Auftragsverarbeitungsvertrag der AIMI GmbH

Stand: 26.10.2026

AIMI GmbH · Sierichstraße 88 · 22301 Hamburg
Amtsgericht Hamburg, HRB 198274 · Geschäftsführer: Jannick Stachowiak

Inhaltsverzeichnis

Abschnitt I
- Klausel 1: Zweck und Anwendungsbereich
- Klausel 2: Unabänderbarkeit der Klauseln
- Klausel 3: Auslegung
- Klausel 4: Vorrang
- Klausel 5 (fakultativ): Kopplungsklausel

Abschnitt II: Pflichten der Parteien
- Klausel 6: Beschreibung der Verarbeitung
- Klausel 7: Pflichten der Parteien
- Klausel 8: Unterstützung des Verantwortlichen
- Klausel 9: Meldung von Verletzungen des Schutzes personenbezogener Daten

Abschnitt III: Schlussbestimmungen
- Klausel 10: Verstöße gegen die Klauseln und Beendigung des Vertrags
- Klausel 11: Änderung der Anhänge und ergänzende Vereinbarungen nach Klausel 2 Buchstabe b

Anhang I: Liste der Parteien

Anhang II: Beschreibung der Verarbeitung
- Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden
- Kategorien personenbezogener Daten, die verarbeitet werden
- Verarbeitete sensible Daten und angewandte Beschränkungen oder Garantien
- Art der Verarbeitung
- Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden
- Dauer der Verarbeitung
- Empfänger, die keine Unterauftragsverarbeiter sind
- Protokolle in eigener Verantwortung des Auftragsverarbeiters

Anhang III: Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten
- 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
- 2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)
- 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)
- 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 DSGVO)
- 5. Unterstützung des Verantwortlichen (Klausel 8 Buchstabe d, Klausel 9.2)
- 6. Maßnahmen der Unterauftragsverarbeiter

Anhang IV: Liste der Unterauftragsverarbeiter

Die Klauseln 1 bis 10 geben den Anhang des Durchführungsbeschlusses (EU) 2021/915 der Kommission wieder. Gewählt sind die Fassungen für die Verordnung (EU) 2016/679 und die allgemeine schriftliche Genehmigung nach Klausel 7.7 Buchstabe a. Klausel 11 ergänzt sie nach Klausel 2 Buchstabe b.

Abschnitt I

Klausel 1: Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2: Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3: Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4: Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 (fakultativ): Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

Abschnitt II: Pflichten der Parteien

Klausel 6: Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7: Pflichten der Parteien

7.1. Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken

der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der

Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8: Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9: Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung

voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

Abschnitt III: Schlussbestimmungen

Klausel 10: Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Klausel 11: Änderung der Anhänge und ergänzende Vereinbarungen nach Klausel 2 Buchstabe b

a) Gemäß Klausel 2 Buchstabe b dieser Vereinbarung vereinbaren die Parteien ergänzend Folgendes: Der Auftragsverarbeiter ist berechtigt, die Anhänge III und IV

zu aktualisieren, soweit dies zur Einhaltung geänderter datenschutzrechtlicher Vorgaben erforderlich ist, zur Aufrechterhaltung oder Verbesserung der technischen und organisatorischen Maßnahmen dient oder ein Wechsel oder eine Hinzunahme von Unterauftragsverarbeitern zur Aufrechterhaltung der vertraglich geschuldeten Leistungen notwendig ist. Maßnahmen nach Anhang III dürfen nur durch gleichwertige oder bessere ersetzt werden; das Schutzniveau nach Anhang III wird nicht unterschritten. Änderungen der Anhänge I und II setzen eine Vereinbarung der Parteien oder eine Weisung des Verantwortlichen voraus. Für Änderungen der Liste der Unterauftragsverarbeiter (Anhang IV) gilt Klausel 7.7 mit den Ergänzungen in den Buchstaben b bis e. Als Änderung dieser Liste gilt auch die Änderung eines Verarbeitungsorts in Anhang IV; sie wird wie das Hinzufügen oder Ersetzen eines Unterauftragsverarbeiters behandelt, die Buchstaben b bis e gelten entsprechend, und an die Stelle des Einsatzes des Unterauftragsverarbeiters tritt die Verarbeitung am neuen Ort. Gleiches gilt, wenn ein in Anhang IV genannter Unterauftragsverarbeiter eine weitere Leistung übernimmt oder weitere Kategorien personenbezogener Daten verarbeitet. Über alle anderen Änderungen der Anhänge III und IV informiert der Auftragsverarbeiter den Verantwortlichen mindestens 30 Tage vor Wirksamwerden in Textform.

b) Die jeweils geltende Liste der Unterauftragsverarbeiter ist zusätzlich öffentlich abrufbar (Anhang IV), mit Stand und Änderungsverlauf. Die Veröffentlichung dient der Information; sie ersetzt die Unterrichtung nach Buchstabe c nicht.

c) Die Unterrichtung nach Klausel 7.7 Buchstabe a erfolgt in der dort genannten Frist per E-Mail an die Adresse, die der Verantwortliche dafür im Vertrag oder in der Software hinterlegt hat. Hat er keine gesonderte Adresse hinterlegt, geht die Mitteilung an die Administratoren seines Unternehmens in der Software. Die Mitteilung nennt mindestens Name, Anschrift, Leistung, Verarbeitungsort und Drittlandbezug samt Grundlage der Übermittlung. Der Verantwortliche sorgt dafür, dass die hinterlegte Adresse erreichbar ist.

d) Der Verantwortliche kann innerhalb der Frist nach Klausel 7.7 Buchstabe a in Textform Einwände erheben. Die Parteien suchen dann innerhalb von 14 Tagen nach Zugang der Einwände eine einvernehmliche Lösung. Bis zu einer Einigung, längstens bis zum Wirksamwerden einer Kündigung nach Buchstabe e, setzt der Auftragsverarbeiter den betroffenen Unterauftragsverarbeiter für die Daten des Verantwortlichen nicht ein.

e) Kommt keine Einigung zustande, ist der Verantwortliche berechtigt, den Vertrag insgesamt oder hinsichtlich der betroffenen Leistungen außerordentlich zu kündigen, frühestens mit Wirkung zum geplanten Einsatz. Weitergehende Rechte des Verantwortlichen bleiben unberührt.

Anhang I: Liste der Parteien

Verantwortlicher: Der Kunde gemäß dem jeweiligen Angebot und den Geschäftsbedingungen der AIMI GmbH. Anschrift sowie Name, Funktion und Kontaktdaten der Kontaktperson und gegebenenfalls des Datenschutzbeauftragten: wie im Angebot.

Auftragsverarbeiter: AIMI GmbH Sierichstraße 88, 22301 Hamburg Amtsgericht Hamburg, HRB 198274 Kontaktperson: Jannick Stachowiak, Geschäftsführer, info@aimipro.com Ein Datenschutzbeauftragter ist nicht benannt; Ansprechstelle für den Datenschutz ist info@aimipro.com.

Unterschrift und Beitrittsdatum: Beide Parteien treten diesen Klauseln mit der Annahme des Angebots bei, auch in elektronischer Form (Art. 28 Abs. 9 der Verordnung (EU) 2016/679). Beitrittsdatum ist das Datum der Annahme. Weitere Einrichtungen treten nach Klausel 5 durch eine von allen Parteien angenommene Ergänzung dieses Anhangs bei.

Anhang II: Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

Beschäftigte des Kunden (Nutzer der Software und der iOS-App), Ansprechpartner und Kontaktpersonen des Kunden, Dritte, deren personenbezogene Daten in den vom Kunden hochgeladenen Dokumenten, in Chatanfragen, in Diktaten oder auf Fotos aus Begehungen enthalten sind (zum Beispiel Mieter, Vertragspartner, Dienstleister, Berater des Kunden, auf Fotos erkennbare Personen).

Kategorien personenbezogener Daten, die verarbeitet werden

- Personenstammdaten der Nutzer: Name, berufliche E-Mail-Adresse, Berufsbezeichnung, Nutzerkennung.
- Nutzungsdaten in der Software: Zugangsberechtigungen und Chat-Historie. Betriebs- und Nutzungsprotokolle, darunter Login-Historie, Fehlermeldungen und die Verbrauchsdaten je Vorgang, führt der Auftragsverarbeiter in eigener Verantwortung (Abschnitt „Protokolle in eigener Verantwortung des Auftragsverarbeiters“).
- IP-Adressen bei der Nutzung der Software.
- Inhalte der vom Kunden hochgeladenen Dokumente, soweit diese personenbezogene Daten enthalten. Dies umfasst Text, Tabellen und Bildinhalte innerhalb der Dokumente. Dazu zählen auch Word-Dokumente und E-Mails, die der Nutzer über das Office-Add-in an die Software übergibt.
- Inhalte der Chatanfragen und -antworten sowie hochgeladener Anhänge, soweit diese personenbezogene Daten enthalten.
- Tonspuren (Audio) aus Begehungsnotizen und Diktaten zu Fotos in der iOS-App und deren Abschrift.
- Daten aus Begehungen mit der iOS-App: Fotos, Notizen und Befunde, Aufnahmezeit, Standort je Foto (Breiten- und Längengrad mit Genauigkeit), relative Höhe aus dem Luftdruck zur Zuordnung zum Geschoss sowie die vom Nutzer in der App gewählten Fotos und Dateien.
- Objektanschriften und Koordinaten aus der Adresssuche.
- Analyseergebnisse der Software, soweit diese personenbezogene Daten enthalten. Dazu zählen Zusammenfassungen, Prüfergebnisse, Berichte und die dabei erzeugten Vektorrepräsentationen der Dokumentinhalte.

Verarbeitete sensible Daten und angewandte Beschränkungen oder Garantien

Kreditunterlagen und andere Dokumente des Verantwortlichen können sensible Daten enthalten, zum Beispiel Angaben zu Gesundheit, Gewerkschaftszugehörigkeit oder

strafrechtlichen Verurteilungen in Gehaltsnachweisen, Kontoauszügen oder Auskünften. Der Verantwortliche kann sie mit Dokumenten einbringen. Als zusätzliche Garantien nach Klausel 7.5 gelten:

- Verschlüsselung bei Übertragung und Speicherung (Anhang III, Weitergabekontrolle).
- Zugriff über die Software nur für die berechtigten Nutzer des Verantwortlichen, mandantengetrennt (Anhang III, Zugriffs- und Trennungskontrolle).
- Zugriff des Auftragsverarbeiters nur, soweit dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist (Klausel 7.4 Buchstabe b).
- Keine Verwendung zum Training von KI-Modellen (Anhang II, Zwecke).

Die Ausnahmen für die Internetrecherche (Anhang IV Nr. 3) und für die Empfänger, die keine Unterauftragsverarbeiter sind (unten), bleiben unberührt.

Art der Verarbeitung

Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten.

Die iOS-App erfasst Fotos, Tonspuren, Notizen, Standort und relative Höhe auf dem Gerät und überträgt sie an die Software. Die Tonspur wird nach der Transkription verworfen; gespeichert wird nur der Text. Die Software speichert Fotos und Notizen mit Standort, Höhe und Aufnahmezeit; Begehungsfotos legt sie zusätzlich als Dokument im Datenraum ab.

Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

Bereitstellung und Betrieb der Software „AIMI Pro“ und der iOS-App gemäß den Geschäftsbedingungen und der Leistungsbeschreibung der AIMI GmbH, einschließlich der semantischen Dokumentenanalyse, der automatischen Benennung und Einsortierung von Dokumenten, der Dokumentation von Begehungen, der Bereitstellung der Softwaremodule, der Nutzerverwaltung sowie der Fehlerbehebung und technischen Wartung.

Der Auftragsverarbeiter und die Unterauftragsverarbeiter verwenden die Daten des Verantwortlichen nicht zum Training von KI-Modellen.

Dauer der Verarbeitung

Gemäß der Laufzeit des zwischen den Parteien geschlossenen Vertrags. Nach Beendigung gilt Klausel 10 Buchstabe d mit folgenden Fristen:

1. **Übergang.** Auf Verlangen des Kunden unterstützt AIMI den Wechsel zu einem anderen Anbieter oder in eigene Systeme während eines Übergangszeitraums von

bis zu 30 Tagen, bei Finanzunternehmen nach Ziffer 19 Buchstabe g der Geschäftsbedingungen von bis zu sechs Monaten. Die Software bleibt in dieser Zeit nutzbar.

2. **Abruf.** Nach dem Übergangszeitraum kann der Kunde seine Daten 30 Tage lang abrufen. Verlangt der Kunde keinen Übergang, beginnt der Abrufzeitraum mit dem Vertragsende. Welche Daten in welchen Formaten exportiert werden können, beschreibt die Leistungsbeschreibung. Verlangt der Kunde die Löschung, löscht AIMI die Daten, ohne den Abrufzeitraum abzuwarten.
3. **Löschung.** Nach Ablauf des Abrufzeitraums löscht AIMI die Daten des Kunden, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Betriebs- und Nutzungsprotokolle sind nicht Gegenstand dieser Klauseln; für sie gilt der Abschnitt „Protokolle in eigener Verantwortung des Auftragsverarbeiters“. Sicherungskopien und das Lösch-Archiv werden spätestens 90 Tage nach der Löschung automatisch entfernt. AIMI bescheinigt die Löschung nach Klausel 10 Buchstabe d.

Innerhalb der Vertragslaufzeit gelöschte Daten bleiben aus technischen Gründen der Wiederherstellbarkeit noch für die Schutzfristen nach Anhang III, längstens 90 Tage nach der Löschung, in Sicherungsbeständen vorhanden und werden danach endgültig entfernt. Gelöschte und überschriebene Stände im Dokumentenspeicher und im Upload-Speicher bleiben als Version erhalten (Anhang III, Verfügbarkeitskontrolle). Weist der Kunde die Löschung bestimmter Daten an, löscht AIMI auch deren Versionen; Sicherungsbestände werden nach den Schutzfristen nach Anhang III, längstens 90 Tage nach der Löschung, entfernt. Mit Vertragsende werden alle Versionen nach Nummer 3 gelöscht.

Empfänger, die keine Unterauftragsverarbeiter sind

Datenflüsse in Systeme des Verantwortlichen. Bindet der Verantwortliche die Software über den MCP-Connector oder die Text-API in eigene Anwendungen oder in KI-Assistenten eines von ihm gewählten Anbieters ein, übermittelt die Software Suchtreffer, Dokumenttexte und Antworten auf seine Veranlassung an diese Systeme. Der Zugriff der Software ist dabei lesend und auf die Berechtigungen des jeweiligen Nutzers beschränkt. Die weitere Verarbeitung in diesen Systemen liegt in der Verantwortung des Verantwortlichen; deren Anbieter sind keine Unterauftragsverarbeiter des Auftragsverarbeiters. Gleiches gilt für die Microsoft-365-Umgebung des Verantwortlichen, aus der die Software auf seine Weisung Dokumente abruft (SharePoint-Anbindung).

Öffentliche Stellen, Register und Kartendienste. Für Recherchen zu Grundstücken, Planungsrecht, Standorten und Recht ruft die Software öffentliche Quellen ab, insbesondere Geoportale und Liegenschaftskataster der Länder, Bebauungspläne, Denkmallisten, Bodenrichtwerte, das Handelsregister, Rechts- und Gesetzesdatenbanken sowie öffentliche Kartendienste. Diese Quellen erhalten Suchbegriffe und Koordinaten, keine Dokumente des Verantwortlichen; Suchbegriffe können Anschriften, Flurstücke oder Firmennamen sein, auch Namen von Einzelkaufleuten. Kartenkacheln und Kartenausschnitte lädt der Browser des Nutzers direkt von Kartendiensten wie OpenStreetMap und den Geodiensten von Bund und Ländern; deren Betreiber erhalten

dabei die IP-Adresse des Nutzers und den angezeigten Kartenausschnitt. Ruft die Software eine Webseite ab, die der Nutzer nennt oder die die Recherche gefunden hat, erhält deren Betreiber die abgerufene Adresse und die IP-Adresse des Servers der Software, nicht die des Nutzers. Die Betreiber all dieser Quellen sind keine Unterauftragsverarbeiter.

Quellen-Symbole und Weiterleitungen im Chat. Zeigt der Chat Webquellen an, lädt der Browser des Nutzers die Symbole dieser Quellen (Favicons) vom Favicon-Dienst der Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. Google erhält dabei die IP-Adresse des Nutzers und die Domain der angezeigten Quelle, keine Dokumente und keine Chatinhalte. Für diesen Dienst besteht keine Zusage einer Verarbeitung in der Europäischen Union. Google LLC ist nach dem EU-US Data Privacy Framework zertifiziert. Öffnet der Nutzer eine Webquelle aus der Internetrecherche, führt der Link über eine Weiterleitung der Google LLC; Google erhält dabei die IP-Adresse des Nutzers und die aufgerufene Quelle. Google LLC ist insoweit kein Unterauftragsverarbeiter.

Dienste des Endgeräts. Nutzt ein Nutzer die Spracheingabe im Browser, verarbeitet der Hersteller seines Browsers die Sprachaufnahme nach dessen eigenen Bedingungen. In der iOS-App erfolgen die Spracherkennung und die Kartendarstellung über Dienste des Betriebssystems von Apple. Die Spracherkennung läuft nur dann ausschließlich auf dem Gerät, wenn das Gerät die Erkennung ohne Netz für die eingestellte Sprache unterstützt; sonst nutzt iOS Server von Apple. Die Tonspuren von Begehungsnotizen und Diktaten zu Fotos verarbeitet zusätzlich die Transkription der Software (Anhang IV Nr. 1). Die Hersteller von Browser und Betriebssystem sind keine Unterauftragsverarbeiter des Auftragsverarbeiters.

Protokolle in eigener Verantwortung des Auftragsverarbeiters

Betriebs- und Nutzungsprotokolle führt der Auftragsverarbeiter als eigener Verantwortlicher; insoweit sind sie nicht Gegenstand dieser Klauseln. Sie dienen der Sicherheit und dem Betrieb der Software, insbesondere dem Erkennen und Abwehren von Angriffen und Missbrauch und der Fehleranalyse, und der Abrechnung. Der Credit-Verbrauch wird aus der Nutzung berechnet, die diese Protokolle festhalten. Deshalb bewahrt der Auftragsverarbeiter sie bis zu 24 Monate auf, damit Abrechnungen auch nachträglich nachvollzogen und geprüft werden können; Anmeldeprotokolle bis zu 12 Monate.

Die Protokolle enthalten den Zeitpunkt, die aufgerufene Funktion und Adresse einschließlich Kennungen von Firma, Projekt und Datenraum sowie Suchparametern wie Koordinaten und Flurstücken, die ungekürzte IP-Adresse, Nutzer- und Firmenkennung, Fehlermeldungen, Verbrauchsangaben (verarbeitete Seiten, Umfang der Modellaufrufe, eingesetztes Modell) und Diagnosedaten der eingesetzten Azure-Dienste. Anmeldeprotokolle enthalten zusätzlich Anmeldename, Gerät, Browser und den ungefähren Ort der Anmeldung. Die Protokolle sind nicht dafür bestimmt, Inhalte von Dokumenten oder Chatverläufen aufzunehmen. Protokollzeilen können aber Dateinamen enthalten.

Die Protokolle liegen bei Microsoft (Application Insights, Log Analytics) in der Azure-Region Westeuropa. Zweck, Rechtsgrundlage und Speicherdauer beschreibt auch die Datenschutzerklärung des Auftragsverarbeiters.

Anhang III: Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

AIMI unterhält keine eigenen Rechenzentren und keine eigenen Geschäfts- oder Serverräume. Der physische Zutrittsschutz richtet sich nach den Zertifizierungen der in Anhang IV genannten Unterauftragsverarbeiter (insbesondere ISO 27001, SOC 2); entsprechende Nachweise werden im Rahmen der Auftragskontrolle eingeholt.

Zugangskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Anmeldung der Nutzer, auch in der iOS-App, ausschließlich über Microsoft Entra External ID (OpenID Connect); kein eigenes Passwortverfahren. Die Anmeldetoken der App liegen im Schlüsselbund des Geräts	Freischaltung von Nutzern nur über die vom Kunden benannte E-Mail-Domain
Vorgelagerter Authentifizierungs-Proxy (Azure EasyAuth): unauthentifizierte Anfragen werden vor Erreichen der Anwendung umgeleitet	Der Kunde benennt mindestens einen Administrator, der die Nutzerverwaltung eigenverantwortlich führt
Sitzungscookie ausschließlich HttpOnly und Secure, damit es Skripten im Browser nicht zugänglich ist	Berechtigungskonzept mit minimaler Zahl an Administratoren
Prüfung jedes Zugriffstokens auf Signatur, Aussteller, Empfänger und Gültigkeitsdauer	Verpflichtung aller für AIMI tätigen Personen auf Vertraulichkeit
Begrenzung der Anfragen je Nutzer und Zeiteinheit (Rate Limiting), verschärft auf Anmeldepfaden	Prüfung der Berechtigungen mindestens halbjährlich
Text-API und Connector zusätzlich über von AIMI ausgestellte, widerrufbare Schlüssel, wahlweise mit Ablaufdatum und IP-Beschränkung	
Zweiter Faktor für alle Konten, mit denen AIMI die Software betreibt und verwaltet	
Verwaltung über ein getrenntes Administrationskonto; gesondertes Notfallkonto, gesichert mit einem Hardware-Schlüssel	
Entfernte Nutzerkonten werden sofort gesperrt	

Zugriffskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Zugriff auf die Azure-Dienste ausschließlich über verwaltete Identitäten; API-Schlüssel auf den Azure-KI- und Analysediensten technisch deaktiviert. Google Vertex AI über Workload-Identitätsföderation ohne gespeicherten Schlüssel. Amazon Bedrock über einen API-Schlüssel, der ausschließlich im Schlüsseltresor liegt und nach dokumentiertem Verfahren rotiert wird	Rollen- und Berechtigungskonzept, rollenbasierte Rechtevergabe nach dem Prinzip der geringsten Rechte
Kein Zugriff auf den Dokumentenspeicher über geteilte Schlüssel; öffentlicher Zugriff auf Speichercontainer ist abgeschaltet	Verwaltung der Nutzerrechte ausschließlich durch Administratoren
Jede Anwendungsroute ist einzeln durch eine Berechtigungsprüfung geschützt	Zugangsdaten und Schlüssel liegen in einem zentralen Schlüsseltresor; Rotation erfolgt nach dokumentiertem Verfahren
Beim Upload wird geprüft, dass der Zielpfad zur angemeldeten Nutzerkennung gehört	
Protokollierung der Zugriffe auf Anwendungen mit Nutzer- und Firmenkennung	

Trennungskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Mandantentrennung im Suchindex durch Filterung jeder Suchanfrage auf Nutzerkennung und Gruppenzugehörigkeit (Security Trimming)	Steuerung über das Berechtigungskonzept
Trennung der Daten je Firma über eigene Partitionen in der Datenbank und getrennte Speicherpfade	
Getrennte Produktiv- und Entwicklungsumgebung; Tests und Abnahmen finden in der Entwicklungsumgebung statt	Keine Echtdaten von Kunden in Tests

Pseudonymisierung (Art. 32 Abs. 1 lit. a, Art. 25 Abs. 1 DSGVO)

Technische Maßnahmen	Organisatorische Maßnahmen
Telemetriedaten der Nutzung führt die Anwendung unter technischen Kennungen (Nutzer- und Firmenkennung), nicht unter Klarnamen; Anmeldeprotokolle enthalten zusätzlich den Anmeldenamen	Interne Anweisung, personenbezogene Daten bei einer Weitergabe und nach Ablauf gesetzlicher Löschfristen zu anonymisieren oder zu pseudonymisieren

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Ausschließlich verschlüsselte Übertragung (HTTPS, TLS ab Version 1.2), auch zwischen iOS-App und Software; unverschlüsselte Verbindungen werden abgewiesen	Dokumentation der Datenempfänger sowie der Dauer der Überlassung und der Löschfristen (Anhang IV)
HSTS mit einem Jahr Gültigkeit einschließlich Subdomains	Der Auftragsverarbeiter setzt nur Unterauftragsverarbeiter ein, die sich vertraglich verpflichtet haben, Herausgabeverlangen von Behörden zu prüfen, soweit möglich an den Kunden zu verweisen, rechtlich anzufechten, wenn dafür Gründe bestehen, und den Kunden zu informieren, soweit dies rechtlich zulässig ist
Content-Security-Policy, X-Frame-Options und Referrer-Policy zur Absicherung des Browserkontexts	Erhält der Auftragsverarbeiter selbst ein Herausgabeverlangen einer Behörde eines Drittstaats, prüft er dessen Rechtmäßigkeit, gibt Daten nur heraus, soweit er nach Unionsrecht oder dem Recht eines Mitgliedstaats dazu verpflichtet ist, ficht das Verlangen an, wenn nach seiner Prüfung Gründe dafür bestehen, und unterrichtet den Verantwortlichen unverzüglich, soweit dies rechtlich zulässig ist; die Klauseln 7.1 Buchstabe a und 7.8 bleiben unberührt
Herkunftsprüfung eingehender Anfragen gegen eine Positivliste (CORS)	
Verschlüsselung ruhender Daten durch die Plattformverschlüsselung der Cloud-Anbieter	
Protokollierung der Zugriffe und Abrufe	

Eingabekontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung von Anlage, Änderung und Löschung von Daten mit Zeitstempel, Nutzer- und Firmenkennung	Nachvollziehbarkeit über individuelle Nutzerkonten, keine Sammelkonten
Jede Löschung schreibt zuvor ein vollständiges Wiederherstellungspaket in ein gesondertes Archiv	Vergabe von Rechten zur Eingabe, Änderung und Löschung auf Basis des Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

Verfügbarkeitskontrolle

Maßnahme	Schutzfrist
Versionierung des Dokumentenspeichers und des Upload-Speichers: gelöschte und überschriebene Stände bleiben als Version erhalten; auf Weisung des Verantwortlichen werden auch die Versionen der betroffenen Daten gelöscht, bei Vertragsende alle Versionen des Kunden mit den übrigen Daten	bis zur Löschung auf Weisung oder nach Anhang II
Versionierung des Zwischenspeichers für Massen-Uploads	7 Tage
Wiederherstellung des Dokumentenspeichers auf einen früheren Zeitpunkt (Point-in-Time-Restore)	29 Tage
Wiederherstellung gelöschter Speichercontainer (Soft Delete)	30 Tage
Fortlaufende Sicherung der Datenbank	30 Tage
Zusätzliche Sicherung außerhalb der Produktivumgebung, georedundant in einer entfernten Partnerregion innerhalb der Europäischen Union, in einem unveränderbar gesperrten Speicher (WORM)	90 Tage Export, 30 Tage Unveränderlichkeit
Lösch-Archiv mit vollständigem Wiederherstellungspaket je Löschvorgang, mit Kopie außerhalb der Produktivumgebung	30 Tage ab Anlage (Kopie 32 Tage), danach 30 Tage Soft Delete

Ergänzend: Ein dokumentiertes Wiederanlaufverfahren beschreibt für jeden Verlustfall den konkreten Ablauf einschließlich Trockenlauf vor der Wiederherstellung. Es ist Teil des Notfallplans, den AIMI mindestens einmal je Kalenderjahr übt. Die Verfügbarkeit der Software wird automatisiert gemessen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 DSGVO)

Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit bedarfsgerechtem Zugriff für die für AIMI tätigen Personen	Alle für AIMI tätigen Personen werden jährlich mit Nachweis geschult
Laufende Überwachung der Anwendung und Alarmierung bei Auffälligkeiten	Regelmäßige Prüfung und Aktualisierung von Abhängigkeiten der Software
Technische Freigabe jeder Änderung über eine Pipeline mit Prüfung der Abhängigkeiten, Suche nach Geheimnissen, statischer Codeanalyse, Prüfung des Container-Images und Prüfung der Webanwendung; zusätzlich monatlicher Lauf	Sicherheitsleitlinie in Anlehnung an ISO/IEC 27001 (ohne Zertifizierung) und Kryptokonzept
Laufzeit-Image ohne Build-Werkzeuge	Risikoregister mit jährlichem Bericht

Incident-Response-Management

Technische Maßnahmen	Organisatorische Maßnahmen
Automatische Alarmierung bei sicherheits- und betriebsrelevanten Ereignissen	Dokumentation von Sicherheitsvorfällen und Datenpannen
Dokumentiertes Verfahren zur sofortigen Rotation kompromittierter Zugangsdaten	Dokumentierter Ablauf für Vorfälle und Schwachstellen

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Technische Maßnahmen	Organisatorische Maßnahmen
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	Zugriff angebundener KI-Assistenten ausschließlich lesend und mandantengetrennt
iOS-App: Zugriff auf Kamera, Mikrofon, Standort, Bewegung und Luftdruck sowie Spracherkennung nur nach Freigabe durch den Nutzer über die Berechtigungsabfrage des Betriebssystems; Standort nur mit der Berechtigung „Beim Verwenden der App“ und nur, solange eine Begehung geöffnet ist; Zugriff auf die Fotomediathek nur über die Auswahl des Systems	
iOS-App: Die lokal gespeicherten Begehungsdaten sind von iCloud- und Geräte-Backups ausgenommen; Bilddateien werden nach bestätigter Übertragung, Tonspuren nach bestätigtem Text vom Gerät gelöscht	
iOS-App: Keine Tracking-, Werbe- oder Analysebibliotheken; einzige eingebundene Fremdbibliothek ist die Anmeldebibliothek von Microsoft (MSAL)	

Auftragskontrolle (Outsourcing an Dritte)

Organisatorische Maßnahmen
Vorherige Prüfung der von den Unterauftragsverarbeitern getroffenen Sicherheitsmaßnahmen und deren Dokumentation
Auswahl der Unterauftragsverarbeiter unter Sorgfaltsgesichtspunkten, insbesondere in Bezug auf Datenschutz und Datensicherheit
Verpflichtung des Personals der Unterauftragsverarbeiter auf Vertraulichkeit
Abschluss eines Vertrags nach Klausel 7.7 Buchstabe b mit jedem in Anhang IV genannten Unterauftragsverarbeiter

5. Unterstützung des Verantwortlichen (Klausel 8 Buchstabe d, Klausel 9.2)

Gegenstand	Maßnahme, Weg und Frist
Anlaufstelle	Der Auftragsverarbeiter nimmt Anfragen des Verantwortlichen zu diesem Abschnitt unter info@aimipro.com entgegen.
Anträge betroffener Personen (Klausel 8 Buchstaben a und b)	Erhält der Auftragsverarbeiter einen Antrag, leitet er ihn unverzüglich per E-Mail an die Adresse weiter, die der Verantwortliche nach Klausel 11 Buchstabe c hinterlegt hat, und beantwortet ihn nicht selbst. Auf Weisung des Verantwortlichen führt er Auskunft, Berichtigung, Einschränkung, Löschung oder Export der betroffenen Daten durch. Die Löschung umfasst auch die Versionen der betroffenen Daten; Sicherungsbestände werden nach Anhang II entfernt.
Datenschutz-Folgenabschätzung und Konsultation der Aufsichtsbehörde (Klausel 8 Buchstabe c Nummern 1 und 2)	Auf Anfrage stellt der Auftragsverarbeiter die für die Abschätzung erforderlichen Informationen aus den Anhängen II bis IV und die Nachweise nach Klausel 7.6 Buchstabe c zur Verfügung.
Verletzung des Schutzes personenbezogener Daten (Klausel 9.2)	Der Auftragsverarbeiter meldet die Verletzung unverzüglich, spätestens innerhalb von 24 Stunden, nachdem sie ihm bekannt wurde, per E-Mail an die Adresse, die der Verantwortliche nach Klausel 11 Buchstabe c hinterlegt hat. Die Meldung enthält die Angaben nach Klausel 9.2 Buchstaben a bis c. Was bei der ersten Meldung noch fehlt, reicht er nach, sobald es vorliegt.
Unrichtige Daten (Klausel 8 Buchstabe c Nummer 3)	Stellt der Auftragsverarbeiter fest, dass verarbeitete Daten unrichtig oder veraltet sind, unterrichtet er den Verantwortlichen unverzüglich an die nach Klausel 11 Buchstabe c hinterlegte Adresse.
Sicherheit der Verarbeitung (Klausel 8 Buchstabe c Nummer 4)	Die Maßnahmen nach den Abschnitten 1 bis 4 dieses Anhangs; Nachweise nach Klausel 7.6 Buchstabe c auf Anfrage.
Meldungen des Verantwortlichen (Klausel 9.1)	Auf Anfrage liefert der Auftragsverarbeiter die ihm vorliegenden Angaben nach Klausel 9.1 Buchstabe b Nummern 1 bis 3.
Sonstige Angaben (Klausel 9.2 letzter Absatz)	Keine über Klausel 9.2 Buchstaben a bis c hinaus.

6. Maßnahmen der Unterauftragsverarbeiter

Die Unterauftragsverarbeiter nach Anhang IV treffen mindestens die Sicherheitsmaßnahmen, die in ihren Verträgen mit dem Auftragsverarbeiter festgelegt sind: Microsoft in den Datenschutzbedingungen für Produkte und Services (Data Protection Addendum), Amazon Web Services im AWS GDPR Data Processing Addendum, Google Cloud im Cloud Data Processing Addendum, jeweils mit ihren Anhängen zu den Sicherheitsmaßnahmen. Zur Unterstützung des Verantwortlichen sind sie verpflichtet, den Auftragsverarbeiter unverzüglich über Verletzungen des Schutzes

personenbezogener Daten zu unterrichten und ihn bei Anträgen betroffener Personen, Datenschutz-Folgenabschätzungen und Prüfungen zu unterstützen. Die Dokumente stellt der Auftragsverarbeiter auf Anfrage zur Verfügung (Klausel 7.6 Buchstabe c, Klausel 7.7 Buchstabe c).

Anhang IV: Liste der Unterauftragsverarbeiter

Dies ist die vereinbarte Liste nach Klausel 7.7 Buchstabe a. Dieselbe Liste ist unter https://www.aimipro.com/legal/unterauftragsverarbeiter veröffentlicht; Änderungen teilt der Auftragsverarbeiter nach Klausel 7.7 und Klausel 11 mit. Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt.

Der Auftragsverarbeiter speichert und verarbeitet die personenbezogenen Daten des Verantwortlichen in Rechenzentren in der Europäischen Union bzw. im Europäischen Wirtschaftsraum, die Daten der Anmeldung am Microsoft-Datenstandort „Europe“ (Nr. 1). KI-Modelle, die außerhalb der Europäischen Union betrieben werden, bietet er nicht an. Ausnahmen bestehen nur, soweit sie in diesem Anhang oder in Anhang II ausdrücklich beschrieben sind: Zugriffe und Übermittlungen im Ausnahmefall (unten), bei Nr. 1 das Office-Add-in und der E-Mail-Versand, bei Nr. 3 die Internetrecherche sowie die Empfänger, die keine Unterauftragsverarbeiter sind (Anhang II).

Für alle Einträge gilt:

- **Konzerngesellschaften.** Genannt ist jeweils die Gesellschaft, mit der der Auftragsverarbeiter den Vertrag geschlossen hat. Setzt diese Gesellschaft ihrerseits verbundene Unternehmen oder weitere Dienstleister ein, sind diese in der Liste des Anbieters aufgeführt, auf die der jeweilige Eintrag verweist. Der Anbieter ist nach seinen Vertragsbedingungen verpflichtet, über Änderungen dieser Liste vorab zu informieren.
- **Zugriffe und Übermittlungen im Ausnahmefall.** Die Daten werden an den genannten Orten gespeichert und verarbeitet. Ein Zugriff von Support- oder Technikpersonal des Anbieters aus Ländern außerhalb des Europäischen Wirtschaftsraums ist nach dessen Vertragsbedingungen nur ausnahmsweise vorgesehen, etwa zur Behebung einer Störung, und setzt, soweit der Auftragsverarbeiter den Supportfall auslöst, seine Freigabe im Einzelfall voraus. Microsoft beschreibt außerdem begrenzte Übermittlungen, die für Betrieb und Sicherheit seiner Dienste erforderlich sind: die Weiterleitung von Datenverkehr über das weltweite Netz von Microsoft, pseudonymisierte Daten für den weltweiten Sicherheitsbetrieb, als betrügerisch erkannte IP-Adressen und Telefonnummern sowie begrenzte Verzeichnisdaten wie Anmeldename und E-Mail-Adresse. Solche Zugriffe und Übermittlungen erfolgen auf der jeweils genannten Grundlage der Übermittlung.

1. Microsoft Ireland Operations Limited

- **Anschrift:** One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland
- **Kontakt Datenschutz:** Datenschutzbeauftragter von Microsoft in der EU, Anschrift wie vor; Webformular https://aka.ms/privacyresponse
- **Leistungen:**
  - Betrieb der Software: Anwendungsserver (Azure Container Apps), Datenbank (Azure Cosmos DB), Suchindex (Azure AI Search), Dokumentenspeicher (Azure Storage), Sicherungen (Azure Backup), Schlüsseltresor (Azure Key Vault).

  - KI-Modelle über Azure OpenAI: Chat, Dokumentenanalyse und Einsortierung, Vektorrepräsentationen (Embeddings), Bilderzeugung im Chat, Abschrift von Diktaten. Daten werden nicht an OpenAI übermittelt; die Modelle laufen in der Azure-Infrastruktur von Microsoft.
  - Texterkennung von Dokumenten (Azure Document Intelligence) und Beschreibung von Bildern in Dokumenten (Azure Content Understanding).
  - Adresssuche (Azure Maps).
  - Anmeldung und Nutzerverwaltung (Microsoft Entra External ID, Microsoft Graph).
  - Systembenachrichtigungen per E-Mail (Azure Communication Services): Guthabenwarnungen an die Administratoren des Kunden sowie Benachrichtigungen an den Auftragsverarbeiter selbst, etwa Fristerinnerungen der Projektsteuerung und Ankündigungen fälliger Kontolöschungen mit den betroffenen Konten.
  - Office-Add-in: Laden der Office-Bibliothek von Microsoft.
  - E-Mail-Kommunikation mit dem Kunden im Support (Microsoft 365).
- **Verarbeitungsort:**
  - Betrieb, Speicherung und Sicherungen: Azure-Region Westeuropa (Niederlande); Schlüsseltresor: Deutschland West-Mitte. Die zusätzliche Sicherung außerhalb der Produktivumgebung liegt georedundant auch in der gepaarten Region Nordeuropa (Irland), innerhalb der Europäischen Union.
  - Azure OpenAI: ausschließlich Bereitstellungen in der EU-Datenzone (Bereitstellungsart „Data Zone Standard“, Regionen Schweden Mitte, Frankreich Mitte, Polen Mitte, Deutschland West-Mitte, Italien Nord, Spanien Mitte) sowie eine regionale Bereitstellung in Schweden Mitte. Globale Bereitstellungen werden nicht genutzt. Zur Missbrauchserkennung speichert Microsoft Ein- und Ausgaben bis zu 30 Tage in der EU-Datenzone; eine Prüfung durch Menschen erfolgt nur bei Verdacht auf Missbrauch und durch Personal im Europäischen Wirtschaftsraum.
  - Texterkennung: Westeuropa, Frankreich Mitte, Deutschland West-Mitte. Bildbeschreibung: Schweden Mitte, Westeuropa. Adresssuche: EU-Endpunkt von Azure Maps. E-Mail-Versand: Azure-Datenstandort „Europe“.
  - Anmeldung (Entra External ID): Verzeichnis im Entra-Mandanten von AIMI mit Datenstandort „Europe“, angelegt mit dem Land Deutschland. Für diesen Standort speichert Microsoft nach eigenen Angaben den größten Teil der Daten des Verzeichnisses in Europa; die begrenzten Übermittlungen, die Microsoft dafür beschreibt, stehen oben unter „Zugriffe und Übermittlungen im Ausnahmefall“.
  - Office-Add-in: Die Office-Bibliothek lädt der Browser des Nutzers vom Content Delivery Network von Microsoft; Microsoft erhält dabei die IP-Adresse und die Browserdaten des Nutzers, keine Dokumente aus der Software. Die Bibliothek verbindet sich zudem mit Telemetriediensten von Microsoft; welche Daten sie

dabei sendet, bestimmt Microsoft. Einen Verarbeitungsort sagt der Auftragsverarbeiter dafür nicht zu.

  - E-Mail im Support (Microsoft 365): Microsoft-365-Mandant von AIMI mit Datenspeicherort Deutschland; Postfachinhalte speichert Microsoft im Ruhezustand in Deutschland.

- **Dauer der Verarbeitung:** Vertragslaufzeit und Fristen nach Anhang II. Ausnahme: Missbrauchserkennung bis zu 30 Tage (wie oben beschrieben).
- **Drittlandbezug und Grundlage:** Konzernmutter ist die Microsoft Corporation, USA. Grundlage für etwaige Übermittlungen sind die Datenschutzbedingungen von Microsoft für Produkte und Services (Data Protection Addendum) mit den EU-Standardvertragsklauseln; die Microsoft Corporation ist zusätzlich nach dem EU-US Data Privacy Framework zertifiziert.
- **Liste der Unterauftragsverarbeiter des Anbieters:** Microsoft Service Trust Portal, https://servicetrust.microsoft.com

2. Amazon Web Services EMEA SARL

- **Anschrift:** 38 Avenue John F. Kennedy, L-1855 Luxemburg
- **Kontakt Datenschutz:** aws-EU-privacy@amazon.com
- **Leistungen:** KI-Modelle der Claude-Reihe von Anthropic über Amazon Bedrock: Chat, Ausweichmodell der Dokumentenanalyse, Erstellung von Prüfergebnissen und Berichten sowie Antworten der Text-API. Daten werden nicht an Anthropic übermittelt.
- **Verarbeitungsort:** Europäische Union. Die Anfragen gehen an die Region Frankfurt am Main (eu-central-1) und werden über EU-Inferenzprofile ausgeführt; dabei verteilt AWS die Anfragen ausschließlich auf AWS-Regionen innerhalb der Europäischen Union. Weltweite Inferenzprofile werden nicht genutzt.
- **Dauer der Verarbeitung:** Vertragslaufzeit und Fristen nach Anhang II.
- **Drittlandbezug und Grundlage:** Konzernmutter ist die Amazon.com, Inc., USA. Grundlage für etwaige Übermittlungen ist der Datenschutz-Nachtrag von AWS (AWS GDPR Data Processing Addendum) mit den EU-Standardvertragsklauseln; Amazon.com, Inc. ist zusätzlich nach dem EU-US Data Privacy Framework zertifiziert.
- **Liste der Unterauftragsverarbeiter des Anbieters:** https://aws.amazon.com/compliance/sub-processors/

3. Google Cloud EMEA Limited

- **Anschrift:** 70 Sir John Rogerson's Quay, Dublin 2, Irland
- **Kontakt Datenschutz:** Datenschutzbeauftragter von Google Cloud, Kontaktformular https://support.google.com/cloud/contact/dpo
- **Leistungen:**

  - KI-Modelle der Gemini-Reihe über Vertex AI: wählbares Modell im Chat sowie Ausweichweg bei der Extraktion von Dokumentinhalten, bei Checklisten und bei der Bildbeschreibung.
  - KI-Modelle der Claude-Reihe (Anthropic) und der OpenAI-Reihe, die Google in Vertex AI anbietet.
  - Internetrecherche der Gemini-Modelle (Grounding mit der Google-Suche): Benötigt das Modell Informationen aus dem Internet, leitet es aus der Nutzerfrage eine Suchanfrage ab, die Google ausführt. Die Suchanfrage stellt die Software des Auftragsverarbeiters von ihren Servern aus, nicht das Endgerät des Nutzers; Google erhält dabei weder die IP-Adresse noch eine Kennung des Nutzers. Übermittelt wird nur die Suchanfrage, keine Dokumente. Vor der Suche entfernt der Auftragsverarbeiter die Namen natürlicher Personen und weitere personenbezogene Daten, die die Software in der Suchanfrage erkennt.
- **Verarbeitungsort:**
  - Gemini-Modelle: Europäische Union. Aufruf über den EU-Endpunkt von Vertex AI (Multiregion EU), ältere Modellversionen in den Regionen Niederlande (europe-west4) und Belgien (europe-west1). Speicherung und Modellverarbeitung erfolgen in der Europäischen Union.
  - Modelle der Claude-Reihe und der OpenAI-Reihe: Europäische Union. Aufruf ausschließlich über Regionen von Vertex AI in der Europäischen Union. Speicherung und Modellverarbeitung erfolgen in der Europäischen Union.
  - **Ausnahme Internetrecherche:** Die Suchanfrage, die das Modell aus der Nutzerfrage ableitet, verlässt den Verarbeitungsort der Europäischen Union; Google sagt für diesen Schritt keinen Verarbeitungsort zu. Namen natürlicher Personen und weitere personenbezogene Daten, die die Software erkennt, sind vor der Suche entfernt (siehe oben). Google speichert die Suchanfragen bis zu drei Tage zur Fehlersuche, nach eigenen Angaben ohne Zuordnung zu einem Kunden oder Nutzer; die Speicherung lässt sich nicht abschalten (Service Specific Terms, Ziffer 20(k)(ii)).
- **Dauer der Verarbeitung:** Vertragslaufzeit und Fristen nach Anhang II. Ausnahme: abgeleitete Suchanfragen der Internetrecherche bis zu drei Tage (wie oben beschrieben).
- **Drittlandbezug und Grundlage:** Konzernmutter ist die Google LLC, USA. Grundlage für etwaige Übermittlungen ist der Datenverarbeitungsnachtrag von Google Cloud (Cloud Data Processing Addendum) mit den EU-Standardvertragsklauseln; Google LLC ist zusätzlich nach dem EU-US Data Privacy Framework zertifiziert.
- **Liste der Unterauftragsverarbeiter des Anbieters:** https://cloud.google.com/terms/subprocessors