatorische Maßnahmen (TOM)

1. Vertraulichkeit

1.1 Zutrittskontrolle

Technische Maßnahmen

- Mechanische Schließanlage für die Büroräume
- Schlüssel nur für autorisierte Personen

Organisatorische Maßnahmen

- Schlüsselregister mit dokumentierter Ausgabe und Rückgabe
- Besucherregister
- Richtlinie zum Umgang mit Besuchern
- Besucher in Begleitung von Mitarbeiter
- Regelmäßige Schulung und Bewusstseinsbildung
- Regelungen für sicheres Arbeiten in Büro und Remote Work Umgebungen
- Regelmäßige Überprüfung physischer Zutrittsberechtigungen

Wir vertrauen auf Cloud-Provider für den Betrieb unserer IT-Infrastruktur und die Bereitstellung von Systemen zur Verarbeitung personenbezogener Daten. Wir betreiben keine internen Serveranlagen im Büro.

1.2 Zugangskontrolle

Technische Maßnahmen

- Einsatz individueller Benutzerkonten
- Login mit Benutzername und Passwort
- Zentral verwaltete Endgeräte mit Virenschutz, Festplattenverschlüsselung und Passwortvorgaben
- Firewall auf Client, Server und Cloud Level
- Verschlüsselung von Datenträgern
- Automatische Desktopsperre
- Verschlüsselung von Clients
- Verpflichtender Einsatz von unternehmenseigenen VPN bei mobilen Arbeiten
- MFA (2FA) Richtlinien
- Verpflichtender Einsatz des zentral verwalteten Passwort-Manager
- Principle of least privilege
- Sperrung oder Entzug von Zugängen bei Austritt oder Rollenwechsel
- Schutz von Zugangsdaten durch definierte Passwortanforderungen
- Zugriff auf sensible Systeme nur über freigegebene und abgesicherte Verbindungen
- Unternehmensverwaltete Laptops und Workstations, inkl. Sicherheitsvorgaben
- Zugriff auf Unternehmensdaten nur von freigegebenen oder konformen Geräten

Organisatorische Maßnahmen

- Passwort Richtlinien
- Löschen / Vernichtung Richtlinien
- Clean Desk Richtlinie
- Clean Office Richtlinie
- Desktop und Mobile Sperre Richtlinie
- Schulungen und Bewusstseinsbildung
- Onboarding Verfahren für die Anlage neuer Zugänge
- Offboarding Verfahren für den Entzug nicht mehr erforderlicher Zugänge
- Regelmäßige Überprüfung von Berechtigungen und Zugängen

1.3 Zugriffskontrolle

Technische Maßnahmen

- Aktenvernichter (P4, crosscut)
- IAM-Systeme
- Verschlüsselung von Daten bei Übertragung und Speicherung
- Principle of least privilege
- Der Verwaltungszugriff auf Produktivsysteme ist ausschließlich über eine gesicherte VPN Verbindung zulässig
- Nicht-konsolenbasierter Zugriff auf die Produktivinfrastruktur nur mit individuellem SSH-Schlüssel oder Zugriffsschlüssel
- Rollenbasierte Vergabe von Berechtigungen
- Beschränkung privilegierter Zugriffe auf besonders autorisierte Personen
- Nachvollziehbarkeit administrativer Zugriffe über individuelle Konten
- Zugriffsbeschränkungen auf besonders schutzbedürftige Daten und Systeme
- Gesicherte Verwaltung gemeinsam genutzter Konten über den Passwort Manager, soweit solche Ausnahmen erforderlich sind

Organisatorische Maßnahmen

- Minimale Anzahl an Administratoren
- Verwaltung von Benutzerrechten durch Administratoren
- Regelmäßige Access Reviews für sensible und kritische Systeme
- Dokumentierte Freigabe für erhöhte Berechtigungen
- Rechtevergabe nach need-to-know und least-privilege
- Dokumentierte Änderung von Zugriffsrechten bei Rollenwechsel

1.4 Trennungskontrolle

Technische Maßnahmen

- Trennung von Produktiv-, Entwicklungs-und Testsystemen
- Trennung von Daten nach Zweck und Berechtigung
- Logische Trennung von Umgebungen und Rollen
- Einschränkung der Nutzung produktiver Daten in Test und Entwicklungsumgebungen
- Schutz gemeinsam genutzter Speicherbereiche durch Berechtigungen und Rollen

Organisatorische Maßnahmen

- Festlegung von Datenbankrechten
- Regelungen zur Nutzung von Testdaten
- Freigabe nur erforderlicher Daten für definierte Zwecke
- Verantwortlichkeiten für Datenfreigaben und Umgebungstrennung

1.5 Pseudonymisierung

Technische Maßnahmen

- Pseudonymisierung in externen Systemen, soweit der Zweck der Verarbeitung dies zulässt
- Pseudonymisierung in Logs
- Trennung von Zuordnungsdaten in getrennt abgesicherten Systemen

Organisatorische Maßnahmen

- Richtlinie, dass bei manueller Weitergabe Daten zu pseudonymisieren sind, so dass eine Zuordnung nicht möglich ist

2. Integrität

2.1 Weitergabekontrolle

Technische Maßnahmen

- Nutzung freigegebener und abgesicherter Kommunikationssysteme
- Verschlüsselte Übertragung vertraulicher Informationen über öffentliche Netze
- Zusätzliche Schutzmaßnahmen bei externer Übermittlung sensibler Daten
- Beschränkung unsicherer Übertragungswege

Organisatorische Maßnahmen

- Weitergabe in anonymisierter oder pseudonymisierter Form, soweit der Zweck der Weitergabe dies zulässt
- Weitergabe nur an berechtigte Empfänger
- Vorgaben zur sicheren externen Übermittlung von Dateien und Informationen
- Keine Übermittlung von Zugangsdaten oder sensiblen Informationen über ungeschützte Kanäle
- Prüfung der Erforderlichkeit vor externer Weitergabe

2.2 Eingabekontrolle

Technische Maßnahmen

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Manuelle Kontrolle der Protokolle
- Zentrale Sammlung oder Auswertung von Logs, soweit vorgesehen
- Alarmierung bei kritischen sicherheitsrelevanten Ereignissen, soweit vorgesehen
- Protokollierung von administrativen Tätigkeiten auf kritischen Systemen
- Überwachung des Netzwerkverkehrs zur Produktivumgebung durch Sicherheitswerkzeuge

Organisatorische Maßnahmen

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Klare Zuständigkeiten für Löschungen
- Regelmäßige Überprüfung relevanter Protokolle
- Dokumentierte Zuständigkeiten für Monitoring und Incident Bearbeitung
- Dokumentierte Freigabe und Prüfung von risikobehafteten Änderungen an Produktivsystemen
- Richtlinie zur sicheren Softwareentwicklung
- Change-Management-Verfahren: Änderungen an Systemen, Netzwerk, Sicherheitseinstellungen und Infrastruktur werden dokumentiert, getestet und freigegeben
- Konfigurations- und Asset-Management für neue und sensible Systeme

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Technische Maßnahmen

- Feuer- und Rauchmeldeanlagen
- Regelmäßige, automatische Backups und Snapshots
- Sichere Speicherung von Backups und Sicherungsdaten
- Backup Verfahren für produktive Daten, Konfigurationen und relevante Dokumentationen
- Überwachung kritischer Systeme und Services
- Automatisierte Überwachung von Verfügbarkeit und Erreichbarkeit
- Hochverfügbare Auslegung der Systeme, soweit sinnvoll
- Schutzmaßnahmen gegen Schadsoftware und sicherheitsrelevante Störungen
- Maßnahmen zur zeitnahen Wiederherstellung der Verfügbarkeit bei Zwischenfällen
- Remote Lock und Remote Wipe für verlorene oder gestohlene mobile Endgeräte

Organisatorische Maßnahmen

- Backup & Recovery-Konzept
- Kontrolle des Sicherungsvorgangs
- Backups werden getrennt von Serverstandorten aufbewahrt
- Getrennte Partitionen für Betriebssysteme und Daten
- Wiederherstellung von Backups in einer Nicht-Produktivumgebung mindestens jährlich, um ihre Integrität zu prüfen
- Verfahren zur Behandlung von Systemausfällen und Sicherheitsvorfällen
- Business Continuity und Disaster Recovery Verfahren
- Regelmäßiger Test des Business-Continuity- und Disaster-Recovery-Plans, etwa durch Planspiele, mit Anpassung des Plans bei Bedarf
- Definition von Zuständigkeiten für Wiederanlauf und Wiederherstellung
- Dokumentation und Nachverfolgung von Störungen und Wiederherstellungsmaßnahmen

4. Datenschutz-Maßnahmen

4.1 Datenschutzmaßnahmen

Technische Maßnahmen

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (Confluence)
- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
- Dokumentierte Klassifizierung, Aufbewahrung und Löschung von Daten
- Dokumentierte Regeln zur sicheren Entsorgung und Datenvernichtung
- Penetrationstest der Netzwerk- und Anwendungsebene der Produktivumgebung durch einen externen Dienstleister mindestens jährlich; kritische und hohe Befunde werden bis zur Behebung nachverfolgt

Organisatorische Maßnahmen

- Interner Datenschutzkoordinator (Geschäftsführung); externer Datenschutzbeauftragter: heyData GmbH (Ziff. 6.1)
- Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
- Monatliche Schulungen und Bewusstseinsbildung:
  - Sensibilisierung
  - Besprechung von neuen bzw. geänderten Richtlinien
  - Informationen über potenzielle Bedrohungen
  - Allgemeiner Wissenstransfer in Bezug auf Datenschutz und Datensicherheit
  - Besprechung, wie unsere Prozesse weiter verbessert werden können
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
- Regelmäßige Überprüfung der Angemessenheit wesentlicher Schutzmaßnahmen
- Informationssicherheitsrichtlinie und interne Kontrollrichtlinie; die Geschäftsführung überprüft alle Sicherheitsrichtlinien mindestens jährlich
- Formale Risikobewertung mindestens jährlich, mit einem Risikoregister und Maßnahmen zur Risikobehandlung
- Organigramm mit klaren Zuständigkeiten und Kommunikationswegen
- Arbeitsrechtliche Konsequenzen bei Verstößen gegen Sicherheitsrichtlinien

4.2 Incident-Response-Management

Technische Maßnahmen

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Unterstützung der Incident Bearbeitung durch Protokollierung und Nachvollziehbarkeit
- Einheitlicher Informationsweg ggü Kunden
- Maßnahmen zur Eindämmung, Untersuchung und Wiederherstellung nach Sicherheitsvorfällen
- Technische Schutzmaßnahmen für den Umgang mit verlorenen oder kompromittierten Geräten

Organisatorische Maßnahmen

- Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Dokumentierte Rollen und Verantwortlichkeiten im Incident Response Prozess
- Dokumentierte Eskalations und Kommunikationswege
- Nachbereitung von Sicherheitsvorfällen und Ableitung von Verbesserungsmaßnahmen

- Dokumentierte Behandlung von Geräteverlusten, unberechtigten Zugriffen und Datenschutzverletzungen
- Transparente externe Kommunikation über eine Status Page, auf der Kunden aktuelle Systemausfälle, betroffene Services, Fortschritte bei der Störungsbehebung und den Abschluss des Vorfalls nachvollziehen können
- Regelmäßiger Test des Incident-Response-Plans, etwa durch Planspiele, mit Anpassung des Plans bei Bedarf

4.3 Datenschutzfreundliche Voreinstellungen

Technische Maßnahmen

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen
- Privacy by Design
- Technische Begrenzung von Datenzugriffen nach Rolle und Zweck
- Standardmäßige datenschutzfreundliche Konfigurationen bei Systemen und Prozessen
- Beschränkung von Speicherorten und Übertragungswegen für personenbezogene Daten
- Vorgaben für die Nutzung verwalteter Speicherorte und Anwendungen

4.4 Auftragskontrolle (Outsourcing an Dritte)

Organisatorische Maßnahmen

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
- Bei längerer Zusammenarbeit laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
- Risikobasierte Einstufung von Dienstleistern vor Beauftragung
- Einholung und Prüfung geeigneter Nachweise zu Datenschutz und Informationssicherheit, etwa SOC-2- oder ISO-27001-Berichte, mindestens jährlich
- Dokumentierte Überwachung kritischer oder besonders risikobehafteter Dienstleister
- Regelungen für Beendigung der Zusammenarbeit und Rückgabe oder Löschung von Daten
- Benennung interner Ansprechpartner für die Steuerung von Dienstleistern

Anlage 3: Arten personenbezogener Daten

Betroffene Personen:

1. MAIA-Nutzer
2. Personen, auf die in Dokumenten und Datenquellen von MAIA-Nutzern verwiesen wird

Nutzerdaten:

- Vorname
- Nachname
- E-Mail-Adresse
- Bevorzugte Softwaresprache

Dokumentinhalte:

- Textinhalte
- Bildinhalte
- Dokumenttitel
- Dokumentmetadaten (Erstellungsdatum, Autor usw.)

Suchanfragen und Chatnachrichten:

- Text der Suchanfragen
- Inhalt der Chatnachrichten

Authentifizierung und Nutzerverwaltung:

- Zeitstempel der Anmeldung
- Zeitstempel der Abmeldung
- Zeitstempel der Token-Aktualisierung
- Zeitstempel des Token-Widerrufs
- Bestätigung der Nutzer-E-Mail-Adresse
- Aktionen zum Zurücksetzen des Passworts
- Registrierungsdaten der Nutzer

Analyse- und Auditdaten (nicht anonymisiert):

- IP-Adressen bei Authentifizierungsvorgängen

Analyse- und Auditdaten (pseudonymisiert):

- Browsertyp und -version
- Gerätetyp
- Betriebssystem und -version
- Erste und aktuelle Referrer-URLs
- Ereignisprotokolle der Softwarenutzung