

Stand 27.11.2025



Claid Legal

Vertraulichkeitsvereinbarung

Nutzung „Claid Legal“

zwischen

[...]

(im Folgenden: „Auftraggeber“)

und

Claid Technologies UG (haftungsbeschränkt), Lemsahler Bargweg 16, 22397 Hamburg
(im Folgenden: „Auftragnehmer“)

Diese Vertraulichkeitsvereinbarung wurde geschlossen am [...] zwischen [...] und der **Claid Technologies UG (haftungsbeschränkt)**. Sie wurde maschinell erstellt und ist ohne Unterschrift rechtsgültig.

Der Auftraggeber plant, die KI-Plattform "Claid Legal" des Auftragnehmers zur Unterstützung der eigenen anwaltlichen Mandatsbearbeitung einzusetzen. Diese Plattform wurde speziell für juristische Zwecke und anwaltliche Anwender entwickelt, wobei der Auftragnehmer die Konformität mit § 43e BRAO zusichert. Im Rahmen der Plattformnutzung kann es technisch bedingt dazu kommen, dass der Auftragnehmer mit Tatsachen in Berührung kommt, die der Verschwiegenheitspflicht des Auftraggebers (bzw. der dort tätigen Berufsträger) gemäß § 43a Abs.2 S.1 BRAO unterliegen. Um die Anforderungen aus §§ 43a, 43e BRAO zu erfüllen und den Schutz vertraulicher Informationen sicherzustellen, vereinbaren die Parteien Folgendes:

- (1) Der Auftragnehmer verpflichtet sich zur Verschwiegenheit über sämtliche Tatsachen, die ihm im Rahmen der Vertragserfüllung bekannt werden und die sich direkt oder indirekt auf Mandate und Mandanten des Auftraggebers sowie auf alle sonstigen Informationen beziehen, die dem Auftraggeber in Ausübung seines Berufs zur Kenntnis gelangt sind und nicht offenkundig sind oder aufgrund ihrer Bedeutung keiner Geheimhaltung bedürfen.
- (2) Bei Unklarheiten bezüglich Inhalt und Umfang der Verschwiegenheitspflicht wird der Auftragnehmer den Auftraggeber unverzüglich informieren und dessen diesbezügliche Anweisungen befolgen.

- (3) Die Verschwiegenheitspflicht gilt unabhängig von der Art und Weise, wie der Auftragnehmer Kenntnis von den Tatsachen erlangt hat. Sie ist zeitlich unbegrenzt (also auch nach Beendigung des Vertrags und/oder des jeweiligen Mandatsverhältnisses) und gegenüber jedermann gültig.
- (4) Der Auftragnehmer wird seine Mitarbeiter und etwaig eingesetzte Subdienstleister, soweit diese im Rahmen der Auftragsdurchführung mit Daten oder Tatsachen in Berührung kommen, die der Verschwiegenheitspflicht des Auftraggebers (bzw. der dort tätigen Berufsträger) unterliegen, entsprechend Abs. 1 in Textform zur Verschwiegenheit verpflichten. Eine Weitergabe vertraulicher Informationen an Subdienstleister, die nicht selbst der vorstehend genannten Verschwiegenheitspflicht unterliegen, erfolgt ausschließlich nach ausdrücklicher, gesonderter Einwilligung des Nutzers für den jeweils konkreten Zweck (z. B. Durchführung von Websuchen) und bedarf vor jeder Übermittlung einer erneuten Bestätigung durch den Nutzer.
- (5) Der Auftragnehmer darf sich nur insoweit Kenntnis von vertraulichen Informationen verschaffen, als dies für die im Hauptvertrag festgelegten Verpflichtungen erforderlich ist. Dies bedeutet insbesondere, dass die individuellen Dateneingaben des Auftraggebers auf der Plattform und die daraus resultierenden Datenausgaben (z.B. im Rahmen der Chatbot- oder KI-Assistenten-Funktionen) vom Auftragnehmer jeweils nur für die Dauer des jeweiligen Nutzungsvorgangs (dies umfasst die vom Nutzer eingestellte Speicherdauer der Vorgänge) gespeichert werden dürfen.

Soweit vom Nutzer hochgeladene Daten (z. B. Vertragsdokumente) gespeichert werden, müssen sie vom Auftragnehmer auf der Plattform endgültig gelöscht werden, sobald der jeweilige User sie in seinem Profil löscht, spätestens jedoch nach der in den Einstellungen festgelegten Zeit. Ein- und Ausgabedaten oder von Nutzern zugespeicherte Daten dürfen ausschließlich für die vom User veranlasste Plattform-Nutzung verwendet werden.

- (6) Der Auftraggeber belehrt den Auftragnehmer hiermit, dass der Bruch der Verschwiegenheit oder die Verwertung fremder Geheimnisse durch den Auftragnehmer für diesen strafbar ist (§§ 203 Abs. 1, Abs. 4 S. 1 StGB, § 204 StGB) und mit Freiheitsstrafe bis zu einem Jahr, im Fall von § 204 StGB mit Freiheitsstrafe bis zu zwei Jahren, oder mit Geldstrafe geahndet werden kann. Die Strafandrohung erhöht sich gem. § 204 Abs. 6 StGB auf Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe, sofern der Auftragnehmer in Bereicherungsabsicht, auch wenn sie zu Gunsten Dritter bestehen sollte, handelt, oder die Absicht hat, durch die Tat einen anderen zu schädigen. Handelt es sich beim Auftragnehmer nicht um eine natürliche Person, trifft die vorstehende Strafandrohung die für den Auftragnehmer mitwirkenden Personen. Dem Auftragnehmer ist auch bekannt, dass nach § 203 Abs. 4 S. 2 Nr. 3 StGB die gleiche Strafbarkeit besteht, wenn im Falle des vorstehenden Abs. 6 eine weitere Person ein fremdes Geheimnis offenbart, und der Auftragnehmer nicht dafür Sorge getragen hat, dass diese Person zur Verschwiegenheit verpflichtet wurde.
- (7) Der Auftraggeber belehrt den Auftragnehmer vorsorglich, dass sich mitwirkende Personen im Falle einer entgegen Abs. 6 vorgenommenen Einschaltung weiterer Personen bei Strafandrohung von Freiheitsstrafe bis zu einem Jahr oder Geldstrafe strafbar machen, wenn diese weitere Person die Verschwiegenheit gem. Abs. 1 bricht, und die mitwirkende Person zugleich nicht dafür Sorge getragen hat, dass erstere zur Verschwiegenheit verpflichtet wurde (§§ 203 Abs. 1, Abs. 4 S. 2 Nr. 2 StGB). Die Strafandrohung erhöht sich auf Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe, sofern der Täter in Bereicherungsabsicht, auch wenn sie zu Gunsten Dritter bestehen sollte, handelt, oder die Absicht hat, durch die Tat einen anderen zu schädigen.

- (8) Der Auftragnehmer wird darauf hingewiesen, dass die sich in seinem Gewahrsam befindlichen Daten des Auftraggebers dem Beschlagnahmeverbot gemäß § 97 StPO unterliegen können. Die Daten dürfen nicht ohne das Einverständnis des Berufsheimnisträgers herausgegeben werden. Im Falle einer Sicherstellung/ Beschlagnahme durch deutsche Ermittlungs- und Aufsichtsbehörden wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren. Dasselbe gilt sinngemäß für die Sicherstellung anderer Sicherheitsbehörden unter der jeweils für diese geltenden Prozessordnung. Des Weiteren wurde der Auftragnehmer über die gesetzlichen Bestimmungen zum Zeugnisverweigerungsrecht gemäß § 53a StPO belehrt.

Der Auftragnehmer verpflichtet sich, sicherzustellen, dass alle Mitarbeiter, die im Rahmen ihrer Tätigkeit mit Daten des Auftraggebers in Berührung kommen oder bei denen ein solcher Kontakt nicht ausgeschlossen werden kann, bei Gerichten und Behörden über Tatsachen, die ihnen im Rahmen oder bei Gelegenheit ihrer Tätigkeit bekannt werden, ohne vorherige Befreiung von der Schweigepflicht weder aussagen noch sonstige Auskünfte erteilen.

- (9) Der Auftragnehmer wird angemessene organisatorische und technische Maßnahmen zum Schutz der Vertraulichkeit der vertraulichen Informationen vornehmen und aufrechterhalten. Er verpflichtet sich, vertrauliche Informationen angemessen gemäß akzeptierter Sicherheitsstandards nach dem aktuellen Stand der Technik zu schützen, jeweils mit dem mindestens entsprechend Art. 32 DSGVO anzuwendenden Niveau. Das Sicherheitsniveau darf hierbei vom Auftragnehmer zudem auch nicht geringer als bei eigenen vertraulichen Informationen angelegt werden.
- (10) Der Auftragnehmer verpflichtet sich ausdrücklich zu einer Vertragsdurchführung in der Weise, dass der Auftraggeber bei Nutzung der Plattform alle Rechte und Pflichten aus § 43a und § 43e der Bundesrechtsanwaltsordnung (BRAO) wahren und beachten kann. Sollten sich hieran berechnigte Zweifel ergeben, ist der Auftraggeber zur sofortigen Kündigung der laufenden Beauftragung unter zeitanteiliger Rückerstattung der Nutzungsgebühren berechnigt. Weitergehende Ansprüche bleiben unberührt. Sollte eine Behörde (z.B. Rechtsanwaltskammer, Staatsanwaltschaft, Datenschutzbehörde) eine Auskunft und/oder einen Nachweis bzgl. der Einhaltung der vorgenannten gesetzlichen Vorschriften und/oder der Pflichten/Maßnahmen aus dieser Vereinbarung fordern oder sollte dies in einem gerichtlichen/behördlichen Verfahren oder aufgrund einer Aufforderung durch einen Mandanten erforderlich werden, hat der Auftragnehmer im Rahmen des Zumutbaren derartige Auskünfte/Nachweise bereitzustellen bzw. mitzuwirken.

Vereinbarung zur Auftragsverarbeitung

Diese Vertraulichkeitsvereinbarung wurde geschlossen am [...] zwischen [...] und der **Claid Technologies UG (haftungsbeschränkt)**. Sie wurde maschinell erstellt und ist ohne Unterschrift rechtsgültig.

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.

ABSCHNITT II - PFLICHTEN DER PARTEIEN

Klausel 5

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 6

Pflichten der Parteien

6.1 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.

6.2 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.

6.3 Dauer der Verarbeitung personenbezogener Daten

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

6.4 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.

6.5 Sensible Daten

Falls die Verarbeitung personenbezogener 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.

6.6 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.

6.7 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 zwei Wochen 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.

6.8 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) Abweichend von (a) kann eine Übermittlung personenbezogener Daten an ein Drittland auch erfolgen, wenn und soweit der jeweilige Nutzer einer Datenverarbeitung im Drittland im Rahmen einer einzelnen Websuchanfrage ausdrücklich zugestimmt hat (Opt-In). Diese Einwilligung wird für jede einzelne Websuche vorab eingeholt.
- (c) 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 7

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:

- (i) 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;
 - (ii) 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;
 - (iii) 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;
 - (iv) 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 8

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.

8.1 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:

- (i) 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;
- (ii) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- (iii) 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.

8.2 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 9

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:
 - (i) 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;
 - (ii) 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;
 - (iii) 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.

ANHANG I - LISTE DER PARTEIEN

Verantwortlicher

[...]

Auftragsverarbeiter

Claid Technologies UG (haftungsbeschränkt), Lemsahler Bargweg 16, 22397 Hamburg

ANHANG II - BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden	Beschäftigte, Mandanten
Kategorien personenbezogener Daten, die verarbeitet werden	Sämtliche Kategorien personenbezogener Daten, die in dem von dem Nutzer eingegebenen Text und/oder hochgeladener Dokumente enthalten sind
Verarbeitete sensible Daten (falls zutreffend)	Ggf., falls in den von dem Nutzer eingegebenen Text und/oder hochgeladener Dokumente enthalten
Art der Verarbeitung	Einsatz einer Software, die mithilfe von künstlicher Intelligenz Antworten zu den von dem Nutzer eingegebenen Aufgaben generiert
Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden	Unterstützung bei der Recherche, Textarbeit mit Dokumenten und Emails
Dauer der Verarbeitung	Bestehen des Hauptvertrags mit dem Verantwortlichen
Verarbeitung durch (Unter-)Auftragsverarbeiter	Siehe die Angaben in Anhang IV

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Technische und organisatorische Sicherheitsmaßnahmen	
1. Zutrittskontrolle (Maßnahmen, die verhindern, dass Unbefugte Zutritt zu Gebäuden und Räumen bekommen, in denen sich Datenverarbeitungsanlagen befinden)	
	• Aufgrund des cloudbasierten Betriebs entfallen klassische physische Zutrittskontrollen. Die Cloudanbieter gewährleisten die physische Sicherheit. Wir verpflichten uns zur regelmäßigen Kontrolle unserer Dienstleister. • Endgerätesicherheit: • Festplattenverschlüsselung auf allen Laptops und mobilen Geräten • Automatische Bildschirmsperre nach kurzer Inaktivität
2. Zugangskontrolle (Maßnahmen, die sicherstellen, dass Unbefugten kein Zugang zu Datenverarbeitungssystemen haben)	
	• Komplexe Passwörter (mindestens 12 Zeichen, inkl. Groß- und Kleinbuchstaben sowie Sonderzeichen) • Aktivierung der Zwei-Faktor-Authentifizierung für alle BenutzerkontenAutomatische Kontosperrung nach mehreren fehlgeschlagenen Anmeldeversuchen. • Ihre Daten werden sowohl bei der Übertragung als auch bei der Speicherung verschlüsselt.
3. Zugriffskontrolle (Maßnahmen, die sicherstellen, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben)	
	• Umsetzung eines Berechtigungskonzepts nach dem Prinzip des minimalen Zugriffs. • Regelmäßige Überprüfung und Anpassung der Zugriffsrechte bei Änderungen der Zuständigkeiten.
4. Weitergabekontrolle (Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben)	
	• Unsere Webapp implementiert ein umfassendes Datenschutzkonzept mit Datenspeicherung und -verarbeitung ausschließlich in Deutschland. • Vor jeder Web-Anfrage erfolgt eine obligatorische manuelle Bestätigung durch den Nutzer, um die unbeabsichtigte Übermittlung sensibler Daten zu verhindern. • Sichere Übertragungsprotokolle wie HTTPS, SFTP oder VPN gewährleisten einen besonders geschützten Datentransfer. • Der Auftragnehmer arbeitet nur remote auf dem System des Auftraggebers. Es erfolgt keine Übertragung von Daten auf das System des Auftragnehmers ohne vorherige Zustimmung/Weisung des Auftraggebers.
5. Eingabekontrolle (Maßnahmen, die sicherstellen, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat)	
	Berechtigungskonzepte und Log-Dateien.
6. Auftragskontrolle (Maßnahmen, die sicherstellen, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden)	
	• Verträge zur Auftragsverarbeitung, die die Vorgaben des Auftraggebers präzise definieren. • Technische Einschränkungen im IT-System, die sicherstellen, dass die Verarbeitung ausschließlich für die vertraglich festgelegten Zwecke erfolgt.

	7. Verfügbarkeitskontrolle (Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Verantwortlichen stets verfügbar sind)
	• Unsere Daten werden in einem Server-Cluster bzw. in virtualisierten Cloud-Umgebungen gehostet, die redundante Systeme beinhalten. • Virtualisierung, Lastverteilung und Redundanz gewährleisten die erforderliche Fehlertoleranz.
	8. Trennungskontrolle (Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden)
	• Es erfolgt keine Datenübertragung ins eigene System des Auftragnehmers; die Verarbeitung erfolgt ausschließlich über die Webapp in einer sicheren Sandbox- oder segregierten Container-Umgebung.
9.	Pseudonymisierung, Verschlüsselung und Datentöschung • Verschlüsselung von ruhenden Daten: Schutz der Daten mittels AES bzw. RSA-Verschlüsselungsverfahren • Verschlüsselung von Daten beim Transport über interne Netze • Verschlüsselung von Daten beim Transport über öffentliche Netze: Absicherung der Datenübertragung durch TLS/SSL- oder VPN-Verbindungen • Datentöschung: Chat-Daten werden je nach Kundenvorgabe gespeichert, jedoch erfolgt eine automatische, unwiderrufliche Löschung aller Chat-Daten spätestens nach sechs Monaten. • Löschung und Backup-Richtlinie: Nicht mehr benötigte Daten werden umgehend gelöscht und eventuelle Backups gemäß den internen Sicherheitsstandards ebenfalls in einem definierten Zeitraum unwiderruflich entfernt.
	10. Regelmäßige Überprüfung (Maßnahmen zur Bewertung und Evaluierung der Wirksamkeit technisch-organisatorischer Maßnahmen)
	• Protokollierung, Auswertung und kontinuierliche Anpassung: ○ In unserer Cloudumgebung werden sicherheitsrelevante Vorgänge selektiv protokolliert und Sicherheitsvorfälle systematisch ausgewertet. ○ Gleichzeitig stellen fortlaufende interne Prüfprozesse sicher, dass alle Sicherheitsmaßnahmen stets den aktuellen technischen Standards und gesetzlichen Anforderungen entsprechen und regelmäßig angepasst werden.

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Name und Anschrift des Unterauftragnehmers	Beschreibung der Verarbeitung	Rechtsgrundlage für Datenübermittlung an Drittländer
Amazon Web Services (AWS) Amazon Web Services EMEA SARL 38 Av. John F. Kennedy Luxemburg	Claid Legal wird in einer modernen, skalierbaren AWS-Cloud gehostet, wobei ausschließlich deutsche Rechenzentren genutzt werden. Alle Kanzleidata werden in einer leistungsstarken und vertrauenswürdigen Umgebung verarbeitet – unter Einhaltung der strengen deutschen und europäischen Datenschutzbestimmungen. Um die Datenintegrität und Verfügbarkeit sicherzustellen, kommen umfassende Sicherheitsmaßnahmen zum Einsatz, einschließlich Richtlinien, die eine konsequente Löschung der Daten vorsehen, sobald sie nicht mehr benötigt werden.	Es findet keine Übermittlung von Ihren Mandantendaten an Drittländer statt. Rechtsgrundlage für etwaige technische Datenübertragungen (z.B. IP-Adressen) ist Art. 45 Abs. 1 DSGVO, Zertifizierung unter dem EU-U.S. Data Privacy Framework.
Microsoft Ireland Operations Limited One Microsoft Place South County Business Park Dublin 18 Ireland	Die Azure-Cloud wird in Deutschland bereitgestellt und dient hauptsächlich als LLM-Anbieter. Dabei werden alle Daten ausnahmslos und ausschließlich in Deutschland verarbeitet, um höchste Datenschutzstandards zu gewährleisten.	Es findet keine Übermittlung von Ihren Mandantendaten an Drittländer statt. Rechtsgrundlage für etwaige technische Datenübertragungen (z.B. IP-Adressen) ist Art. 45 Abs. 1 DSGVO, Zertifizierung unter dem EU-U.S. Data Privacy Framework.
Ionos SE Elgendorfer Str. 57 56410 Montabaur Deutschland	Ionos verarbeitet sämtliche Daten ausschließlich in deutschen Rechenzentren unter Einhaltung der deutschen und europäischen Datenschutzbestimmungen. Es findet keine Datenübermittlung in Drittländer statt, sodass die Daten jederzeit EU-rechtlich geschützt bleiben.	Es findet keine Übermittlung von Ihren Mandantendaten an Drittländer statt.
Fusionbase GmbH Agnes-Pockels-Bogen 1 80992 München Deutschland	Die Fusionbase GmbH unterstützt durch die Bereitstellung strukturierter und aggregierter Unternehmensinformationen, die im Rahmen der automatisierten Recherche verwendet werden.	Es findet keine Übermittlung von Ihren Mandantendaten an Drittländer statt.

Perplexity AI Inc. 140 Geary St, Floor 9 San Francisco, CA 94108 USA The Cube, Monahan Road, Cork, T12 H1XY Republik Irland, als EU-Vertreter gemäß Art. 27 DSGVO	Perplexity wird zur Durchführung ausführlicher Webrecherchen verwendet; eine Weitergabe von Daten erfolgt ausschließlich nach vorheriger manueller Bestätigung durch den jeweiligen Nutzer.	Es findet keine automatische Übermittlung personenbezogener Daten in Drittländer statt. Nach ausdrücklicher Einwilligung des Nutzers können konkrete Daten (z.B. Suchanfragen) übermittelt werden. Rechtsgrundlage hierfür ist Art. 49 Abs. 1 lit. a DSGVO (Einwilligung) und Art. 45 Abs. 1 DSGVO (EU-U.S. Data Privacy Framework).
---	--	---