Allgemeine Geschäftsbedingungen

Allgemeine Geschäftsbedingungen (AGB) für „Medistella“

1. Einleitung

Diese Geschäftsbedingungen regeln die Nutzung des Tools „Medistella“, das von der Medistella GmbH (nachfolgend „Anbieter“) bereitgestellt wird. Das Tool dient der Aufzeichnung von Arzt-Patientengesprächen sowie der Erstellung von Zusammenfassungen mittels künstlicher Intelligenz. Mit Inanspruchnahme des Services erklärt der Kunde, dass er diese Bedingungen in ihrer Gesamtheit anerkennt.

2. Anwendungsbereich

2.1 Diese AGB ergänzen alle zwischen dem Kunden und dem Anbieter bestehenden vertraglichen Vereinbarungen.

2.2 Abweichende oder ergänzende Bedingungen des Kunden finden nur dann Anwendung, wenn der Anbieter diesen ausdrücklich schriftlich zustimmt.

3. Begriffsbestimmungen

3.1 **Künstliche Intelligenz (KI):** Hierunter fallen Computersysteme, Algorithmen und Software, die Aufgaben übernehmen, die normalerweise menschliche Intelligenz erfordern.

3.2 **KI-Zusammenfassung:** Die automatisch erstellte, KI-gestützte Zusammenfassung eines aufgezeichneten Arzt-Patientengesprächs.

3.3 **Vertrauliche Informationen:** Alle Daten und Informationen, die als vertraulich gelten oder aufgrund der Umstände als schutzwürdig anzusehen sind – beispielsweise personenbezogene Daten und insbesondere Gesundheitsdaten sowie technische, wirtschaftliche oder finanzielle Details.

4. Leistungsbeschreibung und Nutzung

4.1 Der Zugang zum Service erfolgt über ein Webinterface sowie über eine Softwareanwendung.

4.2 Der Anbieter stellt den Service mit einer durchschnittlichen Verfügbarkeitsrate von 98 % im Jahresmittel bereit. Diese Quote gilt unter Ausschluss geplanter Wartungszeiten und Ereignissen höherer Gewalt.

4.3 Der Kunde ist verpflichtet, einen stabilen Internetzugang sowie eine kompatible IT-Infrastruktur bereitzustellen. Er ist zudem für die Sicherheit und Stabilität seines eigenen Systems sowie für die Nutzung eines aktuellen Browsers verantwortlich.

4.4 Bei Anzeichen von Missbrauch, unautorisiertem Zugriff oder technischen Störungen behält sich der Anbieter das Recht vor, den Zugang vorübergehend einzuschränken.

5. Vertragsdauer und Kündigung

5.1 Der Vertrag tritt mit der Aktivierung des Services durch den Anbieter in Kraft.

5.2 Sofern keine abweichende Regelung getroffen wurde, verlängert sich der Vertrag automatisch um jeweils einen weiteren Monat.

5.3 Beide Parteien können den Vertrag unter Einhaltung einer Kündigungsfrist von einem Monat zum Ende der Laufzeit schriftlich (zum Beispiel per E-Mail) kündigen.

5.4 Gesetzliche Sonderkündigungsrechte bleiben hiervon unberührt.

6. Vergütungsmodalitäten

6.1 Der Kunde verpflichtet sich, die vereinbarte monatliche Vergütung zu zahlen. Alle Preisangaben verstehen sich exklusive der gesetzlichen Mehrwertsteuer.

6.2 Bei Zahlungsverzug behält sich der Anbieter vor, den Service bis zur vollständigen Begleichung der ausstehenden Beträge auszusetzen.

7. Pflichten des Kunden

7.1 Der Kunde hat den Service vor der regulären Nutzung eingehend zu testen und sicherzustellen, dass seine technische Umgebung kompatibel ist.

7.2 Vor der Erstnutzung von Medistella mit einem Patienten benötigen Sie dessen schriftliche Einwilligung vor der ersten Anwendung. Diese Einwilligung gilt, bis sie widerrufen wird.

7.3 Vor jeder Aufzeichnung eines Arzt-Patientengesprächs soll der Kunde den Patienten gemäß den gesetzlichen Anforderungen über die Nutzung des Tools hinweisen..

7.4 Die vom Tool erstellte Zusammenfassung ist durch den Kunden vor der Übernahme in die Patientendokumentation auf Richtigkeit zu prüfen.

7.5 Es obliegt dem Kunden, seine Mitarbeiter entsprechend über die ordnungsgemäße Nutzung des Tools und die Einhaltung der Datenschutzvorgaben zu unterrichten. Bei allen Anwendern ist die notwendige Kompetenz und Kenntnis bei der Nutzung der Anwendung durch den Kunden herzustellen.

8. Geistiges Eigentum

8.1 Alle Urheber-, Marken- und sonstigen Schutzrechte an dem Tool und der zugehörigen Software verbleiben beim Anbieter.

8.2 Der Kunde ist ohne ausdrückliche schriftliche Genehmigung nicht berechtigt, Inhalte oder Softwarebestandteile zu vervielfältigen, zu modifizieren, zu dekompilieren oder Dritten zugänglich zu machen.

9. Datenschutz

9.1 Die Nutzung des Services umfasst die Verarbeitung personenbezogener, insbesondere sensibler Gesundheitsdaten. Dementsprechend müssen durch den Kunden alle Regelungen gemäß DS-GVO sowie des KI-Acts eingehalten werden.

9.2 Der Kunde handelt als eigenständiger Verantwortlicher für die Einhaltung der Datenschutzbestimmungen und darf personenbezogene Daten nur gemäß geltendem Recht verarbeiten. Der Anbieter übernimmt im Rahmen eines Auftragsverarbeitungsverhältnisses die Verarbeitung der Daten gemäß Art. 28 DSGVO.

9.3 Weiterführende Regelungen zur Datenverarbeitung sind im Anhang A – Auftragsverarbeitungsvertrag detailliert aufgeführt und bilden einen integralen Bestandteil dieser AGB.

10. Einsatz von künstlicher Intelligenz

Medistella nutzt Künstliche Intelligenz (KI), um Arzt-Patienten-Gespräche zu dokumentieren. Die erstellten Inhalte werden maschinell generiert werden und bedürfen einer ärztlichen Überprüfung.

11. Vertraulichkeit

11.1 Beide Parteien verpflichten sich, alle im Rahmen der Zusammenarbeit erhaltenen vertraulichen Informationen streng vertraulich zu behandeln.

11.2 Eine Offenlegung an Dritte erfolgt ausschließlich, wenn dies zur Vertragserfüllung erforderlich ist oder gesetzliche Bestimmungen dies verlangen.

11.3 Informationen, die bereits öffentlich bekannt sind, unterliegen nicht dieser Vertraulichkeitsverpflichtung.

12. Haftung

12.1 Der Anbieter haftet uneingeschränkt für Schäden aus vorsätzlichem oder grob fahrlässigem Verhalten sowie bei Verletzungen von Leben, Körper oder Gesundheit.

12.2 Für andere Schäden haftet der Anbieter nur bei Verletzung wesentlicher Vertragspflichten (sogenannter Kardinalpflichten) und beschränkt auf den vorhersehbaren Schaden.

12.3 Die Haftungsbeschränkung gilt ebenso für die Erfüllungsgehilfen des Anbieters.

12.4 Eine weitergehende Haftung ist, soweit gesetzlich zulässig, ausgeschlossen.

13. Gewährleistung

13.1 Der Service wird ohne ausdrückliche Garantien bereitgestellt – er wird „wie gesehen“ und „wie verfügbar“ angeboten.

13.2 Der Anbieter übernimmt keine Gewährleistung für eine durchgehende Fehlerfreiheit oder ununterbrochene Verfügbarkeit, soweit nicht zwingendes Recht etwas anderes vorschreibt.

13.3 Der Kunde ist verantwortlich für die Konfiguration und den Betrieb seiner IT-Systeme sowie für den Einsatz adäquater Sicherheitsmaßnahmen (z. B. Virenschutz).

14. Weiterentwicklung und Vertragsänderungen

14.1 Der Anbieter ist berechtigt, den Service fortlaufend zu optimieren und an veränderte technische, rechtliche oder betriebliche Anforderungen anzupassen.

14.2 Wesentliche Änderungen, die den Vertragszweck erheblich beeinträchtigen, werden dem Kunden mindestens 15 Tage vor Inkrafttreten schriftlich (z. B. per E-Mail) angekündigt.

14.3 Führen wesentliche Änderungen zu einer erheblichen Einschränkung des Services, steht dem Kunden ein fristloses Kündigungsrecht zu.

15. Sonstige Bestimmungen

15.1 Der Anbieter kann zur Erfüllung seiner Leistungen Dritte oder Unterauftragnehmer einschalten.

15.2 Änderungen oder Ergänzungen dieser AGB bedürfen der Schriftform.

15.3 Sollte eine Bestimmung dieser AGB unwirksam sein, so bleibt die Wirksamkeit der übrigen Regelungen unberührt.

15.4 Alle Mitteilungen im Rahmen dieses Vertrags erfolgen in Textform.

16. Anwendbares Recht und Gerichtsstand

16.1 Es gilt ausschließlich das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

16.2 Für alle Streitigkeiten aus diesem Vertrag ist, soweit gesetzlich zulässig, der Gerichtsstand Regensburg vereinbart.

Anhang A – Auftragsdatenverarbeitung

Die im Anhang A festgelegten Regelungen zur Auftragsdatenverarbeitung konkretisieren den Umgang mit personenbezogenen Daten. Diese Bestimmungen gelten als integraler Bestandteil der vorliegenden AGB.

Anhang A: Auftragsverarbeitung

Auftragsverarbeitungsvertrag zwischen

Nutzer/ Nutzerin (Abonnent/ Abonenntin)

(Verantwortlicher im Sinne der DS-GVO, nachfolgend „Auftraggeber“ genannt)

und

Medistella GmbH, Am Biopark 13 93053 Regensburg

(Auftragsverarbeiter im Sinne der DS-GVO, nachfolgend „Auftragnehmer“ genannt)

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung inkl. den Allgemeinen Geschäftsbedingungen (Hauptvertrag) und deren Durchführung einen Auftragsverarbeitungsvertrag (nachstehend "Vertrag" genannt) im Sinne des Art. 28 DSGVO eingegangen. Um in Ergänzung zu der Leistungsvereinbarung die hieraus resultierenden datenschutzrechtlichen Rechte und Pflichten der Vertragsparteien hinsichtlich der Verarbeitung von personenbezogenen Daten durch den Auftragnehmer im Auftrag des Auftraggebers gemäß den gesetzlichen Verpflichtungen zu konkretisieren, schließen die Vertragsparteien den nachfolgenden Vertrag.

Anwendungsbereich

Sämtliche in diesem Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen bzw. kommen können.

§ 1 Definitionen

Es gelten die Begriffsbestimmungen entsprechend Art. 4 DS-GVO, § 2 UWG und § 2 TMG. Sollten in den Artikeln bzw. Paragraphen sich widersprechende Darstellungen zu finden sein, gelten die Definitionen in der Rangfolge DS-GVO, UWG und TMG. Weiterhin gelten folgende Begriffsbestimmungen:

(1) Anonymisierung

Prozess, bei dem personenbezogene Daten entweder vom für die Verarbeitung der Daten Verantwortlichen allein oder in Zusammenarbeit mit einer anderen Partei unumkehrbar so verändert werden, dass sich die betroffene Person danach weder direkt noch indirekt identifizieren lässt. (Quelle: DIN EN ISO 25237)

(2) Drittland

Ein Land, welches sich außerhalb der EU/EWR befindet.

(3) Hauptvertrag

Vertrag (i.d.R. ein Dienst- oder Werkvertrag), in welchem alle Einzelheiten der Verarbeitung beschrieben sind.

(4) Unterauftragnehmer

Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber dem Auftraggeber benötigt.

(5) Verarbeitung im Auftrag

Verarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch einen Auftragnehmer im Auftrag des Auftraggebers.

(6) Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch einen Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

(7) Verantwortlicher

Verantwortlicher im Sinne des Art. 4 Ziff. 7 DS-GVO ist der Auftraggeber. Er ist für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

§ 2 Gegenstand des Auftrags

Aus der Leistungsvereinbarung ergibt sich der Gegenstand der Auftragsverarbeitung. Eine Spezifizierung, sowie Art und Zweck der Auftragsverarbeitung, lauten wir folgt:

Art der Daten:

- Bestandsdaten (z.B. Namen, Adressen, Beruf, Alter, Geschlecht und weitere personenbezogene Daten aus dem Gespräch zwischen Arzt und Patient)

- Vertragsdaten (z.B. Vertragpartner, User, Daten über vertragliche Inhalte)
- Allgemeiner Schrift- und Zahlungsverkehr (z.B. Bankverbindungen, Daten über den Zahlungsverkehr, Daten aus postalischer, elektronischer bzw. digitaler und telefonischer Kommunikation)

Verarbeitung besonderer Kategorien von Daten (Art. 9 Abs. 1 DSGVO):

- Gesundheitsdaten/ Medizinische Patientendaten (Befunde, Diagnosen, Therapie)

Kategorien der Betroffenen:

- Patienten/innen des Auftraggebers
- Mitarbeiter/innen des Auftraggebers

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien

Art und Zweck der Verarbeitung:

Der Auftragnehmer erbringt für den Auftraggeber bezogen auf die genannten Daten folgende Datenverarbeitung:

Erhebung, Verarbeitung und Speicherung von Daten zum Zweck der medizinischen Dokumentation von Behandlungsgesprächen zwischen dem Auftraggeber und dessen Patienten.

Im Einzelnen sind folgende Verarbeitungsschritt zu nennen:

- Bereitstellung einer Softwareanwendung zur medizinischen Dokumentation
- Aufzeichnung, Transkription und Speicherung von Patientengesprächen
- Aufzeichnung, Transkription und Speicherung von Patientendaten zur Erstellung von medizinischen Korrespondenzen (z.B. Arztbriefe)
- Zusammenfassung und Strukturierung der Inhalte der Transkription zum Zweck der medizinischen Dokumentation, Speicherung der Ausgabedaten
- Löschung der erhobenen und verarbeiteten Daten nach Ablauf einer angemessenen Zeit (zur Übertragung der Daten in das Praxisverwaltungssystem)

§ 3 Verantwortlichkeit

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer allein verantwortlich ("Verantwortlicher" im Sinne des Art. 4 Nr. 7 DSGVO).

Auftraggeber sowie Auftragnehmer müssen gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dazu müssen alle

Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden. Dabei ist jede Partei für die Verpflichtung des eigenen Personals zuständig. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht.

Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich

§ 4 Dauer des Auftrags

Die Laufzeit dieses AV-Vertrages richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus den Bestimmungen dieses AV-Vertrages nicht etwas anderes ergibt.

Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen AV-Vertrages z. B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.

Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

§ 5 Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

Die Weisungen des Auftraggebers werden vom Auftragnehmer dokumentiert und dem Auftraggeber unmittelbar nach erfolgter Dokumentation zur Verfügung gestellt.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis des Auftraggebers gedeckt und entsprechend zu dokumentieren. Bei einer vom Auftragnehmer als wesentlich angesehenen Änderung des Auftrags steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragnehmers auf der Änderung, so ist diese Änderung als wichtiger Grund anzusehen und erlaubt eine fristlose Kündigung des von der Weisung betroffenen AV-Vertrages sowie der von der AV-Vereinbarung betroffenen Bestandteile des entsprechenden Hauptvertrages.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer notiert sich Datum, Uhrzeit und Person, welche die mündliche Weisung erteilte, sowie den Grund, warum keine schriftliche Beauftragung erfolgen konnte.

§ 6 Leistungsort

Der Auftragnehmer wird die vertraglichen Leistungen in Deutschland erbringen, etwaige Unterauftragnehmer dürfen diese Leistungen nur an den mit dem Auftraggeber in Anhang 1 vereinbarten Leistungsstandorten in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) ausführen.

Der Auftraggeber stimmt einer Verlagerung eines Ortes der Leistungserbringung innerhalb des Leistungslandes, für das eine Zustimmung besteht, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt bei dem Auftragnehmer.

Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der EU / EWR sind und über ein diesem Vertrag genügendes und verifiziertes Datenschutzniveau verfügen, wird der Auftraggeber schriftlich informiert.

Sofern der Auftragnehmer vom Auftraggeber nicht innerhalb einer Frist von vier Wochen nach Zugang der Mitteilung gemäß Abs. 3 über die Verlagerung über Gründe informiert wird, die eine Verlagerung nicht zulassen, gilt die Zustimmung zu dieser Verlagerung seitens des Auftraggebers als erteilt.

Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU/EWR in einem sog. sicheren „Drittstaat“ erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, wird der Auftragnehmer zuvor die schriftliche Zustimmung durch den Auftraggeber einholen.

Sofern die Leistungsverlagerung in ein anderes Land nach den vorstehenden Regelungen möglich ist, gilt dies entsprechend für jeglichen Zugriff bzw. jegliche Sicht auf die Daten durch den Auftragnehmer, z. B. im Rahmen von internen Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung.

Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten in das Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird der Auftragnehmer für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

Der Auftraggeber stimmt der Verarbeitung von Daten durch den Auftragnehmer im Homeoffice zu. Im Gegenzug verpflichtet sich der Auftragnehmer, die im Homeoffice notwendigen Sicherheitsbestimmungen zu gewährleisten.

§ 7 Pflichten des Auftragnehmers

Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten.

Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen; diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. Aufsichtsbehörden gegenüber nachweisen. Dieser Nachweis beinhaltet insbesondere die Umsetzung der aus Art. 32 DS-GVO resultierenden Maßnahmen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative, nachweislich adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

Eine Darstellung dieser technischen und organisatorischen Maßnahmen erfolgt im Anlage 2 zu diesem Vertrag.

Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DS-GVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DS-GVO notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

Der Auftragnehmer unterstützt den Auftraggeber bei der Datenschutzfolgenabschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.

Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.

Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit sicur data GmbH, Frau Beate Bender, Seumestraße 12, 90478 Nürnberg benannt. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DS-GVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, benennt der Auftragnehmer dem Auftraggeber einen Ansprechpartner.

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde

bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Artt. 33, 34 DS-GVO.

Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer betroffenen Person verpflichtet, Auskünfte zur Verarbeitung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen, vorausgesetzt der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert.

Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichen im Sinne der DS-GVO liegen.

Sofern der Auftragnehmer durch das Recht der Union oder Mitgliedstaaten verpflichtet ist, die Daten auch auf andere Weise zu verarbeiten, so teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit. Die Mitteilung hat zu unterbleiben, wenn das einschlägige nationale Recht eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet.

Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Auftraggeber auf Anforderung nachzuweisen.

Vereinbarung zur Wahrung des Berufsgeheimnisses nach § 203 StGB

Im Rahmen dieses Auftrages werden auch Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von § 203 StGB) fallen.

Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.

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. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, 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 die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

Der Auftragnehmer ist berechtigt, Unterauftragnehmer zur Vertragserfüllung heranzuziehen. Im Ausland dürfen Unterauftragnehmer zur Vertragserfüllung nur dann herangezogen werden, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist.

Der Auftragnehmer wird etwaige Unterauftragnehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, zur Geheimhaltung verpflichten. Der Auftragnehmer wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzte Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren.

Des Weiteren werden Subunternehmer, über das bestehende Schweigerecht gemäß § 53a StPO sowie den Beschlagnahmeschutz gemäß § 97 StPO informiert; dies beinhaltet auch den Hinweis bzgl. des Rechts des Berufsgeheimnisträgers, über dieses Recht zu entscheiden und der damit verbundenen Pflicht des Auftragnehmers, unverzüglich den Auftraggeber bzgl. der Wahrnehmung dieser Rechte zu kontaktieren.

Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen.

Der Auftragnehmer wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u. U. dem Zeugnisverweigerungsrecht von sogenannten mitwirkenden Personen unterliegen (§ 53a Strafprozessordnung (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.

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

§ 8 Pflichten des Auftraggebers

Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.

Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

Der Auftraggeber ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat – neben der eigenen Verpflichtung des Auftragnehmers – ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.

Dem Auftraggeber obliegen die aus Artt. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.

Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

Der Auftraggeber stellt sicher, dass die aus Art. 32 DS-GVO resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung seinerseits eingehalten werden. Insbesondere gilt dies für Fernzugriffe des Auftragnehmers auf die Datenbestände des Auftraggebers.

§ 9 Kontrollrechte des Auftraggebers

Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichend Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte hierbei weitestgehend vermieden werden.

Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftraggeber im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des

Auftrags wird vom Auftragnehmer unterstützt. Insbesondere verpflichtet sich der Auftragnehmer, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

Vor-Ort-Kontrollen erfolgen innerhalb üblicher Geschäftszeiten, sind vom Auftraggeber mit einer angemessenen Frist (mindestens 14 Tage, außer in Notfällen) anzumelden und durch den Auftragnehmer zu unterstützen (z.B. durch Bereitstellung von Personal).

Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie den Schutz von personenbezogenen Daten Dritter (z.B. anderer Kunden oder Mitarbeiter des Auftragnehmers) Rücksicht nehmen. Zur Durchführung der Kontrolle sind nur fachkundige Personen zugelassen, die sich legitimieren können und im Hinblick auf die Betriebs- und Geschäftsgeheimnisse sowie Prozesse des Auftragnehmers und personenbezogene Daten Dritter zur Verschwiegenheit verpflichtet sind. Im Falle, dass der Dritte in einem direkten oder indirekten Wettbewerbsverhältnis zum Auftragnehmer steht, behält sich der Auftragnehmer ein Widerspruchsrecht und die Beauftragung eines neutralen Prüfers durch den Auftraggeber vor.

Neben der Einsichtnahmen und der Vor-Ort-Kontrollen, darf der Auftragnehmer den Auftraggeber auf eine gleichwertige Kontrolle durch unabhängige Dritte (z.B. neutrale Datenschutzauditoren), Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder geeignete Datenschutz- oder IT-Sicherheitszertifizierungen gem. Art. 42 DSGVO verweisen. Dies gilt insbesondere dann, wenn Betriebs- und Geschäftsgeheimnisse des Auftragnehmers oder personenbezogene Daten Dritter durch die Kontrollen gefährdet wären.

§ 10 Berichtigung, Beschränkung von Verarbeitung, Löschung und Rückgabe von Datenträgern

Während der laufenden Beauftragung berichtigt, löscht oder sperrt der Auftragnehmer die vertragsgegenständlichen Daten nur auf Anweisung des Auftraggebers.

Sofern eine Vernichtung während der laufenden Beauftragung vorzunehmen ist, übernimmt der Auftragnehmer die nachweislich datenschutzkonforme Vernichtung von Datenträgern und sonstiger Materialien nur aufgrund entsprechender Einzelbeauftragung durch den Auftraggeber. Dies gilt nicht, sofern im Hauptvertrag bereits eine entsprechende Regelung getroffen worden ist.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

Nach Abschluss der Erbringung der Verarbeitungsleistungen muss der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen oder diesem

zurückgeben, sofern nicht nach dem Unionsrecht oder dem für den Auftragnehmer geltendem nationalen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Sofern zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten entstehen, bedarf es einer vorherigen schriftlichen Vereinbarung über die Kostentragung.

Soweit ein Transport des Speichermediums vor Löschung unverzichtbar ist, wird der Auftragnehmer angemessene Maßnahmen zu dessen Schutz, insbesondere gegen Entwendung, unbefugtem Lesen, Kopieren oder Verändern, treffen. Die Maßnahmen und die anzuwendenden Löschverfahren werden bei Bedarf ergänzend zu den Leistungsbeschreibungen konkretisierend vereinbart.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Der Auftraggeber kann jederzeit, d. h. sowohl während der Laufzeit als auch nach Beendigung des Vertrages, die Berichtigung, Löschung, Verarbeitungseinschränkung (Sperrung) und Herausgabe von Daten durch den Auftragnehmer verlangen, solange der Auftragnehmer die Möglichkeit hat, diesem Verlangen zu entsprechen.

Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer aufgrund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Hauptvertrag anders vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Sollte dem Auftraggeber eine Rücknahme der Daten nicht möglich sein, wird er den Auftragnehmer rechtzeitig schriftlich informieren. Der Auftragnehmer ist dann berechtigt, personenbezogene Daten im Auftrag des Auftraggebers zu löschen.

§ 11 Unterauftragnehmer

Der Auftragnehmer nimmt keinen Unterauftragnehmer ohne vorherige explizite schriftliche oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch. Der Auftragnehmer stellt sicher, dass eine entsprechende Genehmigung des Auftragsgebers für alle im Zusammenhang mit der vertragsgegenständlichen Verarbeitung eingesetzten weiteren Unterauftragnehmer vorliegt.

Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Wird dem Einsatz dieser Unterauftragsverarbeiter binnen 14 Tage nicht schriftlich oder in elektronische Form

widersprochen, so gilt der Einsatz dieser Unterauftragsverarbeiter als vom Auftraggeber genehmigt. Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.

Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht. Hierbei muss jedoch jeder Unterauftragnehmer (verbundenes Unternehmen) vor Beauftragung dem Auftraggeber schriftlich angezeigt werden, sodass der Auftraggeber bei Vorliegen wichtiger Gründe die Beauftragung untersagen kann.

Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der Anlage 1 aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Unterauftragnehmer gilt die Einwilligung für das Tätigwerden als erteilt.

Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.

Ist der Auftragnehmer im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragnehmers in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Unterauftragnehmer im Wege eines Vertrags dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages sowie den in diesem AV-Vertrag beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt.

Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

Ein zustimmungspflichtiges Unterauftragnehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei Personal-, Post- und Versanddienstleistungen.

Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Die Nebenleistungen sind vorab detailliert zu benennen.

Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers.

§ 12 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

§ 13 Haftung

Es gelten die gesetzlichen Regelungen gem. Art. 82 DSGVO. Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wird gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

- er den aus der DS-GVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
- er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
- er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er

- seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder
- unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

§ 14 Schriftformklausel

Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Regelungen handelt. Das Schriftformerfordernis gilt auch für den Verzicht auf dieses Formerfordernis.

§ 15 Salvatorische Klausel

Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.

Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter § 16 Abs. 1 genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Patientendaten im Sinne dieses Vertrages am besten gewährleistet.

§ 16 Rechtswahl, Gerichtsstand

Es gilt das Recht der Bundesrepublik Deutschland. Zwingende datenschutzrechtliche Vorschriften, insbesondere der Datenschutz-Grundverordnung (DSGVO), bleiben unberührt.

Gerichtsstand ist der Sitz des Auftragnehmers.

Anlagen

Anlage 1: Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

Anlage 2: Nachweis der allgemeinen technischen und organisatorischen Maßnahmen.

Anlage 1 zum AV-Vertrag: Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung
Microsoft Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Transkription der Gesprächsdaten (Azure Speech Service) Analyse und Zusammenfassung (Azure OpenAI) Betrieb der Anwendung (Azure Static Web App, Azure App Service) Speicherung der Daten (Azure SQL Database)	Microsoft Rechenzentren in der **EU** (Region Germany West oder andere Regionen gemäß Azure Data Residency)
Auth0, LLC 100 First Street, Floor 6 San Francisco, CA 94105 San Francisco, CA 94107	Verwaltung der Identität der Nutzer, Registrierung und Authentifizierung und zur Abwehr von Cybersicherheitsbedrohungen. Übermittlung und Verwaltung von Login-Daten wie Name, E-Mail-Adresse, Adresse, Telefonnummer, Passwort sowie weitere Informationen, die der Nutzer in seinem Benutzerprofil konfiguriert.	Die Auth0-Leistungen (Verarbeitung und Speicherung der Kundendaten) erfolgen innerhalb der EU-Region.

Anlage 2 zum AV-Vertrag: Nachweis der allgemeinen technischen und organisatorischen Maßnahmen

Das Gliederungsschema gemäß der Anlage zu § 9 S. 1 BDSG a.F. wird vorerst weiterhin zur Verwendung vorgeschlagen, da es einerseits derzeit noch weit verbreitet ist und andererseits die DS-GVO mit ihren wesentlich abstrakteren Grundprinzipien/Gewährleistungszielen kein ähnlich operationales Schema anbietet.

1) Zutrittskontrolle

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

Der Zutritt zu den Räumlichkeiten, in denen die Anwendung Medistella weiterentwickelt wird, ist durch ein physisches Schließsystem geregelt.

Die Schlüsselvergabe erfolgt ausschließlich gemäß einer internen Zugangsrichtlinie, die die Berechtigungen und den Umgang mit Schlüsseln definiert.

Homeoffice-Tätigkeiten dürfen erfolgen, soweit gewährleistet ist, dass unbefugte Personen – einschließlich Familienmitglieder oder Mitbewohner – keinen Zugang zu dienstlichen Unterlagen haben.

2) Zugangskontrolle

Es existieren folgende Maßnahmen zur Zugangskontrolle:

Die Arbeiten an der Anwendung Medistella erfolgen ausschließlich auf dienstlich zugewiesenen Geräten, um eine sichere Systemumgebung zu gewährleisten.

Alle dienstlich genutzten Geräte sind mit starken Passwörtern und biometrischer Authentifizierung geschützt. Zusätzlich sorgt eine automatische Bildschirmsperre nach einer definierten Inaktivitätszeit für erhöhten Schutz.

3) Zugriffskontrolle

Es existieren folgende Maßnahmen zur Zugriffskontrolle:

Der Zugriff auf Systeme, die personenbezogene oder Gesundheitsdaten enthalten, erfolgt ausschließlich über ein rollenbasiertes Zugriffskontrollsystem (RBAC).

Die Vergabe und Verwaltung von Zugriffsrechten unterliegt einem definierten Berechtigungskonzept, das regelmäßig überprüft und dokumentiert wird.

4) Weitergabekontrolle

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

Alle gesundheits- und personenbezogenen Daten werden gemäß dem aktuellen Stand der Technik verschlüsselt gespeichert und übertragen, um die Vertraulichkeit zu gewährleisten.

Der Zugriff auf diese Daten setzt eine eindeutige Benutzerkennung sowie eine sichere Authentifizierung mittels Passwortschutz voraus.

5) Eingabekontrolle

Es existieren folgende Maßnahmen zur Eingabekontrolle:

Sämtliche sicherheitsrelevanten Aktivitäten, darunter erfolgreiche und fehlgeschlagene Anmeldeversuche, Passwortänderungen, API-Zugriffe und administrative Änderungen, werden protokolliert und regelmäßig überprüft.

Die Protokolle werden sicher gespeichert und unterliegen einer definierten Aufbewahrungsrichtlinie, um die Integrität und Nachvollziehbarkeit der Daten sicherzustellen.

6) Auftragskontrolle

Es existieren folgende Maßnahmen zur Auftragskontrolle:

Der Auftraggeber behält sich das Recht vor, die Einhaltung der vertraglichen Datenschutzanforderungen regelmäßig durch Audits oder Stichprobenprüfungen zu kontrollieren. Der Auftragnehmer stellt hierfür die erforderlichen Unterlagen und Zugänge zur Verfügung.

Der Auftragnehmer verpflichtet sich, sämtliche Verarbeitungsvorgänge und technischen Sicherheitsmaßnahmen nachvollziehbar zu dokumentieren und dem Auftraggeber auf Anfrage vorzulegen.

Der Auftragnehmer darf personenbezogene Daten ausschließlich gemäß den schriftlichen Weisungen des Auftraggebers verarbeiten. Der Auftraggeber behält sich das Recht vor, stichprobenartig zu überprüfen, ob die Verarbeitung dieser Weisungen entspricht

7) Verfügbarkeitskontrolle

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

Hochverfügbarkeit durch Azure SQL-Datenbank-Replikation durch Geo-redundante Replikation

Tägliche Backups mit einer definierten Aufbewahrungsfrist sorgen für die Möglichkeit zur Wiederherstellung von Daten

8) Trennungskontrolle

Es existieren folgende Maßnahmen zur Trennungskontrolle:

Die Anwendung Medistella ist mandantenfähig konzipiert, sodass Daten logisch voneinander getrennt und nur durch berechtigte Benutzer einsehbar sind.

Zweckgebundene Speicherung und Verarbeitung von Daten: Die Verarbeitung personenbezogener Daten erfolgt ausschließlich für den jeweiligen vorgesehenen Zweck.

Funktionstrennung zwischen Entwicklungs-, Test- und Produktivsystemen: Es existieren getrennte Entwicklungs-, Test- und Produktivumgebungen, um eine Vermischung von Echtdaten mit Testdaten zu verhindern.