MeinGPT

Auftragsverarbeitungsvertrag

Vereinbarung gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

V2.0 Stand: 2026-09-17

VERTRAGSPARTEIEN

VERANTWORTLICHER

VOLLSTÄNDIGER NAME / FIRMA

ANSCHRIFT

VERTRETUNG (NAME / FUNKTION)

AUFTRAGSVERARBEITER

SelectCode GmbH
Oskar-von-Miller-Straße 11
82008 Unterhaching · Deutschland
Amtsgericht München · HRB 234337

Der Verantwortliche und die SelectCode GmbH als Auftragsverarbeiter werden gemeinsam als „Parteien“ bezeichnet.

Präambel

Der Verantwortliche hat den Auftragsverarbeiter im bereits geschlossenen Vertrag (nachfolgend „**Hauptvertrag**“) zu den dort genannten Leistungen beauftragt. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag (nachfolgend die „**Vereinbarung**“), dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

(1) **Verantwortlicher** ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) **Auftragsverarbeiter** ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) **Personenbezogene Daten** sind gem. Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „**Betroffener**“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu 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.

(4) **Besonders schutzbedürftige personenbezogene Daten** sind personenbezogene Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DSGVO, biometrische Daten gem. Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) **Verarbeitung** ist gem. Art. 4 Abs. 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, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) **Aufsichtsbehörde** ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

§ 2 Vertragsgegenstand

(1) Der Auftragsverarbeiter erbringt für den Verantwortlichen die im Hauptvertrag genannten Leistungen. Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten, die der Auftragsverarbeiter für den Verantwortlichen ausschließlich im Auftrag und nach Weisung des Verantwortlichen verarbeitet. Umfang und Zweck der Datenverarbeitung durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag und etwaigen zugehörigen Leistungsbeschreibungen. Dem Verantwortlichen obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragsverarbeiter und seine Beschäftigten oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Verantwortlichen stammen oder für den Verantwortlichen erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Weisungsrecht

(1) Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen im Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Alle erteilten Weisungen sind vom Verantwortlichen zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Arten der verarbeiteten Daten, Kreis der Betroffenen, Drittland

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragsverarbeiter Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in **Anlage 2** dargestellt.

(3) Die Verarbeitung personenbezogener Daten findet grundsätzlich innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums statt. Soweit **Anlage 4** für einen Unterauftragsverarbeiter ausdrücklich eine Verarbeitung in einem Drittland ausweist, ist diese Verarbeitung für den dort beschriebenen Zweck genehmigt; der Auftragsverarbeiter stellt hierfür die Einhaltung der Art. 44 ff. DSGVO sicher, insbesondere durch einen Angemessenheitsbeschluss nach Art. 45 DSGVO oder geeignete Garantien nach Art. 46 DSGVO. Eine darüber hinausgehende Übermittlung in ein Drittland erfolgt nur auf dokumentierte Weisung des Verantwortlichen – insbesondere, wenn der Verantwortliche innerhalb der Plattform ein Modell oder einen Integrierten Dienst mit einem Serverstandort außerhalb der EU/des EWR aktiv auswählt – und unter Einhaltung der Art. 44 ff. DSGVO.

§ 5 Schutzmaßnahmen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Verantwortlichen erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er hat die in **Anlage 3** genannten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gem. Art. 32 DSGVO getroffen, die der Verantwortliche als angemessen anerkennt. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragsverarbeiter wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (nachfolgend „**Mitarbeiter**“), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

(4) Der Auftragsverarbeiter hat einen Datenschutzbeauftragten benannt. Der Datenschutzbeauftragte des Auftragsverarbeiters ist heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu, www.heydata.eu.

(5) **Der Auftragsverarbeiter bestätigt ausdrücklich, dass keiner seiner Unterauftragsverarbeiter die Daten des Auftraggebers für das Training seines eigenen KI-Modells verwendet. Der Auftragsverarbeiter verwendet die Daten auch nicht für andere Zwecke als die Erbringung der Dienstleistungen.**

§ 6 Informationspflichten des Auftragsverarbeiters

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragsverarbeiters, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragsverarbeiter den Verantwortlichen unverzüglich informieren. Dasselbe gilt für Prüfungen des Auftragsverarbeiters durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
b) eine Beschreibung der von dem Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen;
c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.

(2) Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Verantwortlichen und ersucht um weitere Weisungen.

(3) Der Auftragsverarbeiter ist darüber hinaus verpflichtet, dem Verantwortlichen jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 5 Abs. 2 hat der Auftragsverarbeiter den Verantwortlichen zu unterrichten.

§ 7 Behördliche Zugriffsverlangen

(1) Erhält der Auftragsverarbeiter von einer Behörde, einem Gericht oder einer Strafverfolgungsstelle ein Verlangen auf Herausgabe, Offenlegung, Sicherung oder Einsichtnahme in personenbezogene Daten, die er für den Verantwortlichen verarbeitet, so unterrichtet er den Verantwortlichen hierüber unverzüglich und so rechtzeitig, dass dieser eigene Rechtsschutzmöglichkeiten wahrnehmen kann.

Er gibt die Daten nicht heraus, bevor er den Verantwortlichen unterrichtet hat, es sei denn, er ist hierzu gesetzlich verpflichtet.

(2) Ist dem Auftragsverarbeiter die Unterrichtung rechtlich untersagt, so prüft er, ob das Verbot angreifbar oder befristet ist, und unterrichtet den Verantwortlichen, sobald es entfällt. Er dokumentiert das Verbot und dessen Grundlage.

(3) Der Auftragsverarbeiter kommt einem Verlangen nur nach, soweit er hierzu nach dem Recht der Union oder dem Recht eines Mitgliedstaats verpflichtet ist. Einem Verlangen einer Behörde eines Drittstaats, das keine Grundlage in einem Rechtshilfeabkommen oder einer sonstigen unionsrechtlich anerkannten Grundlage hat, kommt er nicht nach.

(4) Der Auftragsverarbeiter prüft jedes Verlangen auf Rechtsgrundlage, Umfang und Verhältnismäßigkeit. Gegen ein Verlangen, das seine Grundlage überschreitet, unverhältnismäßig ist oder gegen Unionsrecht verstößt, legt er Rechtsmittel ein, soweit ihm dies zumutbar ist.

(5) Gibt der Auftragsverarbeiter Daten heraus, beschränkt er die Herausgabe auf das von der Anordnung Gedeckte. Er dokumentiert Verlangen, Prüfung, Entscheidung und Umfang der Herausgabe und stellt dem Verantwortlichen diese Dokumentation auf Anforderung zur Verfügung, soweit gesetzliche Offenlegungsverbote nicht entgegenstehen; entgegenstehende Bestandteile werden unkenntlich gemacht, im Übrigen wird die Dokumentation herausgegeben.

(6) Der Auftragsverarbeiter verpflichtet die von ihm eingesetzten Dienstleister auf entsprechende Pflichten, soweit diese Daten des Verantwortlichen verarbeiten.

§ 8 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche kann sich vor der Aufnahme der Datenverarbeitung und sodann jährlich von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters überzeugen. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören.

(2) **Nachweis im Regelfall.** Der Auftragsverarbeiter betreibt ein nach ISO/IEC 27001:2022 zertifiziertes Informationssicherheits-Managementsystem (Anlage 3). Der Nachweis der Einhaltung der Pflichten aus dieser Vereinbarung und aus Art. 28 DSGVO erfolgt deshalb regelmäßig durch Vorlage des jeweils aktuellen Zertifikats nebst Erklärung zur Anwendbarkeit, ergänzt um Auskünfte, Dokumentation und die Beantwortung eines Prüfungsfragebogens in angemessenem Umfang.

(3) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters erforderlich sind.

(4) Der Verantwortliche dokumentiert das Kontrollergebnis und teilt es dem Auftragsverarbeiter mit. Bei Fehlern oder Unregelmäßigkeiten, die der Verantwortliche insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragsverarbeiter unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Verantwortliche dem Auftragsverarbeiter die notwendigen Verfahrensänderungen unverzüglich mit.

(5) **Vor-Ort-Prüfungen sind nachrangig.** Eine Prüfung in den Räumen des Auftragsverarbeiters kann der Verantwortliche verlangen, soweit (i) er einen konkreten, begründeten Verdacht auf einen Verstoß gegen diese Vereinbarung oder gegen datenschutzrechtliche Bestimmungen darlegt, (ii) die nach dem vorstehenden Absatz bereitgestellten Nachweise im Einzelfall eine angemessene Überprüfung nicht ermöglichen, oder (iii) eine Aufsichtsbehörde dies gegenüber dem Verantwortlichen verlangt oder eine gesetzliche Pflicht dies gebietet. Vor-Ort-Prüfungen sollen im Regelfall nicht häufiger als einmal jährlich stattfinden. Dies gilt nicht, wenn ein erneuter konkreter und begründeter Anlass besteht, die bereitgestellten Nachweise weiterhin unzureichend sind oder eine Aufsichtsbehörde beziehungsweise eine gesetzliche Pflicht eine weitere Prüfung verlangt. Vor-Ort-Prüfungen sind mit angemessenem Vorlauf anzukündigen und auf die üblichen Geschäftszeiten beschränkt. Der Verantwortliche trägt seine eigenen Kosten sowie die angemessenen und

erforderlichen zusätzlichen Aufwendungen des Auftragsverarbeiters; dieser legt die Kostenbasis auf Verlangen nachvollziehbar dar. Die Kostenregelung darf die Ausübung des Kontrollrechts nicht faktisch unmöglich machen oder wesentlich erschweren. Ergibt die Prüfung einen wesentlichen Verstoß des Auftragsverarbeiters, trägt dieser die angemessenen Kosten der Prüfung.

(6) **Bündelung von Prüfungen.** Der Auftragsverarbeiter kann zeitlich oder sachlich gleichartige Vor-Ort-Prüfungen mehrerer Verantwortlicher in einer gemeinsamen Prüfung bündeln, soweit der Prüfungsgegenstand jedes Verantwortlichen dadurch angemessen abgedeckt wird. Er stellt durch strikte Vertraulichkeit, Mandantentrennung und geeignete organisatorische und technische Maßnahmen sicher, dass kein Verantwortlicher oder von ihm beauftragter Prüfer Zugang zu personenbezogenen Daten, vertraulichen Informationen oder Betriebs- und Geschäftsgeheimnissen eines anderen Kunden erhält. Jeder Verantwortliche erhält die für ihn relevanten Prüfungsergebnisse gesondert. Lässt sich ein kundenspezifischer Prüfungsgegenstand im Rahmen der gebündelten Prüfung nicht angemessen untersuchen, bleibt das individuelle Kontrollrecht des betroffenen Verantwortlichen unberührt.

(7) Der Auftragsverarbeiter ist berechtigt, die Offenlegung von Informationen insoweit zu beschränken, als dies erforderlich ist, um die Vertraulichkeit der Daten anderer Kunden, Sicherheitsanforderungen sowie berechtigte Betriebs- und Geschäftsgeheimnisse zu wahren.

(8) Beauftragt der Verantwortliche einen Dritten mit der Durchführung einer Prüfung, darf dieser kein Wettbewerber des Auftragsverarbeiters sein; er ist vor Durchführung schriftlich zur Vertraulichkeit zu verpflichten.

§ 9 Einsatz von Dienstleistern

(1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in **Anlage 4** genannten Dienstleister (nachfolgend „**Unterauftragsverarbeiter**“) durchgeführt. Der Verantwortliche erteilt dem Auftragsverarbeiter seine allgemeine Genehmigung im Sinne von Art. 28 Abs. 2 S. 1 DSGVO, im Rahmen seiner vertraglichen Verpflichtungen weitere Unterauftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen.

(2) Der Auftragsverarbeiter wird den Verantwortlichen vor jeder beabsichtigten Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters informieren. Der Verantwortliche kann gegen eine beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters aus wichtigem datenschutzrechtlichen Grund Einspruch erheben.

(3) Der Einspruch gegen die beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters ist innerhalb von 2 Wochen nach Erhalt der Information über die Änderung zu erheben. Wird kein Einspruch erhoben, gilt die Hinzuziehung oder Ersetzung als genehmigt. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösungsfindung zwischen dem Verantwortlichen und dem Auftragsverarbeiter nicht möglich, steht jeder Partei ein Sonderkündigungsrecht hinsichtlich des Hauptvertrags und dieser Vereinbarung zum auf den Einspruch folgenden Monatsende zu.

(4) Der Auftragsverarbeiter hat bei der Einschaltung von Unterauftragsverarbeitern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten.

(5) Ein Unterauftragsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden.

§ 10 Anfragen und Rechte Betroffener

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 bis 36 DSGVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragsverarbeiter geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen an den Verantwortlichen und wartet dessen Weisungen ab.

§ 11 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragsverarbeiter allein der Verantwortliche gegenüber dem Betroffenen verantwortlich.

(2) Im Übrigen richtet sich die Haftung des Auftragsverarbeiters aus oder im Zusammenhang mit dieser Vereinbarung – einschließlich der im Hauptvertrag vereinbarten Haftungsausschlüsse und -begrenzungen – nach den Regelungen des Hauptvertrags. Die zwingende gesetzliche Haftung, insbesondere die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO sowie die Haftung wegen der Verletzung von Leben, Körper oder Gesundheit, aus Vorsatz oder grober Fahrlässigkeit oder aus der Übernahme einer Garantie, bleibt hiervon unberührt.

§ 12 Beendigung des Hauptvertrags

(1) Der Auftragsverarbeiter wird dem Verantwortlichen nach Beendigung des Hauptvertrags — bei einem im Hauptvertrag vereinbarten Zeitraum zum Export der Inhalte beginnend mit dessen Ablauf — spätestens innerhalb von 30 Tagen alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Verantwortlichen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragsverarbeiter. Der Auftragsverarbeiter hat den dokumentierten Nachweis der ordnungsgemäßen Löschung auf Anfrage zu führen.

(2) Der Verantwortliche hat das Recht, die vollständige und vertragsgerechte Rückgabe oder Löschung der Daten beim Auftragsverarbeiter in geeigneter Weise zu kontrollieren.

(3) Der Auftragsverarbeiter ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm vom Verantwortlichen zugeleitet wurden oder die er für diesen erhoben hat.

§ 13 Schlussbestimmungen

(1) Soweit der Auftragsverarbeiter Unterstützungshandlungen nach dieser Vereinbarung nicht ausdrücklich kostenlos durchführt, kann er dem Verantwortlichen dafür eine angemessene Gebühr in Rechnung stellen, es sei denn, eigene Handlungen oder Unterlassungen des Auftragsverarbeiters haben diese Unterstützung unmittelbar erforderlich gemacht.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung wird dem Verantwortlichen vom Auftragsverarbeiter als bereits angenommenes Angebot zur Verfügung gestellt und wird mit ihrer Unterzeichnung durch den Verantwortlichen wirksam. Einer gesonderten Unterzeichnung durch den Auftragsverarbeiter bedarf es nicht; die Wirksamkeit tritt spätestens mit Wirksamwerden des Hauptvertrags ein. Die Unterzeichnung durch den Verantwortlichen kann auch elektronisch erfolgen; bei Online- bzw. Self-Service-Bestellungen wird diese Vereinbarung durch die elektronische Annahme im Bestellprozess wirksam.

(5) Eine isolierte Kündigung dieser Vereinbarung ist ausgeschlossen; ihre Laufzeit richtet sich nach dem Hauptvertrag und dauert – auch über dessen Ende hinaus – so lange fort, wie der Auftragsverarbeiter über personenbezogene Daten des Verantwortlichen verfügt. Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen hinsichtlich der Verarbeitung personenbezogener Daten die Regelungen dieser Vereinbarung vor.

(6) Diese Vereinbarung unterliegt deutschem Recht.

VERANTWORTLICHER

ORT / DATUM

_____

NAME / FUNKTION

_____

UNTERSCHRIFT

_____

AUFTRAGSVERARBEITER

SelectCode GmbH
vertreten durch Florian Baader
(Geschäftsführer)

Diese Vereinbarung ist seitens des Auftragsverarbeiters bereits angenommen. Eine gesonderte Unterschrift des Auftragsverarbeiters ist nicht erforderlich; sie wird mit der Unterzeichnung durch den Verantwortlichen wirksam.

Anlagen

Anlage 1 – Beschreibung der Daten/Datenkategorien

- Nutzerdaten: Name, E-Mail-Adresse, Abteilung, Profilbild (optional)
- Inhaltsdaten (insofern datenschutzrechtlich relevant)
- Bei Nutzung ausführender Werkzeuge oder Outpost Remote Operations: Befehle, Werkzeugparameter, Status- und Fehlermeldungen, Ausgaben, Bildschirmaufnahmen, eingegebene Zeichenfolgen und hieraus abgeleitete KI-Eingaben und -Ausgaben (soweit jeweils personenbezogen)
- Meta- und Kommunikationsdaten (wie z.B. Geräteinformationen, IP-Adressen)
- Nutzungs- & Analysedaten (wie z.B. gesparte Zeit, Anzahl der Prompts)

Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen

Mitarbeitende des Verantwortlichen, Nutzer der angebundenen Systeme und ggf. weitere Dritte, soweit deren personenbezogene Daten durch Nutzer, Connections, Werkzeuge oder Remote Operations verarbeitet werden

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragsverarbeiters

1. Einleitung

Der Auftragsverarbeiter betreibt ein nach **ISO/IEC 27001:2022** zertifiziertes Informationssicherheits-Managementsystem (ISMS) — Zertifikat-Nr. DE-IS-20250256, Proks Certification GmbH (DAkkS-akkreditiert), Geltungsbereich „Entwicklung und Betrieb der meinGPT AI SaaS-Plattform, einschließlich der angebotenen kundenspezifischen Dienstleistungen“, gültig bis 2028-12-16, Statement of Applicability (SoA) 1.2 (04.12.2025). Die nachfolgenden technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sind Bestandteil dieses ISMS; die rechte Spalte weist das zugrunde liegende Annex-A-Control aus. Der Betrieb der Plattform erfolgt in ISO-27001-zertifizierten Rechenzentren (Hetzner, Deutschland).

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

Maßnahme	ISO/IEC 27001:2022
Physische Sicherheitszonen, gesicherte Zutritte und Zutrittskontrolle	A.7.1–A.7.3
Physische Sicherheitsüberwachung (u. a. Videoüberwachung)	A.7.4
Clear-Desk-/Clear-Screen-Richtlinie	A.7.7
Sichere Authentifizierung, Zwei-Faktor-Authentifizierung	A.8.5
Verwaltung privilegierter Zugriffsrechte (Least Privilege)	A.8.2, A.8.18
Zugriffsbeschränkung nach Berechtigungskonzept, rollenbasiert	A.8.3
Verschlüsselung von Endgeräten; zentrale Authentifizierungs-/Passwortrichtlinien	A.8.1, A.5.17
Netzwerksicherheit: Firewalls, VPN, sichere Netzdienste	A.8.20, A.8.21
Netzsegmentierung; logische Mandantentrennung; Trennung Produktiv-/Testsystem	A.8.22
Schutz vor Schadsoftware	A.8.7
Data Leakage Prevention, Data Masking, Web-Filtering	A.8.12, A.8.11, A.8.23

Maßnahme	ISO/IEC 27001:2022
Sichere Löschung und Entsorgung von Daten und Datenträgern	A.8.10, A.7.14

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

Maßnahme	ISO/IEC 27001:2022
Verschlüsselung bei Übertragung (TLS) und Speicherung (at rest)	A.8.24
Protokollierung (Logging) und Überwachung von Aktivitäten	A.8.15, A.8.16
Schwachstellen-Management	A.8.8
Konfigurationsmanagement	A.8.9

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

Maßnahme	ISO/IEC 27001:2022
Regelmäßige, getestete Backups	A.8.13
Redundanz der Informationsverarbeitungssysteme	A.8.14
Kapazitätsmanagement	A.8.6
Business-Continuity- und Notfallkonzept (definierte RTO/RPO, regelmäßige Tests)	A.5.29, A.5.30

5. Sicherer Entwicklungszyklus

Maßnahme	ISO/IEC 27001:2022
Sicherer Entwicklungslebenszyklus, Secure Coding	A.8.25, A.8.28
Sichere Systemarchitektur und -entwicklungsgrundsätze	A.8.27

6. Verfahren, Governance und Auftragskontrolle (Art. 32 Abs. 1 lit. d; Art. 25 DSGVO)

Maßnahme	ISO/IEC 27001:2022
Zertifiziertes ISMS, interne Audits und Management-Reviews	ISO/IEC 27001 Kap. 4–10
Risikomanagement und Threat Intelligence	A.5.7
Incident-Management und Meldeprozesse (Art. 33/34 DSGVO)	A.5.24–A.5.28
Lieferanten- und IKT-Lieferkettenmanagement	A.5.19–A.5.23
Verpflichtung der Mitarbeiter auf Vertraulichkeit; regelmäßige Schulungen	A.6.1–A.6.6
Privacy by Design & Default; Verzeichnis von Verarbeitungstätigkeiten	Art. 25, 30 DSGVO

heyData

Externer Datenschutzbeauftragter
heyData GmbH · Schützenstr. 5 · 10117 Berlin · datenschutz@heydata.eu

Anlage 4 – Aktuelle Unterauftragnehmer

Die Aufnahme eines Unterauftragnehmers in diese Liste bedeutet dessen allgemeine Genehmigung für den beschriebenen Zweck. Sie bedeutet nicht, dass der Anbieter bei jeder Verarbeitung oder für jede Organisation eingesetzt wird. Der tatsächliche Einsatz richtet sich nach der gebuchten Leistung, der Administratorkonfiguration, der konkreten Funktionsnutzung und gegebenenfalls der Modellwahl.

Die ausgewiesene Einsatzbedingung zeigt, wann der jeweilige Anbieter einbezogen werden kann: „Allgemeiner Plattformbetrieb“ bezeichnet regulär verfügbare Basisdienste. „Nur im Notfall- oder Ausweichfall“ bezeichnet Rückfalldienste. „Nur bei konkreter Nutzung“ bedeutet, dass der Anbieter nur durch die Nutzung der zugeordneten Funktion, eines entsprechenden Modells oder einer darauf beruhenden Konfiguration einbezogen wird.

Das EU-Symbol kennzeichnet die Verarbeitung von Kundeninhalten innerhalb der Europäischen Union; die konkrete Region kann innerhalb der EU variieren. Es bezeichnet nicht den Unternehmenssitz des jeweiligen Anbieters. ZDR (Zero Data Retention) kennzeichnet Dienste, bei denen keine dauerhafte Kopie der übermittelten Inhaltsdaten auf anbietereigener Infrastruktur gespeichert wird. Eine Speicherung in einem von SelectCode kontrollierten Speicher bleibt unberührt. Ein Gedankenstrich bedeutet, dass die Kennzeichnung für den jeweiligen Dienst nicht anwendbar ist.

Basisinfrastruktur und Plattformbetrieb

Diese Anbieter können unabhängig von einer konkreten Modell- oder Funktionsauswahl für den allgemeinen Plattformbetrieb eingesetzt werden.

Name	Einsatzbedingung und Zweck	Datenstandort	ZDR
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen	ALLGEMEINER PLATTFORMBETRIEB Hosting und Speicherung von Plattform- und Kundendaten	EU	—
Ubicloud B.V. Turfschip 267 1186XK, Amstelveen, The Netherlands	ALLGEMEINER PLATTFORMBETRIEB Datenbankbetrieb	EU	—
BunnyWay d.o.o. Dunajska cesta 165, 1000 Ljubljana, Slovenia	ALLGEMEINER PLATTFORMBETRIEB Schutz der Plattform und Auslieferung von Bildinhalten	EU	—
Lettermint B.V. Willemsvaart 16 B, 8019 AB Zwolle, Niederlande	ALLGEMEINER PLATTFORMBETRIEB Versand und Empfang plattformbezogener E-Mails	EU	—
Amazon Web Services EMEA SARL 38 avenue John F. Kennedy, L-1855 Luxembourg	NUR IM NOTFALL- ODER AUSWEICHFALL Versand und Empfang plattformbezogener E-Mails (Amazon SES)	EU	—
Scaleway SAS 8 rue de la Ville l'Évêque, 75008 Paris, France	NUR IM NOTFALL- ODER AUSWEICHFALL Backup-Infrastruktur	EU	—

Bedarfsabhängige KI- und Funktionsdienste

KI-Modelle und KI-Funktionen können abhängig von der Nutzung Texte, Bilder und Dokumente verarbeiten, insbesondere zur Generierung, Analyse, Texterkennung (OCR) und Erstellung von Embeddings. Administratoren können verfügbare Modelle organisationsweit freigeben oder sperren. Welcher der folgenden Anbieter eingesetzt wird, richtet sich nach der Modell- oder Funktionswahl, der Administratorkonfiguration, einem konfigurierten Assistenten oder Workflow oder der automatischen Modellauswahl. Nicht alle aufgeführten Anbieter werden gleichzeitig eingesetzt.

Name	Einsatzbedingung und Zweck	Datenstandort	ZDR
DeepL SE Maarweg 165, 50825 Köln, Deutschland	NUR BEI KONKRETER NUTZUNG Maschinelle Übersetzung	EU	✓
Microsoft Ireland Operations, Ltd. One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	NUR BEI KONKRETER NUTZUNG KI-Modelle und KI-Funktionen; Dokumentenerkennung mit Microsoft Document Intelligence (OCR)	EU	✓
OpenAI Ireland Ltd. The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	NUR BEI KONKRETER NUTZUNG KI-Modelle und KI-Funktionen	EU	✓
Mistral AI SAS 15 rue des Halles 75001, Paris, Frankreich	NUR BEI KONKRETER NUTZUNG KI-Modelle und KI-Funktionen	EU	✓
Google Ireland Limited Gordon House, Barrow Street, Dublin 4, Dublin, Irland	NUR BEI KONKRETER NUTZUNG KI-Modelle und KI-Funktionen; maschinelle Übersetzung	EU	✓
SAS SPOKE (Meeting BaaS) 35 rue Pauline Borghèse, 92200 Neuilly-sur-Seine, Frankreich	NUR BEI KONKRETER NUTZUNG Teilnahme an und Aufzeichnung von Online-Meetings	EU	✓
GLADIA SAS 38 rue de la Tremblaie 35510 Cesson-Sévigné, Frankreich	NUR BEI KONKRETER NUTZUNG Transkription von Audio- und Videoaufnahmen	EU	✓
Nebius B. V. Gustav Mahlerlaan 300, 1082 ME Amsterdam, Niederlande	NUR BEI KONKRETER NUTZUNG KI-Modelle und Embeddings	EU	✓
Amazon Web Services EMEA SARL 38 avenue John F. Kennedy, L-1855 Luxembourg	NUR BEI KONKRETER NUTZUNG KI-Modelle und KI-Funktionen (AWS Bedrock)	EU	✓
IONOS Cloud GmbH Elgendorfer Straße 57, 56410 Montabaur, Deutschland	NUR BEI KONKRETER NUTZUNG KI-Modelle, OCR und Embeddings	EU	✓
STACKIT GmbH & Co. KG Stiftsbergstraße 1, 74172 Neckarsulm, Deutschland	NUR BEI KONKRETER NUTZUNG KI-Modelle und Embeddings (STACKIT AI Model Serving)	EU	✓
T-Systems International GmbH Friedrich-Ebert-Allee 140, 53113 Bonn, Deutschland	NUR BEI KONKRETER NUTZUNG Telekom-gehostete KI-Modelle, Embeddings und Spracherkennung (AIFS)	EU	✓
DataCrunch Oy (Verda) Sanomatalo, Töölönlahdenkatu 2, 00100 Helsinki, Finland	NUR BEI KONKRETER NUTZUNG Kundenspezifische KI-Modelle	EU	✓
TensorX Ltd. Unit 25, Classon House, Dundrum Business Park, Dublin 14, Ireland	NUR BEI KONKRETER NUTZUNG Open-Source-KI-Modelle	EU	✓
Linkup Technologies 28 avenue des Pépinières, 94260 Fresnes, France	NUR BEI KONKRETER NUTZUNG Websuche für KI-Funktionen	EU	✓