Auftragsverarbeitungsvertrag

Stand November 2026

Zwischen

- **Auftraggeber** -

und

Intoconvo GmbH, Agnes-Pockels-Bogen 1, 80992 München

- **Auftragnehmer** -

- gemeinsam **die Parteien** genannt -

Präambel

(1) Der Auftragnehmer erbringt für den Auftraggeber Software-as-a-Service-Leistungen (SaaS) auf Grundlage des zwischen den Parteien geschlossenen Hauptvertrages. Gegenstand der Leistung ist die Bereitstellung der KI-Assistenz-Software „Clara“, die sich in die E-Mail-Infrastruktur des Auftraggebers integriert. Clara analysiert eingehende E-Mails und Anhänge mittels KI-Modellen, die über die in Anlage 3 genannten Cloud-Anbieter bereitgestellt werden, klassifiziert und verschlagwortet sie nach den Regeln des Auftraggebers, verschiebt sie in Ordner, leitet sie auf Weisung weiter, erzeugt Antwortentwürfe und Zusammenfassungen, legt Dokumente im angebundenen Dokumentenmanagementsystem (z. B. DATEV DMS) ab und verarbeitet Spracheingaben (Diktat).

(2) Im Rahmen der Leistungserbringung hat der Auftragnehmer Zugriff auf personenbezogene Daten, die der Auftraggeber als Verantwortlicher verarbeitet. Da der Auftraggeber als Berufsträger besonderen Verschwiegenheitspflichten (u. a. § 203 StGB) unterliegt, konkretisiert dieser Vertrag die Rechte und Pflichten der Parteien zum Schutz dieser Daten gemäß Art. 28 DSGVO.

§ 1 Gegenstand der Beauftragung

(1) Der Auftragnehmer erbringt für den Auftraggeber auf Grundlage des zwischen den Parteien geschlossenen Hauptvertrages Leistungen und verarbeitet dabei Datenbestände, die unter Umständen auch personenbezogene Daten i.S.v. Art. 4 Nr. 1 DSGVO beinhalten können. Die Verarbeitung erfolgt ausschließlich im Auftrag und nach Weisung des Auftraggebers. Dieser Vertrag geht im Fall von Widersprüchen anderen vertraglichen Vereinbarungen der Parteien vor und konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer.

(2) Dieser Vertrag gilt auch für die Konstellation, dass der Auftraggeber selbst nicht Verantwortlicher i.S.v. Art. 4 Nr. 7 DSGVO sondern Auftragsverarbeiter i.S.v. Art. 4 Nr. 8 DSGVO ist und seine datenschutzrechtlichen Pflichten aus dem Verhältnis zum Verantwortlichen auf den Auftragnehmer als weiteren Auftragsverarbeiter gem. Art. 28 Abs. 4 DSGVO auferlegt. Die Regelungen dieses Vertrages sind, sofern sie sich auf den Verantwortlichen beziehen, entsprechend anzuwenden.

§ 2 Umfang, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen

(1) Die Verarbeitung der personenbezogenen Daten im Rahmen der Auftragsverarbeitung erfolgt entsprechend der in der Präambel und unter § 1 aufgeführten Tätigkeiten zu Art und Zweck der Datenverarbeitung. Sie bezieht sich auf die in Anlage 1 festgelegten Arten der personenbezogenen Daten.

(2) Ferner besteht bei bestimmten Leistungen des Auftragnehmers die Möglichkeit der Kenntnisnahme personenbezogener Daten des Auftraggebers aufgrund der Tätigkeit des Auftragnehmers auf Systemen des Auftraggebers. Auch für diese Fälle finden die Regelungen dieses Vertrages Anwendung.

(3) Zu den Zwecken der Verarbeitung gehört auch die kundenspezifische Analyse von E-Mail-Inhalten zur Erstellung, Verfeinerung und Anpassung von Regeln für den Auftraggeber. Diese Analysen erfolgen ausschließlich kundenspezifisch; eine Verwendung der Daten oder Analyseergebnisse für andere Auftraggeber des Auftragnehmers oder für eigene Zwecke des Auftragnehmers findet nicht statt.

(4) Bei der Analyse durch KI-Modelle setzt der Auftragnehmer dem Stand der Technik entsprechende Maßnahmen ein, um die Verarbeitung personenbezogener und mandantenbezogener Inhalte auf das für die jeweilige Analyseaufgabe erforderliche Maß zu beschränken.

§ 3 Ort und Dauer der Auftragsverarbeitung

(1) Die Verarbeitung der personenbezogenen Daten findet im Gebiet der Bundesrepublik Deutschland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und eine entsprechende Weisung vorliegt. Die Genehmigung der in Anlage 3 genannten Unterauftragsverarbeiter gilt insoweit als Weisung.

(2) Dieser Vertrag gilt für die Laufzeit des Hauptvertrages. Bei einer Beendigung dieses Vertrages gelten die Bestimmungen dieses Vertrags sinngemäß fort, sofern der Auftragnehmer in der Beendigungsphase noch personenbezogene Daten des Auftraggebers verarbeitet.

§ 4 Verantwortlichkeit und Weisungsrecht des Auftraggebers

(1) Der Auftraggeber ist für die Verarbeitungen der Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO. Er ist für die Einhaltung der

gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Modalitäten der Weitergabe der Daten an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung, verantwortlich.

(2) Der Auftraggeber hat jederzeit das Recht, ergänzende Weisungen über Art, Umfang und Verfahren der Verarbeitung der personenbezogenen Daten zu erteilen. Weisungen können mündlich oder in Textform erfolgen. Mündliche Weisungen des Auftraggebers sind durch diesen unverzüglich in Textform zu bestätigen.

(3) Der Auftraggeber hat den Auftragnehmer unverzüglich unter Angabe der Gründe zu informieren, wenn er in den Auftragsergebnissen oder hinsichtlich der Tätigkeit des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich der Vorgaben dieses Vertrages oder der anwendbaren datenschutzrechtlichen Bestimmungen feststellt.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich in Textform informieren, wenn nach seiner Auffassung eine vom Auftraggeber erteilte Weisung gegen gesetzliche Regelungen verstößt. Solange die Parteien die Bedenken des Auftragnehmers nicht ausgeräumt haben, ist der Auftragnehmer berechtigt, die Durchführung der betreffenden Weisung auszusetzen. Wenn die Parteien keine Einigung erzielen können und der Auftraggeber an seiner Weisung festhält, ist der Auftragnehmer zu einer Kündigung dieses Vertrages mit angemessener Frist von mindestens einem Monat berechtigt.

(5) Sofern der Auftragnehmer der Auffassung sein sollte, eine Weisung des Auftraggebers aus technischen Gründen nicht befolgen zu können, wird er den Auftraggeber hierüber in Textform informieren und sich zum weiteren Vorgehen mit diesem abstimmen.

§ 5 Pflichten des Auftragnehmers

(1) Jegliche Verarbeitung der personenbezogenen Daten erfolgt ausschließlich entsprechend den vereinbarten Vorgaben sowie den vom Auftraggeber ggf. separat erteilten Weisungen. Dies gilt auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. Dieser Absatz 1 gilt nicht, wenn der Auftragnehmer zu der Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftragnehmer hat einen externen Datenschutzbeauftragten benannt: Gregor Klar, brainosphere 1 GmbH. Er ist erreichbar unter datenschutz@intoconvo.com. Ansprechpartner des Auftragnehmers für diesen Vertrag ist Elias Bienek, elias.bienek@intoconvo.com.

(3) Der Auftragnehmer hat die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit zu verpflichten, sofern sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Umfang der Verpflichtung hat in einem angemessenen Verhältnis zu den verarbeiteten personenbezogenen Daten und den Folgen einer etwaigen Verletzung des Schutzes der personenbezogenen Daten zu stehen. Sie hat sich ferner auf alle personenbezogenen Daten zu beziehen, die der Auftragnehmer für den Auftraggeber verarbeitet. Der Inhalt und die Tatsache der Verpflichtung ist dem Auftraggeber auf Anforderung nachzuweisen.

(4) Der Auftragnehmer wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten unterstützen.

(5) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung, Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden oder ist es zu entsprechenden Maßnahmen gekommen, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber umfassend zu informieren, es sei denn, dies ist ihm gesetzlich nicht gestattet. Ferner ist der Auftragnehmer verpflichtet, alle insoweit relevanten Dritten darauf hinzuweisen, dass es sich bei den Daten um personenbezogene Daten handelt, für die der Auftraggeber Verantwortlicher ist und er selbst nur als Auftragsverarbeiter tätig wird.

§ 6 Besondere Geheimnisschutzverpflichtung (§ 203 StGB)

(1) Im Rahmen dieses Vertrages könnten auch Daten verarbeitet werden, die in den Anwendungsbereich von § 203 StGB fallen und dem dort geregelten Geheimnisschutz (im Folgenden „Geheimnisschutzdaten“) unterliegen. Der Auftragnehmer verpflichtet sich, über Geheimnisschutzdaten Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit einer der in § 203 StGB genannten Berufsgruppen mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1 StGB. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

(2) Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z. B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben,

die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden.

(3) Der Auftragnehmer wird darauf hingewiesen, dass Geheimnisschutzdaten, die er im Auftrag verarbeitet, u.U. dem Zeugnisverweigerungsrecht von sogenannten mitwirkenden Personen unterliegen (§ 53a StPO). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der Auftragnehmer unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

(4) Der Auftragnehmer wird darauf hingewiesen, dass die sich in seinem Gewahrsam befindenden Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers herausgegeben werden. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

§ 7 Einsatz von KI-Modellen

(1) Der Auftragnehmer setzt zur Leistungserbringung KI-Modelle ein, die über die in Anlage 3 benannten Unterauftragsverarbeiter Amazon Web Services, Google Cloud und Mistral AI bereitgestellt werden (im Folgenden „KI-Anbieter"). Die Verarbeitung der Kundendaten durch KI-Anbieter erfolgt ausschließlich innerhalb der Europäischen Union oder des EWR. Die konkret eingesetzten Modelle teilt der Auftragnehmer auf Anfrage mit. Der Wechsel zu einem anderen Modell desselben KI-Anbieters, das in einer der in Anlage 3 genannten Regionen betrieben wird, ist keine Änderung im Sinne von § 12 Abs. 2.

(2) Der Auftragnehmer stellt vertraglich sicher, dass KI-Anbieter Kundendaten weder zum Training ihrer Modelle verwenden noch dauerhaft speichern. Maßgeblich sind die mit den jeweiligen KI-Anbietern geschlossenen Datenverarbeitungsverträge (insbesondere das Google Cloud Data Processing Addendum, das AWS Data Processing Addendum und das Mistral AI Data Processing Addendum), die dem Auftraggeber auf Anforderung zur Verfügung gestellt werden.

(3) Der Auftragnehmer ist gegenüber dem Auftraggeber dafür verantwortlich, dass die KI-Anbieter ihre datenschutzrechtlichen Pflichten einhalten. Der Auftraggeber muss keine eigenen Auftragsverarbeitungsverträge mit KI-Anbietern schließen.

(4) Clara ist nach Einschätzung des Auftragnehmers kein Hochrisiko-KI-System im Sinne von Art. 6 in Verbindung mit Anhang III der Verordnung (EU) 2024/1689 (KI-VO) und wird nicht als solches angeboten. Clara trifft keine Entscheidungen über natürliche Personen; Arbeitsergebnisse sind Vorschläge, die vom Auftraggeber geprüft werden. Der Auftraggeber setzt Clara nicht für die in Anhang III KI-VO genannten Zwecke ein. Ändert sich die Einstufung, insbesondere durch Änderungen der KI-VO, behördliche Leitlinien oder den Funktionsumfang von Clara, informiert der Auftragnehmer den Auftraggeber unverzüglich.

§ 8 Sicherheit der Verarbeitung

(1) Der Auftragnehmer ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen, insbesondere geeignete technische und organisatorische Maßnahmen (Anlage 2), um ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau zu gewährleisten. Er hat die Einhaltung dieser Vorgaben dem Auftraggeber auf dessen Verlangen mit geeigneten Mitteln nachzuweisen.

(2) Der Auftragnehmer ist zur Anpassung an geänderte technische oder rechtliche Gegebenheiten berechtigt, Änderungen an den in Anlage 2 beschriebenen Maßnahmen vorzunehmen. Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen, eine Erhöhung der Risiken für die Rechte und Freiheiten der von der Verarbeitung Betroffenen oder generell eine Reduktion des vereinbarten Schutzniveaus mit sich bringen könnten, bedürfen der Zustimmung des Auftraggebers. Andere Änderungen, insbesondere eine Verbesserung der ergriffenen Maßnahmen, können vom Auftragnehmer ohne Zustimmung des Auftraggebers umgesetzt werden. Nach Vornahme solcher Änderungen passt der Auftragnehmer die Anlage 2 entsprechend an und übermittelt die jeweils aktuelle Version der Anlage 2 unverzüglich dem Auftraggeber.

§ 9 Betroffenenrechte

(1) Der Auftragnehmer wird, soweit es ihm möglich ist, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel 3 der DSGVO genannten Rechte der betroffenen Personen nachzukommen. Hierfür hat der Auftraggeber den Auftragnehmer in Textform zu informieren, welche Unterstützungshandlung des Auftragnehmers er benötigt und diesem insoweit die Daten zu überlassen, die zur Erfüllung der Anfrage erforderlich sind. Der Auftragnehmer erbringt seine Unterstützungshandlung in angemessener Frist, so dass der Auftraggeber die ihm obliegenden Fristen wahren kann. Er hat den Auftraggeber unverzüglich unter Angabe der Gründe zu informieren, wenn er sich nicht in der Lage sieht, die verlangte Unterstützungshandlung zu erbringen.

(2) Wenn ein Betroffener sich zur Ausübung der diesem aus Kapitel 3 der DSGVO zustehenden Rechte unmittelbar an den Auftragnehmer wenden sollte, wird der Auftragnehmer diesen an den Auftraggeber verweisen, soweit ihm die Zuordnung zu diesem möglich ist. Sollte ihm eine Zuordnung nicht möglich und der Auftragnehmer auch nicht als Verantwortlicher unmittelbar gegenüber dem Betroffenen aus Kapitel 3 der

DSGVO verpflichtet sein, wird er ihn darüber informieren, dass er als Auftragsverarbeiter für Dritte tätig ist und er den Dritten hinsichtlich des Betroffenen nicht identifizieren kann. Sofern und soweit der Auftragnehmer gegenüber dem Betroffenen selbst als Verantwortlicher nach Kapitel 3 der DSGVO verpflichtet ist, obliegt die Erfüllung der entsprechenden Verpflichtungen alleine dem Auftragnehmer als Verantwortlichen.

§ 10 Kontrollrechte des Auftraggebers

(1) Dem Auftraggeber stehen alle Kontrollrechte, insbesondere Inspektionen, zu, die zur Wahrung der ihm nach den Vorgaben der DSGVO obliegenden Pflichten erforderlich sind. Das Kontrollrecht ist grundsätzlich mit einer angemessenen Ankündigungsfrist und zu den üblichen Geschäftszeiten des Auftragnehmers auszuüben. Unangekündigte Kontrollen sind zulässig, wenn andernfalls der Kontrollzweck gefährdet erschiene. Der Auftragnehmer ist zur Reduktion der Auswirkungen von Inspektionen auf seinen Geschäftsbetrieb berechtigt, diese mit denen anderer Auftraggeber zu verbinden, soweit dies dem Auftraggeber zumutbar ist (z. B. gemeinsame Inspektionstermine, die in angemessener Frist durchgeführt werden). Der Auftraggeber wird Sorge dafür tragen, dass Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers nicht unverhältnismäßig zu stören.

(2) Der Auftraggeber ist berechtigt, die Ausübung der Kontrollrechte auf einen von diesem beauftragten Dritten zu übertragen. Sollte der Dritte in einem unmittelbaren Wettbewerbsverhältnis zum Auftragnehmer stehen, hat dieser gegen dessen Tätigkeit ein Einspruchsrecht.

(3) Der Auftragnehmer hat an der Ausübung der Kontrollrechte im erforderlichen Umfang mitzuwirken. Er darf Kontrollen durch den Auftraggeber von der Unterzeichnung einer üblichen und angemessenen Verschwiegenheitserklärung abhängig machen, soweit dies zum Schutz seiner Geschäftsgeheimnisse nach den gesetzlichen Vorgaben erforderlich ist.

(4) Der Auftragnehmer kann die Einhaltung der Pflichten aus diesem Vertrag gegenüber dem Auftraggeber auch durch Übersendung einer Selbstauskunft oder durch Vorlage eines geeigneten Zertifikats eines Sachverständigen nachweisen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung alle erforderlichen Auskünfte und Informationen bezüglich der Einhaltung seiner Pflichten aus diesem Vertrag zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen der Anlage 2 nachzuweisen. Der Nachweis solcher Maßnahmen kann durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder Zertifizierungen gemäß Art. 42 DSGVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit erfolgen.

§ 11 Maßnahmen von Aufsichtsbehörden

(1) Der Auftragnehmer informiert, soweit zulässig, den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen einer (Aufsichts-)Behörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt insbesondere, soweit eine Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Auftragsverarbeitung beim Auftragnehmer ermittelt.

(2) Soweit der Auftraggeber seinerseits einer Kontrolle der (Aufsichts-)Behörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer im erforderlichen Umfang zu unterstützen. Für die insoweit zu erbringenden Leistungen steht dem Auftragnehmer ein angemessenes, am Zeitaufwand orientiertes Entgelt zu, sofern und soweit er die entsprechende Kontrolle o.ä. nicht zu vertreten hat. Der Auftragnehmer darf die Erbringung der von ihm geschuldeten Leistungen nicht davon abhängig machen, dass der Auftraggeber eine bestimmte Vergütung anerkennt und/oder vorab leistet.

(3) Erhält der Auftragnehmer von einer Behörde oder einem Gericht ein Ersuchen auf Herausgabe von Daten des Auftraggebers, wird er die anfragende Stelle unverzüglich an den Auftraggeber verweisen. Soweit diesem Verweis gesetzliche oder behördliche Anordnungen entgegenstehen, prüft der Auftragnehmer das Ersuchen auf Plausibilität und gibt nur die Daten heraus, zu deren Herausgabe er nach dieser Prüfung verpflichtet ist. Eine vertiefte rechtliche Prüfung wird durch den Auftragnehmer nicht geschuldet. § 6 Abs. 3 und 4 bleiben unberührt.

§ 12 Unterauftragsverarbeiter

(1) Der Auftragnehmer setzt für die Verarbeitung die in der Anlage 3 benannten Unterauftragsverarbeiter ein. Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung für den Einsatz der benannten Unterauftragsverarbeiter.

(2) Der Auftragnehmer wird den Auftraggeber in Textform frühzeitig über Änderungen an der Beauftragung von Unterauftragsverarbeitern (Neu-Hinzuziehung oder Ersetzung) informieren. Zu diesem Zweck wird der Auftragnehmer dem Auftraggeber in Textform folgende Informationen übersenden: Beschreibung der geplanten Änderung; Name und Adresse des Unterauftragsverarbeiters; welche Leistungen der Unterauftragsverarbeiter erbringen soll und welche personenbezogenen Daten hiervon betroffen sind; den Inhalt der entsprechenden Vereinbarungen mit dem Unterauftragsverarbeiter sowie ggf. alle Nachweise zur Einhaltung des Kapitels 5 der DSGVO.

(3) Der Auftraggeber kann innerhalb einer Frist von drei Wochen

seit Zugang der Information der Änderung widersprechen. Der Auftragnehmer setzt die Änderung nicht vor Ablauf der Widerspruchsfrist um. Im Falle eines Widerspruchs ist der Auftragnehmer berechtigt, diesen Vertrag mit einer Frist von mindestens einem Monat zu kündigen, sofern die Änderung dem Auftraggeber zumutbar gewesen wäre und der Widerspruch dem Auftragnehmer unzumutbar ist. Zumutbarkeit für den Auftraggeber ist gegeben, wenn mit der Änderung keine Nachteile für ihn zu befürchten gewesen wären und insbesondere sichergestellt gewesen wäre, dass die Vorgaben dieses Vertrages und der DSGVO bei Umsetzung der Änderung weiter eingehalten worden wären. Unzumutbarkeit für den Auftragnehmer ist gegeben, wenn er seine Auftragsverarbeitungsleistungen als im Wesentlichen gleichförmigen Prozess für eine Vielzahl von Auftraggebern erbringt und individuelle Abweichungen bei den Unterauftragsverarbeitern für den Auftragnehmer nicht einfach umzusetzen sind.

(4) Der Auftragnehmer wird für Unterauftragsverarbeiter die in den Absätzen 2 und 4 des Art. 28 DSGVO genannten Bedingungen einhalten und dem Unterauftragsverarbeiter dieselben Datenschutzpflichten auferlegen, die in diesem Vertrag festgelegt sind. Der Auftragnehmer hat dies dem Auftraggeber auf dessen Anforderung hin nachzuweisen.

(5) Im Hinblick auf Geheimnisschutzdaten dürfen Unterauftragsverarbeiter im EU- und Nicht-EU-Ausland zur Erfüllung der gegenständlichen Datenverarbeitungen nur dann herangezogen werden, wenn der dort bestehende Schutz der Geheimnisse dem Schutz in Deutschland vergleichbar ist. Der Auftragnehmer wird Unterauftragsverarbeiter sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von Geheimnisschutzdaten erlangen könnten, schriftlich zur Geheimhaltung verpflichten. Der Auftragnehmer wird ferner etwaige Unterauftragsverarbeiter dazu verpflichten, sämtliche von diesen eingesetzten Personen und etwaige weitere Unterauftragsverarbeiter, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor unter § 6 genannten Grundsätzen zur Geheimhaltung zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren. Des Weiteren werden Unterauftragsverarbeiter über das bestehende Schweigerecht gemäß § 53a StPO sowie den Beschlagnahmeschutz gemäß § 97 StPO informiert; dies beinhaltet auch den Hinweis auf das Recht des Berufsgeheimnisträgers über dieses Recht zu entscheiden und die damit verbundene Pflicht, unverzüglich den Auftraggeber bzgl. der Wahrnehmung dieser Rechte zu kontaktieren. Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen.

§ 13 Verstoß gegen datenschutzrechtliche Vorschriften, Vereinbarungen oder Weisungen

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften, gegen die getroffenen Vereinbarungen und/oder die erteilten Weisungen unverzüglich, spätestens 48 Stunden nach erster Kenntnis, in Textform mitzuteilen. Die entsprechende Meldung soll zumindest folgende Informationen enthalten:

- Eine Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Art und Menge der betroffenen Daten sowie Kategorien der betroffenen Personen;
- Kontaktinformationen für konkret zuständige Personen und/oder weitere Ansprechpartner;
- Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- Eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Jegliche, etwaige erforderliche Meldung an eine Aufsichtsbehörde oder Information von Betroffenen obliegt allein dem Auftraggeber. Der Auftragnehmer wird hieran im erforderlichen Umfang mitwirken.

(3) Der Auftragnehmer ist weiter verpflichtet, den Verstoß im erforderlichen Umfang unverzüglich aufzuklären und dem Auftraggeber eine entsprechende Dokumentation zu überlassen. Die Dokumentation hat eine Darstellung zu umfassen, welche Maßnahmen der Auftragnehmer ergriffen hat, um weitere Verstöße zu unterbinden und warum er der Auffassung ist, dass die ergriffenen Maßnahmen ausreichend sind, um den Vorgaben dieses Vertrages und der gesetzlichen Vorschriften zu genügen.

§ 14 Vergütung des Auftragnehmers

Dem Auftragnehmer steht für die von ihm unter diesem Vertrag erbrachten Leistungen kein gesondertes Entgelt zu, sofern nicht anders in diesem Vertrag vereinbart.

§ 15 Haftung

Die Haftung der Parteien richtet sich im Übrigen nach den gesetzlichen Regelungen des Datenschutzrechts.

§ 16 Folgen der Vertragsbeendigung

(1) Der Auftragnehmer wird nach Abschluss der Erbringung der Verarbeitungsleistungen oder sonstigen Beendigung der Leistungserbringung alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen oder zurückgeben und die vorhandenen Kopien löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der Auftragnehmer unterliegt, eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Der Auftragnehmer hat die Durchführung der Löschung entsprechend den Vorgaben des Auftraggebers diesem zu bestätigen und auf Anforderung nachzuweisen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim

Auftragnehmer zu kontrollieren.

§ 17 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Jegliches Zurückbehaltungsrecht des Auftragnehmers hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ist im Übrigen ausgeschlossen.

Anlage 1 - Kategorien personenbezogener Daten & Personen

Kategorien personenbezogener Daten

- Stammdaten & Metadaten der Nutzer: Namen, E-Mail-Adressen, Microsoft-Tenant-IDs und technische Protokolldaten (Logfiles) von Mitarbeitern und sonstigen Nutzern des Auftraggebers.
- Kommunikations- und Inhaltsdaten (Input): Inhalte aus E-Mails (Betreff, Textkörper, Header-Informationen) und Dokumenten (Anhänge wie PDF, Word, Excel), die zur Analyse oder Bearbeitung an die Software übergeben werden.
- Spracheingaben (Diktat): Audiodaten, die zur Umwandlung in Text verarbeitet und nicht gespeichert werden, sowie die daraus erzeugten Texte.
- Daten aus dem angebundenen DATEV-System (nur bei aktivierter DATEV-Anbindung): Mandantenstammdaten, Dokumente aus DATEV DMS sowie, soweit vom Auftraggeber freigegeben, Daten aus Rechnungswesen und Lohn.
- Generierte Daten (Output): Vom System erstellte E-Mail-Entwürfe, Zusammenfassungen und Analyseergebnisse, die personenbezogene Informationen enthalten können.

Kategorien betroffener Personen

- Mitarbeiter und sonstige Nutzer des Auftraggebers
- Mandanten des Auftraggebers sowie deren Ansprechpartner und Mitarbeiter
- Externe Kommunikationspartner des Auftraggebers (z. B. Behörden, Finanzverwaltung, Sozialversicherungsträger, Lieferanten, sonstige Dritte), die mit dem Auftraggeber per E-Mail in Kontakt stehen
- Betroffene Personen, deren personenbezogene Daten in E-Mails oder deren Anhängen enthalten sind

Hinweis zu besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO):

E-Mail-Anhänge können besondere Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO enthalten (z. B. Gesundheitsdaten, Religionszugehörigkeit oder Angaben zu einer Schwerbehinderung in Lohn- und Gehaltsabrechnungen). Das Auslesen von Anhängen ist regelmäßiger Bestandteil der geschuldeten Leistung. Der Auftraggeber entscheidet, welche Postfächer angebunden werden, und stellt als Verantwortlicher sicher, dass die erforderlichen Rechtsgrundlagen (insbesondere Art. 9 Abs. 2 DSGVO) vorliegen.

Verarbeitung von Kontaktdaten des Auftraggebers in eigener Verantwortlichkeit:

Unbeschadet der konkret beauftragten Leistung verarbeitet der Auftragnehmer auch personenbezogene Daten von Beschäftigten des Auftraggebers (insbesondere Vor- und Nachnamen, Position beim Auftraggeber, Kommunikationsdaten (Telefonnummer und E-Mail-Adressen)). Diese personenbezogenen Daten unterfallen nicht der Auftragsverarbeitung, da sie durch den Auftragnehmer in Erfüllung seiner vertraglichen Pflichten als eigenständiger Verantwortlicher verarbeitet werden.

Anlage 2 - Technische und organisatorische Maßnahmen (TOM)

Vorbemerkung: Die Software „Clara“ wird als Software-as-a-Service (SaaS) bereitgestellt. Die physische Infrastruktur wird durch zertifizierte Cloud-Provider (Google Cloud Platform, Amazon Web Services) bereitgestellt. Der Auftragnehmer besitzt keine eigenen Rechenzentren.

1 Vertraulichkeit

1.1 Physische Zugangskontrolle: *Maßnahmen, um Unbefugten den Zutritt zu Rechenzentren zu verwehren.*

Technische Maßnahmen	Organisatorische Maßnahmen
Nutzung zertifizierter Rechenzentren: Hosting erfolgt ausschließlich in Hochsicherheits-Rechenzentren der Cloud-Provider (Google/AWS) mit biometrischen Scannern, Schleusen und 24/7-Überwachung.	Keine lokalen Server: Es werden keine Kundendaten auf lokalen Servern in den Büroräumen des Auftragnehmers gespeichert.
Alarmanlage in den Büroräumen des Auftragnehmers.	Clean-Desk-Policy: Verbot, sensible Akten oder Passwörter offen am Arbeitsplatz liegen zu lassen.

1.2 Logische Zugangskontrolle: *Maßnahmen, um unbefugte Systemnutzung zu verhindern.*

Technische Maßnahmen	Organisatorische Maßnahmen
Authentifizierung: Anmeldung über Microsoft Entra ID (Single Sign-On) oder mit E-Mail-Adresse und Passwort. Passwörter werden ausschließlich als Hash gespeichert. Zugangsdaten für IMAP- und Exchange-Postfächer werden mit AES-256-GCM verschlüsselt gespeichert.	Passwort-Richtlinie: Für interne Dienste gilt eine Mindestlänge von 12 Zeichen (administrative Zugänge 16 Zeichen); Passwörter werden in einem Passwort-Manager verwaltet.
Zwingende 2-Faktor-Authentifizierung (2FA) für alle administrativen Zugänge (Google Workspace, Google Cloud, AWS, GitHub).	Berechtigungskonzept: Zugriffsrechte werden restriktiv nach dem „Need-to-Know“-Prinzip vergeben.
Verschlüsselung der Endgeräte: Festplattenverschlüsselung (BitLocker/FileVault) auf allen Firmenlaptops.	Onboarding/Offboarding: Sofortiger Entzug aller Zugriffsrechte beim Austritt von Mitarbeitern.

1.3 Zugriffskontrolle: *Maßnahmen, dass Berechtigte nur auf ihre Daten zugreifen können.*

Technische Maßnahmen	Organisatorische Maßnahmen
Verschlüsselung (Data at Rest): Speicherung aller Daten in der Cloud erfolgt verschlüsselt nach AES-256 Standard. Zugangsdaten und Original-Inhalte von E-Mails werden zusätzlich auf Anwendungsebene mit AES-256-GCM verschlüsselt; der Schlüssel wird nicht in der Datenbank gespeichert.	Protokollierung: Administrative Zugriffe auf die Cloud-Infrastruktur werden über die Audit-Logs von Google Cloud und AWS protokolliert.
Logische Mandantentrennung: Technische Trennung der Daten verschiedener Kunden durch eindeutige IDs (Tenant-ID) und PostgreSQL Row-Level Security in der Datenbank.	Verpflichtung auf Vertraulichkeit: Alle Mitarbeiter sind vertraglich auf das Datengeheimnis und § 203 StGB verpflichtet.

2. Integrität

2.1 Weitergabekontrolle & Transport: *Maßnahmen gegen unbefugtes Lesen bei der Übertragung.*

Technische Maßnahmen	Organisatorische Maßnahmen
Verschlüsselung (Data in Transit): Jegliche Datenübertragung erfolgt via HTTPS/TLS (mindestens Version 1.2).	Kein Training mit Kundendaten: Vertragliche Zusicherung der KI-Anbieter, dass Kundendaten weder zum Training der Modelle verwendet noch dauerhaft gespeichert werden (§ 7 Abs. 2).
API-Sicherheit: Absicherung aller Schnittstellen durch OAuth2-Token.	Verbot privater Datenträger: Nutzung von privaten USB-Sticks ist untersagt.

2.2 Eingabekontrolle: *Nachvollziehbarkeit, wer Daten verändert hat.*

Technische Maßnahmen	Organisatorische Maßnahmen
System-Logs: Automatische Protokollierung von Dateneingaben, Änderungen und Löschungen inkl. Zeitstempel und User-ID.	Individuelle User-Accounts: Verbot von geteilten Accounts (Shared Accounts) für Administratoren.

2.3 Pseudonymisierung / Anonymisierung

Technische Maßnahmen	Organisatorische Maßnahmen
Automatisierte Erkennung und Maskierung direkter Identifikatoren	Dokumentation der eingesetzten Verfahren und regelmäßige Überprüfung der Wirksamkeit.

3. Verfügbarkeit und Belastbarkeit

Technische Maßnahmen	Organisatorische Maßnahmen
Redundanz: Dateien werden in zonenredundantem Speicher der Cloud-Provider abgelegt; Datenbank und Dateien werden zusätzlich täglich bei einem zweiten Anbieter gesichert.	Disaster Recovery Plan: Notfallplan zur Wiederherstellung des Betriebs bei Ausfall einer Cloud-Region.
Automatisierte Backups: Tägliche verschlüsselte Backups der Datenbank (Aufbewahrung 30 Tage, Point-in-Time Recovery über 7 Tage) sowie eine nächtliche verschlüsselte Kopie von Datenbank und Dateien bei einem zweiten Anbieter (AWS, Region Irland). In Clara gelöschte Daten sind spätestens nach 30 Tagen aus allen Sicherungen entfernt. Die Wiederherstellung wird regelmäßig getestet.	SLA-Monitoring: Laufende Überwachung der Verfügbarkeit der Cloud-Dienste.
DDoS-Schutz: Bereitstellung über den Google Cloud Load Balancer mit integriertem Schutz vor volumetrischen Angriffen.	

4. Verfahren zur regelmäßigen Überprüfung

Technische Maßnahmen	Organisatorische Maßnahmen
	Jährliche Evaluierung: Überprüfung der Sicherheitsmaßnahmen durch die Geschäftsführung.
	Auditierung von Sub-Dienstleistern: Regelmäßige Prüfung der Nachweise der Unterauftragsverarbeiter (insbesondere ISO 27001 und SOC 2 bei Google und AWS).

Anlage 3 – Unterauftragsverarbeiter

Firma / Unternehmen (Rechtsträger)	Anschrift	Dienstleistung (Leistung)	Ort der Datenverarbeitung
Google Cloud EMEA Ltd.	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Hosting von Anwendung, Datenbank und Dateien; KI-Modelle über Vertex AI	Europäische Union: Deutschland, Belgien, Niederlande und weitere EU-Staaten
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxemburg	KI-Modelle über Amazon Bedrock; Spracherkennung; E-Mail-Versand und -Empfang; Sicherungskopien	Europäische Union: Deutschland, Irland und weitere EU-Staaten
Mistral AI SAS	15 rue des Halles, 75001 Paris, Frankreich	Texterkennung (OCR) in PDF-Dokumenten über die Mistral-API (EU-Endpunkt)	Europäische Union / EWR (EU-Endpunkt von Mistral AI)
PostHog, Inc.*	2261 Market Street #4008, San Francisco, CA 94114, USA	Produktanalyse und Fehlerprotokolle	Europäische Union (Hosting in Frankfurt am Main)
Riecken Webservice & Application GmbH	Nussdorfer Straße 4/1/112, 1090 Wien, Österreich	DATEV-Anbindung (nur bei aktivierter DATEV-Anbindung über Riecken): Cloud Gateway für den Zugriff auf DATEVconnect.	Europäische Union / EWR
Klardaten GmbH	Kolonnenstraße 8, 10827 Berlin	DATEV-Anbindung (nur bei aktivierter DATEV-Anbindung über Klardaten): Klardaten-Connector für den Zugriff auf DATEVconnect.	Europäische Union / EWR

PostHog: PostHog erhält keine Inhalte aus E-Mails, Anhängen oder Chats. Texte, Eingaben und Attributwerte werden in Sitzungsaufzeichnungen vor der Übermittlung maskiert.

AWS verarbeitet über Amazon Bedrock E-Mail-Inhalte, Anhänge und Chat-Eingaben zur KI-Verarbeitung sowie über Amazon Transcribe Spracheingaben; die Audiodaten werden nicht gespeichert. Im Rahmen des Mailversands (Amazon SES) verarbeitet AWS die E-Mail-Adressen der Nutzer sowie Inhalte von System-, Verifikations- und Benachrichtigungsmails; Benachrichtigungen (z. B. Aufgaben-Erinnerungen oder Ergebnisse geplanter Abläufe) können Inhalte aus den angebundenen Postfächern enthalten. Zusätzlich läuft der optionale inbox@-Kanal über Amazon

SES: E-Mails, die Nutzer oder deren Mandanten aktiv an eine Clara-Inbox-Adresse senden (z. B. per Weiterleitung), werden von AWS entgegengenommen und in Amazon S3 gespeichert, bis sie nach § 16 dieses Vertrages oder auf Anforderung des Auftraggebers gelöscht werden. Darüber hinaus legt der Auftragnehmer täglich eine verschlüsselte Sicherungskopie der Datenbank und der in Clara gespeicherten Dateien in Amazon S3 ab. In Clara gelöschte Daten sind spätestens nach 30 Tagen auch aus den Sicherungskopien entfernt. Die KI-Verarbeitung über Amazon Bedrock und Amazon Transcribe findet in der Region Frankfurt (eu-central-1) statt, wobei Amazon Bedrock Anfragen auf weitere Rechenzentren innerhalb der EU verteilen kann; Mailversand, inbox@-Kanal und Sicherungskopien in der Region Irland (eu-west-1). Sämtliche Verarbeitung durch AWS erfolgt innerhalb der EU.

Mistral AI verarbeitet PDF-Dokumente (E-Mail-Anhänge, in Clara hochgeladene Dateien und Dokumente aus dem angebundenen DATEV-System) zur Texterkennung (OCR) über den EU-Endpunkt der Mistral-API. Für die Organisation des Auftragnehmers ist bei Mistral AI „Zero Data Retention“ aktiviert und die Verwendung von API-Daten zum Training abgeschaltet: Mistral AI speichert die übermittelten Dokumente nicht und verwendet sie nicht zum Training seiner Modelle. Mistral AI hat sich gegenüber dem Auftragnehmer schriftlich zur Vertraulichkeit von Berufsgeheimnissen nach § 203 StGB verpflichtet (Erklärung vom 28.10.2026). Sämtliche Verarbeitung durch Mistral AI erfolgt innerhalb der EU bzw. des EWR.

* Hinweis zu Drittstaatentransfers: PostHog, Inc. ist eine Gesellschaft mit Sitz in den USA. Die technische Datenverarbeitung erfolgt ausschließlich in der EU (Frankfurt am Main); gleichwohl kann ein potenzieller Zugriff durch die US-Gesellschaft nicht vollständig ausgeschlossen werden. Die Datenübermittlung erfolgt daher auf Grundlage des EU-US Data Privacy Framework (DPF), für das PostHog zertifiziert ist, sowie ergänzend auf Basis von EU-Standardvertragsklauseln (SCCs).