

ATLAS.ti Auftragsverarbeitungsvertrag

Präambel

Dieser Auftragsverarbeitungsvertrag regelt die Datenverarbeitung im Auftrag des Kunden durch die ATLAS.ti Scientific Software Development GmbH als Auftragsverarbeiter. Er wird durch Verweis in den Nutzungsbedingungen Bestandteil des jeweiligen Vertrages.

Begriffsbestimmungen

1.1 „Verantwortlicher“ ist gemäß Art. 4 Nr. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

1.2 „Auftragsverarbeiter“ ist gemäß Art. 4 Nr. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

1.3 „Personenbezogene Daten“ sind gemäß Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (nachfolgend „betroffene Person“) beziehen; als identifizierbar gilt eine Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

1.4 „Besonders sensible personenbezogene Daten“ sind personenbezogene Daten gemäß Art. 9 DSGVO, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit der betroffenen Personen hervorgehen, personenbezogene Daten gemäß Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen sowie genetische Daten gemäß Art. 4 Nr. 13 DSGVO, biometrische Daten gemäß Art. 4 Nr. 14 DSGVO, Gesundheitsdaten gemäß Art. 4 Nr. 15 DSGVO und Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

1.5 „Verarbeitung“ ist gemäß Art. 4 Nr. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das

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

1.6 „Aufsichtsbehörde“ ist gemäß Art. 4 Nr. 21 DSGVO eine von einem Mitgliedstaat gemäß Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

Gegenstand

2.1 Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich „Bereitstellung von Software“ auf der Grundlage des zwischen den Parteien geschlossenen Hauptvertrages. Im Rahmen des Hauptvertrages erhält der Auftragnehmer Zugang zu personenbezogenen Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Der Gegenstand der Verarbeitung, die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in Anlage 1 zu diesem Auftragsverarbeitungsvertrag festgelegt. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt dem Auftraggeber.

2.2 Die Parteien schließen diesen Auftragsverarbeitungsvertrag, um die gegenseitigen datenschutzrechtlichen Rechte und Pflichten zu konkretisieren. Im Zweifelsfall gehen die Regelungen dieses Vertrages den Regelungen des Hauptvertrages vor.

2.3 Die Regelungen dieses Auftragsverarbeitungsvertrages gelten für alle Tätigkeiten im Zusammenhang mit dem Hauptvertrag, bei denen der Auftragnehmer und seine Mitarbeiter oder die von ihm beauftragten Erfüllungsgehilfen mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für ihn erhoben wurden.

2.4 Dieser Auftragsverarbeitungsvertrag beginnt mit der Unterzeichnung; die Laufzeit dieses Auftragsverarbeitungsvertrages richtet sich nach der Laufzeit des Hauptvertrages, sofern sich nicht aus den nachfolgenden Bestimmungen darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

Weisungsbefugnis

3.1 Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrages und nach Weisung des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere im Hinblick auf die Übermittlung

personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Ist der Auftragnehmer nach dem Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu einer weitergehenden Verarbeitung verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

3.2 Die Weisungen des Auftraggebers ergeben sich zunächst aus diesem Vertrag und können nachfolgend durch Einzelweisungen in Schriftform oder Textform geändert, ergänzt oder ersetzt werden (Einzelweisungen). Der Auftraggeber ist jederzeit berechtigt, entsprechende Weisungen zu erteilen. Dies umfasst Weisungen zur Berichtigung, Löschung und Sperrung von Daten. Mündliche Weisungen sind unverzüglich in Schriftform oder Textform zu bestätigen.

3.3 Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die im Hauptvertrag vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

3.4 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Ausführung der betreffenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Ausführung einer offensichtlich rechtswidrigen Weisung verweigern.

Datenkategorien, betroffene Personen

Im Rahmen der Durchführung des Hauptvertrages erhält der Auftragnehmer Zugang zu den in **Anlage 1** bezeichneten personenbezogenen Daten. Die von der Datenverarbeitung betroffenen Personen sind ebenfalls in **Anlage 1** festgelegt.

Pflichten des Auftragnehmers

5.1 Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen zum Datenschutz zu beachten und Informationen aus der Sphäre des Auftraggebers nicht an Dritte weiterzugeben oder Dritten Zugang zu diesen zu gewähren. Unterlagen und Daten sind unter Berücksichtigung des Stands der Technik gegen unbefugten Zugriff zu sichern.

5.2 Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer trifft

alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gemäß Art. 32 DSGVO, insbesondere mindestens die in Anlage 2 aufgeführten Maßnahmen. Der Auftragnehmer behält sich das Recht vor, die getroffenen Sicherheitsmaßnahmen zu ändern, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

5.3 Den bei dem Auftragnehmer mit der Datenverarbeitung beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer verpflichtet alle von ihm mit der Verarbeitung und Erfüllung dieses Vertrages betrauten Personen (nachfolgend „Mitarbeiter“) entsprechend (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und stellt die Einhaltung dieser Verpflichtung mit der erforderlichen Sorgfalt sicher. Diese Verpflichtungen sind so zu gestalten, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer fortbestehen. Auf Verlangen sind dem Auftraggeber geeignete Nachweise über die Verpflichtungen in geeigneter Weise vorzulegen.

Informationspflichten des Auftragnehmers

6.1 Bei Störungen, dem Verdacht auf Datenschutzverstöße oder Verstöße gegen vertragliche Pflichten des Auftragnehmers, dem Verdacht auf sicherheitsrelevante Vorfälle oder sonstige Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten durch den Auftragnehmer, durch im Rahmen des Auftrags beim Auftragnehmer beschäftigte Personen oder durch Dritte hat der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform zu informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch eine Datenschutzaufsichtsbehörde. Die Meldung einer Verletzung des Schutzes personenbezogener Daten enthält mindestens folgende Angaben:

- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich einschließlich der Kategorien und der Anzahl der betroffenen Personen sowie der Kategorien und der Anzahl der betroffenen personenbezogenen Datensätze
- b) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

6.2 Der Auftragnehmer ergreift unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen, informiert den Auftraggeber hierüber und ersucht um weitere Weisungen.

6.3 Der Auftragnehmer ist ferner verpflichtet, dem Auftraggeber jederzeit Auskunft zu erteilen, soweit Daten des Auftraggebers von einer Verletzung gemäß Ziffer 6.1 betroffen sind.

6.4 Werden die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet, hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren, sofern dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. In diesem Zusammenhang informiert der Auftragnehmer unverzüglich alle zuständigen Stellen darüber, dass die Entscheidungsbefugnis über die Daten ausschließlich beim Auftraggeber als Verantwortlichem liegt.

6.5 Der Auftragnehmer informiert den Auftraggeber unverzüglich über jede wesentliche Änderung der Sicherheitsmaßnahmen gemäß Ziffer 5.2.

6.6 Über jeden Wechsel in der Person des Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist der Auftraggeber unverzüglich zu informieren.

6.7 Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis der im Auftrag des Auftraggebers durchgeführten Verarbeitungstätigkeiten, das alle nach Art. 30 Abs. 2 DSGVO erforderlichen Angaben enthält. Das Verzeichnis wird dem Auftraggeber auf Anfrage zur Verfügung gestellt.

6.8 Der Auftragnehmer wirkt in angemessenem Umfang bei der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber mit. Der Auftragnehmer hat dem Auftraggeber die erforderlichen Angaben in geeigneter Weise zur Verfügung zu stellen.

Kontrollrechte des Auftraggebers

7.1 Der Auftraggeber hat das Recht, jederzeit im erforderlichen Umfang zu überprüfen, ob der Auftragnehmer die gesetzlichen Bestimmungen zum Datenschutz und/oder die zwischen den Parteien vereinbarten vertraglichen Regelungen einhält und/oder ob der Auftragnehmer die Weisungen des Auftraggebers beachtet. Der Auftragnehmer ist berechtigt, die Einhaltung der in diesem Auftragsverarbeitungsvertrag

festgelegten Pflichten durch geeignete Mittel, einschließlich Selbstauskünften, Zertifikaten etc., nachzuweisen.

7.2 Der Auftragnehmer ist verpflichtet, dem Auftraggeber Auskunft zu erteilen, soweit dies zur Durchführung der Kontrolle im Sinne des vorstehenden Absatzes 1 erforderlich ist.

7.3 Sofern im Einzelfall erforderlich, kann der Auftraggeber eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die eingesetzten Datenverarbeitungssysteme und -programme verlangen.

7.4 Nach vorheriger Ankündigung und mit angemessener Vorlaufzeit kann der Auftraggeber die Kontrolle im Sinne des Absatzes 1 in den Geschäftsräumen des Auftragnehmers während der üblichen Geschäftszeiten durchführen. Der Auftraggeber stellt dabei sicher, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um den Betriebsablauf des Auftragnehmers nicht unverhältnismäßig zu stören. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Kontrollen sind vom Auftraggeber unter Angabe des Grundes zu begründen. Bei Vor-Ort-Kontrollen erstattet der Auftraggeber dem Auftragnehmer die entstandenen Aufwendungen einschließlich Personalkosten für die Betreuung und Begleitung der Prüfer vor Ort in angemessenem Umfang. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt. Der Auftragnehmer kann die Kontrollen von einer vorherigen Ankündigung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Vertraulichkeitsvereinbarung abhängig machen. Steht der vom Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zum Auftragnehmer, hat der Auftragnehmer ein Widerspruchsrecht.

7.5 Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstelle einer Vor-Ort-Kontrolle auch durch Vorlage eines geeigneten, aktuellen Prüfzertifikats, von Berichten oder Berichtsauszügen unabhängiger Stellen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder durch eine geeignete Zertifizierung erbracht werden, sofern der Prüfbericht es dem Auftraggeber ermöglicht, sich in angemessener Weise davon zu überzeugen, dass die technischen und organisatorischen Maßnahmen gemäß Anlage 2 zu diesem Auftragsverarbeitungsvertrag eingehalten werden. Hat der Auftraggeber berechtigte Zweifel an der

Geeignetheit des Prüfnachweises im Sinne von Satz 1, kann eine Vor-Ort-Kontrolle durch den Auftraggeber durchgeführt werden. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.

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

7.7 Der Auftragnehmer weist dem Auftraggeber auf Verlangen die Verpflichtung der Mitarbeiter gemäß Ziffer 5.3 nach.

Einsatz von Subunternehmern und Datenübermittlung

8.1 Der Auftragnehmer ist berechtigt, für die Verarbeitung der Daten des Auftraggebers Subunternehmer einzusetzen. Der Auftragnehmer hat die Subunternehmer sorgfältig auszuwählen und vor der Auftragserteilung zu prüfen, ob diese die zwischen dem Auftraggeber und dem Auftragnehmer getroffenen Vereinbarungen einhalten können. Insbesondere hat der Auftragnehmer vorab und regelmäßig während der Vertragslaufzeit zu prüfen, ob der Subunternehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.

8.2 Der Auftraggeber stimmt zu, dass der Auftragnehmer weitere Subunternehmer einsetzt oder Subunternehmer erforderlichenfalls austauscht. Der Auftragnehmer informiert den Auftraggeber über solche Änderungen mit angemessener Vorlaufzeit in elektronischer Form. Der Auftraggeber kann der Änderung aus wichtigem Grund innerhalb einer vom Auftragnehmer nach billigem Ermessen bestimmten angemessenen Frist widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Zustimmung zur Änderung als erteilt.

8.3 Der Auftragnehmer ist verpflichtet, vom Subunternehmer die Bestätigung einzuholen, dass dieser einen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat, sofern der Subunternehmer gesetzlich zur Benennung eines Datenschutzbeauftragten verpflichtet ist.

8.4 Der Auftragnehmer stellt sicher, dass die in diesem Auftragsverarbeitungsvertrag vereinbarten Regelungen sowie

ergänzende Weisungen des Auftraggebers auch für den Subunternehmer gelten.

8.5 Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollrechte des Auftraggebers und der Aufsichtsbehörden auch gegenüber dem Subunternehmer gelten und dass entsprechende Kontrollrechte des Auftraggebers und der Aufsichtsbehörden vereinbart werden. Darüber hinaus ist vertraglich zu vereinbaren, dass der Subunternehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

8.6 Als Subunternehmerverhältnisse im Sinne der Absätze 1 bis 5 gelten nicht Leistungen, die der Auftragnehmer als reine Nebenleistung zur Durchführung der Geschäftstätigkeit bei Dritten in Anspruch nimmt. Hierzu gehören beispielsweise Reinigungsdienste, reine Telekommunikationsdienstleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportdienstleistungen sowie Wachdienste. Der Auftragnehmer ist dennoch verpflichtet, auch bei Nebenleistungen Dritter sicherzustellen, dass angemessene Vorkehrungen sowie technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten getroffen wurden. Die Wartung und Pflege von IT-Systemen oder Anwendungen stellt ein genehmigungspflichtiges Subunternehmerverhältnis und eine Datenverarbeitung im Auftrag im Sinne des Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Leistungserbringung für den Auftraggeber genutzt werden, und wenn bei der Wartung auf im Auftrag des Auftraggebers verarbeitete personenbezogene Daten zugegriffen werden kann.

8.7 Der Auftraggeber erkennt an und stimmt zu, dass der Auftragnehmer Daten des Auftraggebers an seine Unterauftragsverarbeiter in Drittländer, einschließlich Länder außerhalb des EWR ohne Angemessenheitsbeschluss der Europäischen Kommission, übermitteln und dort verarbeiten darf, namentlich an OpenAI LLC, 3180 18th St, San Francisco, California, 94110, USA (generative KI-Analysefunktionen) und Deepgram, Inc., San Francisco, California, USA (Transkription von Audio- und Videoaufzeichnungen) und/oder andere KI-Anbieter. Der Auftragnehmer stellt sicher, dass solche Übermittlungen im Einklang mit dem anwendbaren Datenschutzrecht und diesem Auftragsverarbeitungsvertrag erfolgen. Insbesondere schließt der Auftragnehmer Standardvertragsklauseln gemäß Art. 46 Abs. 2 lit. c

DSGVO oder andere geeignete Garantien (wie verbindliche interne Datenschutzvorschriften gemäß Art. 47 DSGVO) ab. Ist ein Unterauftragsverarbeiter im Rahmen eines Angemessenheitsbeschlusses gemäß Art. 45 DSGVO zertifiziert, etwa nach dem EU-US Data Privacy Framework, kann die Übermittlung auch auf diesen Angemessenheitsbeschluss gestützt werden; die Standardvertragsklauseln bleiben als Rückfallgarantie bestehen.

Verarbeitung für KI-Funktionen

9.1 Nutzt der Auftraggeber KI-gestützte Funktionen der Software (einschließlich automatisierter Kodierung, Zusammenfassungen, dialogbasierter Dokumentenanalyse und Transkription), verarbeitet der Auftragnehmer die vom Auftraggeber übermittelten Inhalte ausschließlich zur Bereitstellung der angeforderten Funktion. Weder der Auftragnehmer noch – nach den vom Auftragnehmer geschlossenen Vereinbarungen – seine Unterauftragsverarbeiter verwenden solche Inhalte, um Modelle künstlicher Intelligenz zu trainieren, nachzutrainieren oder zu verbessern. Die KI-Unterauftragsverarbeiter des Auftragnehmers speichern übermittelte Inhalte nur temporär in dem Umfang, der zur Bereitstellung des Dienstes und zur Missbrauchserkennung erforderlich ist; auf Anfrage informiert der Auftragnehmer den Auftraggeber über die jeweils geltenden Speicherfristen seiner KI-Unterauftragsverarbeiter.

9.2 Der Auftragnehmer stellt dem Auftraggeber auf angemessene Anfrage die Informationen über die KI-gestützten Funktionen zur Verfügung, die der Auftraggeber zur Erfüllung seiner eigenen Pflichten nach der Verordnung (EU) 2024/1689 (KI-Verordnung), insbesondere der Transparenzpflichten, in angemessener Weise benötigt. Gesetzliche Informationspflichten des Auftragnehmers bleiben unberührt.

Rechte der betroffenen Personen

10.1 Für die Wahrung der Rechte der betroffenen Personen ist allein der Auftraggeber verantwortlich. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Möglichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Pflichten des Auftraggebers nach Art. 12 – 22 sowie 32 und 36 DSGVO.

10.2 Macht eine betroffene Person Rechte, wie das Recht auf Auskunft/Information, Berichtigung oder Löschung ihrer Daten, unmittelbar gegenüber dem Auftragnehmer geltend, reagiert der Auftragnehmer nicht eigenständig, sondern verweist die betroffene

Person unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

Vertraulichkeitspflichten

11.1 Beide Parteien verpflichten sich, alle im Zusammenhang mit der Durchführung dieses Auftragsverarbeitungsvertrages erhaltenen Informationen zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung dieses Auftragsverarbeitungsvertrages und/oder des Hauptvertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den vorgenannten Zwecken zu nutzen oder Dritten zugänglich zu machen.

11.2 Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweislich von Dritten ohne Verpflichtung zur Geheimhaltung erhalten hat oder die öffentlich bekannt sind.

Beendigung

Nach Beendigung des Hauptvertrages oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer dem Auftraggeber alle ihm überlassenen Unterlagen, Daten und Datenträger zurückzugeben oder – auf Verlangen des Auftraggebers und sofern keine Verpflichtung zur Speicherung personenbezogener Daten nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland besteht – zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren und auf Verlangen nachzuweisen.

Schlussbestimmungen

13.1 Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer (gemäß § 273 BGB) hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

13.2 Änderungen und Ergänzungen dieses Auftragsverarbeitungsvertrages und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – erfordern eine schriftliche Vereinbarung, die auch in elektronischer Form (Textform) erfolgen kann, sowie den ausdrücklichen Hinweis darauf, dass es sich um eine Änderung oder Ergänzung dieses Auftragsverarbeitungsvertrages handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

13.3 Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hiervon nicht berührt.

13.4 Dieser Vertrag unterliegt deutschem Recht.

Anlagen:

Anlage 1: Beschreibung der Verarbeitung

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 1: Beschreibung der Verarbeitung

1. Umfang und Zweck der Verarbeitung

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

Bereitstellung der Datenanalyseplattform des Auftragnehmers als SaaS, Dienste künstlicher Intelligenz, einschließlich KI-gestützter Analysefunktionen (automatisierte Kodierung, Zusammenfassungen, dialogbasierte Dokumentenanalyse) und KI-gestützter Transkription von Audio- und Videoaufzeichnungen

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Datenverarbeitung:

Daten, die der Auftraggeber mithilfe der Datenanalyseplattform des Auftragnehmers analysiert oder verarbeitet und deren Art der Auftraggeber nach eigenem Ermessen bestimmt und die beispielsweise insbesondere Daten zu Einrichtungen und Projekten des Auftraggebers, zu Testpersonen, Patienten und anderen Teilnehmern und betroffenen Personen im Rahmen wissenschaftlicher Studien und Forschungsprojekte umfassen können. Vom Auftraggeber zu Transkriptionszwecken hochgeladene Sprach- und Videoaufzeichnungen sowie die daraus erzeugten Transkripte; die Verarbeitung von Sprachaufzeichnungen ist auf die Transkription beschränkt, eine Sprechererkennung und eine biometrische Analyse im Sinne des Art. 4 Nr. 14, Art. 9 Abs. 1 DSGVO finden nicht statt.

3. Datenkategorien

Von der Datenverarbeitung betroffene Daten:

Datenkategorien, die der Auftraggeber mithilfe der Datenanalyseplattform des Auftragnehmers analysiert oder verarbeitet und deren Kategorien der Auftraggeber nach eigenem Ermessen bestimmt und die beispielsweise folgende Datenkategorien umfassen

können: Vor- und Nachname, Kontaktdaten, medizinische Daten, genetische Daten, biometrische Daten, sonstige besondere Kategorien personenbezogener Daten, Daten zu Lebensgewohnheiten und sonstigen Umständen, Informationen aus Interviews, Kundenfeedback und Verhaltensdaten.

4. Kategorien betroffener Personen

Von der Datenverarbeitung betroffene Personen:

Testpersonen, Patienten, Studienteilnehmer oder Interviewpartner, Mitarbeiter, sonstige Teilnehmer und betroffene Personen in Studien oder Forschungsprojekten sowie jede natürliche Person in den vom Auftraggeber analysierten Inhalten.

Anlage 1: Beschreibung der Verarbeitung

1. Umfang und Zweck der Verarbeitung

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

Bereitstellung der Datenanalyseplattform des Auftragnehmers als SaaS, Dienste künstlicher Intelligenz

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Datenverarbeitung:

Daten, die der Auftraggeber mithilfe der Datenanalyseplattform des Auftragnehmers analysiert oder verarbeitet und deren Art der Auftraggeber nach eigenem Ermessen bestimmt und die beispielsweise insbesondere Daten zu Einrichtungen und Projekten des Auftraggebers, zu Testpersonen, Patienten und anderen Teilnehmern und betroffenen Personen im Rahmen wissenschaftlicher Studien und Forschungsprojekte umfassen können.

3. Kategorien betroffener Personen

Von der Datenverarbeitung betroffene Personen:

Datenkategorien, die der Auftraggeber mithilfe der Datenanalyseplattform des Auftragnehmers analysiert oder verarbeitet und deren Kategorien der Auftraggeber nach eigenem Ermessen bestimmt und die beispielsweise folgende Datenkategorien umfassen können: Vor- und Nachname, Kontaktdaten, medizinische Daten, genetische Daten, biometrische Daten, sonstige besondere Kategorien personenbezogener Daten, Daten zu Lebensgewohnheiten und sonstigen Umständen,

Informationen aus Interviews, Kundenfeedback und Verhaltensdaten.

Anlage 2: Technische und organisatorische Maßnahmen

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

a. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

- Schließsystem mit Codeschloss
- Sicherheitsschlösser
- Schlüsselverwaltung (Schlüsselausgabe etc.)
- Protokollierung der Besucher
- Sorgfältige Auswahl des Sicherheitspersonals
- Sorgfältige Auswahl des Reinigungspersonals
- Manuelles Schließsystem

b. Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Vergabe von Benutzerrechten
- Passwortvergabe
- Authentifizierung mit Benutzername / Passwort
- Einsatz von Antivirensoftware
- Einsatz einer Software-Firewall

c. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Rechteverwaltung durch den Systemadministrator
- Anzahl der Administratoren auf das absolut Notwendige reduziert
- Protokollierung der Zugriffe auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Einsatz von Aktenvernichtern oder Dienstleistern
- Protokollierung der Vernichtung

d. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Logisch strikt getrennte Speicherung der Daten in verschiedenen Kundensystemen
- Verschlüsselung von Datensätzen, die zum gleichen Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Trennung von Produktiv- und Testsystem

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

a. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden sollen:

- Eine Übermittlung personenbezogener Daten, die im Auftrag von Kunden erfolgt, darf nur in dem mit dem Kunden vereinbarten Umfang oder in dem zur Erbringung der vertraglichen Leistungen für den Kunden erforderlichen Umfang erfolgen.
- Alle an einem Kundenprojekt arbeitenden ATLAS.ti-Mitarbeiter werden über die zulässige Verwendung der Daten und die Modalitäten der Datenübermittlung unterrichtet.
- Soweit möglich werden Daten verschlüsselt an Empfänger übermittelt.
- ATLAS.ti-Mitarbeitern ist die Nutzung privater Datenspeichermedien im Zusammenhang mit Kundenprojekten untersagt.

b. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten über individuelle Benutzernamen (nicht Benutzergruppen)

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

a. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Unterbrechungsfreie Stromversorgung (USV)
 - Einrichtungen zur Überwachung von Temperatur und Luftfeuchtigkeit in Serverräumen
 - Feuer- und Rauchmeldeanlagen
 - Erstellung eines Backup- und Recovery-Konzepts
 - Erstellung eines Notfallplans
 - Serverräume nicht unter Sanitäreinrichtungen
 - Klimatisierung der Serverräume
 - Schutzsteckdosenleisten in Serverräumen
 - Feuerlöscheinrichtungen in Serverräumen
- b. Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei Verlust oder Störung unverzüglich wiederhergestellt werden können:

- Regelmäßige Backups
- Test der Datenwiederherstellung

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

a. Datenschutz- und Informationssicherheitsmanagement

Bei ATLAS.ti ist ein Datenschutzmanagementsystem implementiert. Es existiert eine Richtlinie zu Datenschutz und Datensicherheit sowie Richtlinien, die sicherstellen, dass die Ziele der Richtlinie umgesetzt werden. Alle Richtlinien werden regelmäßig hinsichtlich ihrer Wirksamkeit bewertet und angepasst.

Es wurde ein Team für Datenschutz und Informationssicherheit eingerichtet, das Maßnahmen zum Datenschutz und zur Datensicherheit plant, umsetzt, bewertet und anpasst.

Es wurde ein Datenschutzbeauftragter benannt.

Alle Mitarbeiter werden regelmäßig in Datenschutz und Informationssicherheit geschult.

b. Incident-Response-Management

Alle Mitarbeiter werden unterrichtet und geschult, um sicherzustellen, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich an das Team für Datenschutz und Informationssicherheit gemeldet werden. Das Team für Datenschutz und Informationssicherheit untersucht den Vorfall unverzüglich. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, ist sichergestellt, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

c. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Bei ATLAS.ti stellen wir sicher, dass der Grundsatz der Erforderlichkeit und der Datenminimierung bereits ab der Softwareentwicklung berücksichtigt wird.

d. Auftragskontrolle

Maßnahmen, die gewährleisten, dass im Auftrag verarbeitete personenbezogene Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Sorgfältige Auswahl der Subunternehmer (insbesondere im Hinblick auf die Informationssicherheit)
- Regelmäßige Kontrolle der Subunternehmer