Auftragsverarbeitungsvertrag

Diese Vereinbarung wird geschlossen zwischen der AI Mapping GmbH, Rolshover Kirchweg 62b, 51105 Köln (nachfolgend „Auftragnehmer“ genannt) und dem im Hauptvertrag bezeichneten Kunden (nachfolgend „Auftraggeber“ genannt)

1. Allgemeines

(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) 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. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 3 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte im Zusammenhang mit dieser Verarbeitung von Daten im Auftrag gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

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

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

(6) 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.

4. Allgemeine Pflichten des Auftragnehmers

(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, 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 zugestimmt hat.

(2) Der Auftragnehmer wird die Datenverarbeitung im Auftrag grundsätzlich in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchführen. Dem Auftragnehmer ist eine Datenverarbeitung auch außerhalb von EU oder EWR erlaubt, wenn entsprechende Unterauftragnehmer im Drittland unter Einhaltung der Voraussetzungen von Ziff. 10 eingesetzt werden und die Voraussetzungen der Art. 44-48 DSGVO erfüllt sind bzw. eine usnahme i.S.d. Art. 49 DSGVO vorliegt.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

6. Meldepflichten des Auftragnehmers

(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.

(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.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht im Falle von Datenschutzverletzungen 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. 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:

- 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;
- 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.

7. Mitwirkungspflichten des Auftragnehmers

(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.

(2) Der Auftragnehmer unterstützt ggf.. bei der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(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.

8. Regelung zu mobilen Arbeitsplätzen

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen außerhalb der Geschäftsräume des Auftragnehmers erlauben.

(2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch bei der Nutzung von mobilen Arbeitsplätzen der Beschäftigten des Auftragnehmers gewährleistet ist. Abweichungen von einzelnen vertraglich vereinbarten technischen und organisatorischen Maßnahmen sind vorab mit dem Auftraggeber abzustimmen und von diesem in Textform zu genehmigen.

(3) Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen soweit möglich ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere am Ort des jeweiligen mobilen Arbeitsplatzes befindliche Personen keinen Zugriff auf diese Daten erhalten.

(4) Der Auftragnehmer ist verpflichtet, Sorge dafür zu tragen, dass eine wirksame Kontrolle der Verarbeitung personenbezogener Daten im Auftrag an mobilen Arbeitsplätzen durch den Auftraggeber möglich ist.

(5) Sofern auch bei Unterauftragnehmern Beschäftigte an mobilen Arbeitsplätzen eingesetzt werden sollen, gelten die Regelungen der Absätze 1 bis 4 entsprechend.

9. Kontrollbefugnisse

(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 jederzeit im erforderlichen Umfang zu kontrollieren.

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

(3) 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. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenen Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.

(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 3 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments i.S.d. Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.

(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.

(6) Die Parteien sind sich darüber einig, dass die Kontrollmaßnahmen bei einer Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen zur Wahrung der Persönlichkeitsrechte von weiteren Personen an diesen mobilen Arbeitsplätzen primär durch eine Kontrolle der Sicherstellung der vom Auftragnehmer nach Ziff. 9 Abs. 2 und 3 zu treffenden Maßnahmen erfolgt. Anlassbezogen ist dem Auftraggeber auch eine Kontrolle des mobilen Arbeitsplatzes von Beschäftigten durch den Auftragnehmer zu ermöglichen.

10. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, die in der **Anlage 2** zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 2 genannten Voraussetzungen zulässig.

(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. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen 2 Wochen nach Zugang der „Information“ zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information“ erfolgt, gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat, sofern der Unterauftragnehmer zur Benennung eines Datenschutzbeauftragten gesetzlich verpflichtet ist.

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

(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 Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(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.

(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-System 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 personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

11. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

(2) Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

12. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. 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.

(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.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

13. Vergütung

Etwaige Regelungen zu einer Vergütung von Leistungen sind zwischen den Parteien gesondert zu vereinbaren.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(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.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** 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.

15. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

16. Beendigung

(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 Löschung ist in geeigneter Weise zu dokumentieren.

(2) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

17. Schlussbestimmungen

(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.

(2) Für Nebenabreden ist die Schriftform erforderlich.

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

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag.

Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Zusammenhang mit der Bereitstellung einer KI-gestützten Softwarelösung („Reiner AI“) zur Analyse, Verarbeitung, Strukturierung und Auswertung von Dokumenten und Texteingaben.

Die Leistungen umfassen insbesondere:

- Bereitstellung eines webbasierten KI-Chat-Systems,
- Verarbeitung von vom Auftraggeber bereitgestellten Text-, Dokumenten- und Audiodaten,
- Analyse und Extraktion von Inhalten aus technischen Dokumenten (z. B. Leistungsverzeichnissen, Verträgen, Planunterlagen, Normen),
- Erstellung von Zusammenfassungen, Bewertungen, Prüfvermerken und strukturierten Ausgaben,
- semantische Suche und Vektorisierung von Inhalten (Embedding-Verarbeitung),
- Bereitstellung technischer Funktionen zur Dokumentenkonvertierung und -anzeige,
- Monitoring, Protokollierung und technische Fehleranalyse zur Sicherstellung des Systembetriebs.

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zum Zweck der Durchführung des Hauptvertrages, insbesondere zur Bereitstellung der vereinbarten Softwarefunktionalitäten, zur Bearbeitung von Nutzeranfragen sowie zur Sicherstellung der Stabilität, Sicherheit und Weiterentwicklung der Plattform.

Eine Nutzung der Daten zu Trainings- oder Modellverbesserungszwecken von KI-Systemen erfolgt nicht, sofern nicht ausdrücklich anderweitig vertraglich vereinbart.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind Gegenstand dieses Auftrags:

Bestands- und Kontaktdaten

- Vor- und Nachname
- E-Mail-Adresse
- Telefonnummer
- Arbeitgeber / Unternehmenszugehörigkeit
- Funktion / Position
- Rollen- und Berechtigungszuweisungen innerhalb der Anwendung

Authentifizierungs- und Zugangsdaten

- Authentifizierungsdaten (z. B. Passwort-Hash)
- Login-Informationen
- Nutzer-IDs und organisationsbezogene Kennungen

Kommunikations- und Inhaltsdaten

- Chat-Verläufe und Chat-Inhalte
- Nachrichtenhistorien
- Support-Tickets und sonstige Korrespondenz
- Angaben zur Problembeschreibung und -lösung

Dokumenten- und Uploaddaten

- Vom Auftraggeber oder dessen Nutzern hochgeladene Dokumente und Dateien
- In diesen enthaltene personenbezogene Daten (z.B. Namen, Kontaktdaten, projektbezogene Angaben)

Nutzungsdaten

- Zugriffszeiten
- Interaktions- und Aktivitätsdaten innerhalb der Anwendung
- Technische Protokoll- und Gerätedaten
- IP-Adresse
- Browser-Typ

Geräte- und Systeminformationen

- API-Aufrufe
- Server-Logs, Fehlerprotokolle und Traces

Audio- und Sprachdaten (sofern genutzt)

- Sprachaufzeichnungen
- daraus erzeugte Transkripte
- technische Metadaten zur Verarbeitung

Eine Verarbeitung besonderer Kategorien personenbezogener Daten (bspw. Gesundheitsdaten, Daten über die rassische / ethnische Herkunft) ist im Rahmen des Auftragsverarbeitungsverhältnisses nicht vorgesehen.

3. Kategorien betroffener Person

Folgende Kreise von Betroffenen sind Gegenstand des Auftrags:

- Mitarbeitende des Auftraggebers/des Verantwortlichen
- Kunden, Lieferanten und sonstige Geschäftspartner des Auftraggebers/des Verantwortlichen (soweit deren Daten durch den Auftraggeber in der Anwendung verarbeitet oder in Dokumenten/Chat-Inhalten bereitgestellt werden)

Anlage 2 - Unterauftragnehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

Subunternehmer	**Adresse**	**Gegenstand der Beauftragung**	**Datenübermittlung in Drittstaaten (Rechtsgrundlage)**
AWS (Amazon Web Services EMEA SARL)	Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855, Luxemburg	Cloud-Hosting und IT-Infrastruktur; KI-Modelldienste über AWS Bedrock zur Verarbeitung von Text- und Audiodaten sowie Vektorisierung	Serverstandort in der EU (Region eu-central-1, Frankfurt am Main, Deutschland).
Functional Software, Inc. (Sentry)	Functional Software, Inc., 45 Fremont Street, 8th Floor, San Francisco, CA 94105	Fehler- und Performance-Monitoring (Logs und Traces)	Serverstandort ist in der EU gemäß gewählter Hosting-Region. Functional Software ist unter dem EU-US-Data Privacy Framework zertifiziert (Angemessenheitsbeschluss gemäß Art. 45 DSGVO).
Google Cloud EMEA Limited	Google Cloud EMEA Limited, 70 Sir John Rogerson’s Quay, Dublin 2, Irland	API-basierte KI-Modelldienste (z.B. Gemini)	Serverstandort ist in der EU-Region gemäß Google Cloud-Konfiguration.
Intercom R&D Unlimited Company	Intercom R&D Unlimited Company, 124 St Stephen's Green, Dublin 2, DC02 C628, Ireland	Kundenkommunikations- und Support-Plattform	Datenverarbeitung erfolgt in der EU.

LangChain, Inc.	LangChain, Inc., 2261 Market Street, STE 22961, San Francisco, California 94114, United States	Monitoring- & Observability Tool für KI-Anwendungen	Serverstandort ist in der EU gemäß gewählter Hosting-Region (LangSmith EU Cloud). Die etwaige Übermittlung basiert auf abgeschlossenen EU-Standardvertragsklauseln (Art. 46 DSGVO).
Lunaweb GmbH	Lunaweb GmbH, Nördliche Münchner Straße 47, 82031 Grünwald, Deutschland	Dateikonvertierungsdienste (sofern personenbezogene Daten hochgeladen werden)	Die Datenverarbeitung erfolgt innerhalb der EU.
Meili SAS (Meilisearch)	Meili SAS, 52 Boulevard de Sébastopol, 75003 Paris, Frankreich	Such-/Indexierungsdienst, Search API (sofern personenbezogene Daten hochgeladen werden)	Die Datenverarbeitung erfolgt innerhalb der EU.
OpenAI Ireland Ltd	OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland	API-basierte KI-Modelldienste zur Verarbeitung von Text- und Audiodaten sowie Vektorisierung	Serverstandort ist in der EU gemäß gewählter Hosting-Region (EU Data Residency).
Microsoft Ireland Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	KI-Modelldienste zur Verarbeitung von Text- und Audiodaten sowie Vektorisierung	Serverstandort ist in der EU.
PostHog, Inc.	PostHog, Inc., 2261 Market Street Suite 4008, San Francisco,	Produktanalyse- und Feature-	Serverstandort ist in der EU gemäß gewählter

	CA 94114, United States	Management Plattform	Hosting-Region (EU-Cluster). PostHog ist unter dem EU-US-Data Privacy Framework zertifiziert (Angemessenheitsbeschluss gemäß Art. 45 DSGVO).
Qdrant Solutions GmbH	Qdrant Solutions GmbH, Chausseestraße 86, 10115 Berlin	Vektor-Datenbankdienste	Die Datenverarbeitung erfolgt innerhalb der EU.
Sinch AB (Mailgun)	Lindhagensgatan 112, 112 51 Stockholm, Schweden	Transaktionale E-Mails im Rahmen des Services	Die Datenverarbeitung erfolgt innerhalb der EU.
Raintank Inc. (Grafana Labs)	165 Broadway 23rd Floor, New York, NY 10006, United States	Monitoring	Serverstandort ist in der EU gemäß gewählter Hosting-Region (eu-central-1). Raintank Inc. ist unter dem EU-US-Data Privacy Framework zertifiziert (Angemessenheitsbeschluss gemäß Art. 45 DSGVO).

Anlage 3
Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit

Physische Zugangskontrolle

Diese Kategorie umfasst Maßnahmen zur Verhinderung des unbefugten physischen Zugangs zu Bereichen, in denen sensible Daten gespeichert oder verarbeitet werden.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Zugangskontrollsystem		Besucherprotokoll/Gästebuch
	Alarmanlage		Sorgfältige Auswahl des Reinigungspersonals
	Chipkarten-/Transponder-Schließsystem		

Logische Zugangskontrolle

Zu dieser Kategorie gehören Maßnahmen, die den unbefugten Zugriff auf digitale Systeme und Daten einschränken und sicherstellen, dass nur befugte Personen auf sensible Informationen und Ressourcen zugreifen können.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	„Zentrale Authentifizierung via Verzeichnisdienst (z. B. LDAP, AD) mit optionalem Single Sign-On“.		Passwort-Management-System
	Multi-Faktor-Authentifizierung (MFA)		Passwortrichtlinie
	Automatische Abmeldeverfahren		Keine geteilten Nutzeraccounts
	Verschlüsselung von Datenbanken		Dokumentierte Regelungen für das Ausscheiden von Mitarbeitern
	Einsatz von Anti-Viren-Lösungen		Verschlüsselungskonzept
	Authentifizierung mit Benutzernamen und Passwort		Erstellung von Benutzerprofilen
	Zero-Trust-Architektur (kontinuierliche Überprüfung und minimale Vertrauensbasis)		
	Konfiguration des VPN für den Fernzugriff		

Berechtigungskontrolle

In dieser Kategorie geht es darum, sicherzustellen, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten nur auf die Daten zugreifen können, für die sie eine Zugriffsberechtigung haben, und dass Kontrollen vorhanden sind, um die Zugriffsrechte zu verwalten und einzuschränken, eine unbefugte Nutzung zu verhindern und sensible Daten sicher zu behandeln.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Zugriff auf Server erfolgt ausschließlich verschlüsselt (z. B. via SSH mit Public Key)		Zuweisung von Administratorrechten an eine Mindestanzahl von Personen
	Automatische Kontosperrung nach mehrfacher Falscheingabe eines Passworts		Implementierung eines Rollen- und Berechtigungskonzepts
	Protokollierung des Anwendungszugriffs		Verpflichtung der Mitarbeiter zur Einhaltung der Anforderungen der Datenschutz-Grundverordnung

Trennungskontrolle

Diese Kategorie stellt sicher, dass Daten und Systeme bei Bedarf voneinander isoliert werden, um das Risiko von Datenlecks zu minimieren.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Trennung von Produktion und Testsystem		Datenschutzrichtlinie
	Physische Trennung von Datenbanken und Systemen		Sichere Kodierungspraktiken
	Segmentierung des Netzes		Logische Benutzertrennung
	Keine Nutzung von Daten zu Trainings- oder Modellverbesserungszwecken		Zugriffsrechte auf die Datenbank
			Zweckbindung der KI-Verarbeitung
			Verarbeitung abgeleiteter Daten (Embeddings, Vektoren, Metadaten) ausschließlich zur technischen Umsetzung der vereinbarten Funktionen

Pseudonymisierung

Diese Kategorie umfasst Maßnahmen, die sicherstellen, dass personenbezogene Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Übermittlung von Daten in pseudonymisierter Form		Frühzeitige Pseudonymisierung von personenbezogenen Daten

	Pseudonymisierung bei der Weiterverarbeitung oder Übermittlung		
	Pseudonymisierte Daten: Kennung wird in einem separaten IT-System gespeichert		

4. Integrität

Übertragungskontrolle

In dieser Kategorie geht es darum, die Integrität und Sicherheit von Daten während der Übertragung zu gewährleisten. Sie umfasst Maßnahmen, die Daten während der Übertragung zwischen Systemen oder Parteien vor unbefugtem Zugriff, Veränderung oder Verlust schützen und sicherstellen, dass die Daten während des gesamten Prozesses unverändert bleiben.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Inhaltsverschlüsselte Datenübertragung		
	Protokollierung von Datenzugriffen und Aktivitäten		
	Nutzung moderner Verschlüsselungsprotokolle (z. B. TLS 1.2/1.3, Ende-zu-Ende-Verschlüsselung)		
	Verschlüsselter E-Mail-Verkehr		

Eingabekontrolle

Diese Kategorie gewährleistet die Richtigkeit und Integrität der Daten bei Eingabe, Änderung und Zugriff. Sie umfasst Maßnahmen zur Verfolgung und Protokollierung aller Dateneingaben und -änderungen, zum Schutz der Daten vor unbefugten Änderungen und zur Ermöglichung von Korrekturen bei Bedarf. Diese Maßnahmen sind notwendig, um die Daten während ihres gesamten Lebenszyklus genau und konsistent zu halten und gleichzeitig Transparenz und Rechenschaftspflicht zu gewährleisten.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Möglichkeit, eine Berichtigung auf elektronischem Wege zu beantragen		Plausibilitätsprüfungen und automatische Validierung bei der Datenverarbeitung
	Protokollierung (von Datenzugriff, Eingabe, Änderung, Löschung, Übertragung, fehlgeschlagenen Zugriffsversuchen usw.)		Einrichtung eines Verfahrens zur Berichtigung von Daten auf Antrag
	Sicherung der Protokolldaten gegen Veränderung und Verlust		Sofortige Korrektur/Löschung fehlerhafter Daten
	Automatisierte Auswertung von Protokolldaten		Dokumentation der getroffenen Sicherheitsmaßnahmen
	Firewall-Paketfilter		Veröffentlichung von Informationen über die Verarbeitung personenbezogener Daten

	Manuelle oder automatisierte Überprüfung von Protokollen		Dokumentation der Vertrags- und Untervertragsbeziehungen
			Dokumentation der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
			Dokumentation der Verarbeitungstätigkeiten
			Zweckgebundene Verarbeitung von Eingaben und Ausgaben

5. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

In dieser Kategorie geht es darum, sicherzustellen, dass Daten und Systeme bei Bedarf durchgängig zugänglich und betriebsbereit sind, um Ausfallzeiten zu vermeiden und vor Datenverlusten oder Systemausfällen zu schützen.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Klimaüberwachung und Klimatisierung in Serverräumen		Dokumentierter Krisenplan (Notfallplan) beim Cloud-Anbieter
	Schutz vor Wasserschäden / Überschwemmungen (falls zutreffend)		Vermeidung von lokaler Datenspeicherung
	Überspannungsschutz		
	Unterbrechungsfreie Stromversorgung		
	Redundante IT-Systeme		
	Automatische Skalierung virtueller Systeme		
	Lastenausgleich der Netzwerkkomponenten / Server / Dienste		
	RAID-System		

Back-Up Kontrolle

Diese Kategorie gewährleistet, dass Daten und Systeme nach einem Zwischenfall schnell wieder voll funktionsfähig gemacht werden können.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Automatisierte Erstellung von Datensicherungen		Speicherung von Datensicherungen in einem anderen sicheren Fach außerhalb des Serverraums
			Regelmäßige Tests der Datenwiederherstellung

6. Verfahren zur regelmäßigen Überprüfung

Datenschutz-Management

Zu dieser Kategorie gehören die Verfahren und die Dokumentation, die erforderlich sind, um die ständige Einhaltung der Datenschutzvorschriften zu gewährleisten und den Datenschutz in die Betriebsabläufe, das Risikomanagement und die Entscheidungsprozesse des Unternehmens zu integrieren.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Die Datenschutzdokumentation ist zentralisiert und für alle Mitarbeiter zugänglich		Datenschutz-Folgenabschätzung, wo notwendig
	Keine automatisierte Entscheidungsfindung gemäß Art. 22 DSGVO		Regelmäßige Überprüfung der TOMs
			Datenschutzbeauftragter ernannt
			Regelmäßige Datenschutz- und Sensibilisierungsschulungen für Mitarbeiter
			Dokumentierte Prozesse bezüglich der Informationspflichten
			Formalisierte Verfahren für Informationsanfragen von betroffenen Personen

Management der Reaktion auf Zwischenfälle

In dieser Kategorie geht es um die laufende Bewertung und Verbesserung der Verfahren und Protokolle, die zur Reaktion auf Datenschutzverletzungen und Sicherheitsvorfälle eingesetzt werden.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Automatisierte Aktualisierungsprozesse für Betriebssysteme, Anwendungen und Dienste		Dokumentierte Verfahren zur Erkennung und Überwachung von Vorfällen
	Intrusion Prevention System		Dokumentierte Prozesse für die Meldung von Sicherheitsvorfällen
			Dokumentiertes Verfahren zur Benachrichtigung über Datenschutzverletzungen
			Strafanzeige

Datenschutz durch Technikgestaltung durch datenschutzrechtliche Voreinstellungen

Diese Kategorie gewährleistet, dass der Datenschutz von Anfang an in die Gestaltung und den Betrieb von Systemen und Prozessen integriert wird.

	Technische Maßnahmen		Organisatorische Maßnahmen
	Integration von Datenschutz-Voreinstellungen bereits im Systementwicklungsprozess		Dokumentation der Grundsätze des "eingebauten und standardmäßigen Datenschutzes" in der Datenschutzpolitik
			Regelmäßige Sicherheitsprüfungen bei der Entwicklung
			Durchführung von Datenschutz-Folgenabschätzungen (DPIAs) für neue Projekte, wenn notwendig

Auftragsverarbeitung

Diese Kategorie umfasst die Überwachung und Verwaltung von externen Parteien, die an der Datenverarbeitung beteiligt sind. Sie umfasst Maßnahmen, die sicherstellen, dass die Auftragsverarbeitungen das erforderliche Maß an Datenschutz und -sicherheit gewährleisten.

	Technische Maßnahmen		Organisatorische Maßnahmen
			Abschluss von Auftragsverarbeitungsverträgen gemäß Art. 28 DSGVO
			Durchführung einer Due-Diligence-Prüfung vor der Auswahl des Auftragnehmers