Standardvertragsklauseln zwischen Verantwortlichem und Auftragsverarbeiter gemäß Art. 28 Abs. 7 DS-GVO – Durchführungsbeschluss (EU) 2021/915

synthemis-Plattform
Version 1.2 Stand: 14.11.2026

Hinweis zur Struktur: Abschnitte I–III sowie die Anhänge I–IV geben den amtlichen Wortlaut des Durchführungsbeschlusses (EU) 2021/915 wieder. Nicht einschlägige Bezugnahmen auf die Verordnung (EU) 2018/1725 wurden an zwei Stellen redaktionell weggelassen. Ausgefüllt sind nur die in den Klauseln und Anhängen vorgesehenen Felder und Optionen. Sämtliche darüber hinausgehenden, vom Auftragnehmer ergänzten Regelungen sind in Anhang V gesondert zusammengefasst (gemäß Klausel 2 Buchst. b zulässige ergänzende Klauseln, die den Standardvertragsklauseln nicht widersprechen).

Abschnitt I

Klausel 1 – Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2 – Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3 – Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4 – Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Die fakultative Klausel 5 (Kopplungsklausel) wird nicht verwendet.

Abschnitt II – Pflichten der Parteien

Klausel 6 – Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7 – Pflichten der Parteien

7.1. Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

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

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

Gewählt: OPTION 2 – Allgemeine schriftliche Genehmigung

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Kalendertage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen),

so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8 – Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

(1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

(2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

(3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

(4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9 – Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

(1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

(2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

(3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

Abschnitt III – Schlussbestimmungen

Klausel 10 – Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

(1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

(2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

(3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln,

der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Anhang I – Liste der Parteien

Verantwortlicher

Name: Die Organisation (Kunde), für die bei der Registrierung auf der synthemis-Plattform ein Konto angelegt wird. Beim Website-Check ohne Anmeldung (§ 5a Abs. 2 AGB) ist Verantwortlicher der Unternehmer, für den der Check gestartet wird („Nutzer des Checks“); Anschrift und Kontaktperson werden dabei nicht erhoben.

Anschrift: ergibt sich aus den bei der Kontoerstellung hinterlegten Stammdaten des Kunden.

Name, Funktion und Kontaktdaten der Kontaktperson: Es gelten die Angaben im Kundenkonto.

Unterschrift und Beitrittsdatum: Annahme elektronisch mit Abschluss der Registrierung; angenommene Version, Zeitpunkt und Konto werden protokolliert (vgl. Anhang V Ziff. 1). Beim Website-Check ohne Anmeldung: Annahme elektronisch mit dem Start des Checks (Anhang V Ziff. 1.1).

Auftragsverarbeiter

Name: synthemis UG (haftungsbeschränkt) i. G.

Anschrift: Rheinaustraße 149, 53225 Bonn

Vertretungsberechtigte Geschäftsführer und Kontaktpersonen: Moritz Albrecht und Martin Zwick, hallo@synthemis.ai

Unterschrift und Beitrittsdatum: elektronisch bereitgestellt mit der jeweils gültigen Version dieser Klauseln.

Anhang II – Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

Abhängig von den vom Kunden eingestellten Dokumenten, seinen Angaben im Audit, den Inhalten seiner Website und der im Website-Check geprüften Website, insbesondere:

- Beschäftigte, Bewerber und ehemalige Beschäftigte des Kunden;
- Organe und Funktionsträger des Kunden, insbesondere Geschäftsführung, Datenschutzbeauftragter, IT-Sicherheitsbeauftragter und Ansprechpersonen;
- Kunden, Mandanten, Interessenten und sonstige Vertragspartner des Kunden;
- Dienstleister, Lieferanten und Auftragsverarbeiter des Kunden sowie deren Ansprechpersonen;
- sonstige Personen, die in den Dokumenten oder auf der Website des Kunden oder der im Website-Check geprüften Website genannt oder abgebildet sind.

Kategorien personenbezogener Daten, die verarbeitet werden

- **Stammdaten und Angaben im Audit:** Namen, Funktionen und Kontaktdaten von Geschäftsführung, Datenschutzbeauftragtem, IT-Sicherheitsbeauftragtem und Ansprechpersonen; Antworten und Freitexte des Kunden zu Unternehmensfragen und Rückfragen.
- **In hochgeladenen Dokumenten enthaltene Daten:** Kontakt- und Identifikationsdaten sowie weitere im jeweiligen Dokument enthaltene personenbezogene Daten; ggf. in Geschäftsgeheimnissen enthaltene personenbezogene Daten.
- **Inhalte der Website des Kunden:** öffentlich abrufbare Texte einschließlich der darin genannten personenbezogenen Daten, etwa im Impressum oder auf Team- und Kontaktseiten.
- **Website-Check: auf der geprüften Website veröffentlichte personenbezogene Daten, soweit sie in den erfassten Angaben oder auf Bildschirmfotos der Website erscheinen, etwa Namen und Kontaktdaten im Impressum.**

Verarbeitete sensible Daten und angewandte Beschränkungen oder Garantien

Keine. Die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DS-GVO) sowie personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO) ist nicht Gegenstand des Auftrags und ausgeschlossen. Der Kunde verpflichtet sich, keine derartigen Daten in die Plattform einzustellen (vgl. Anhang V Ziff. 4).

Art der Verarbeitung

Erhebung (einschließlich Abruf der Website des Kunden), Speicherung, Pseudonymisierung, Auswertung auch mithilfe großer Sprachmodelle (externe Sprachmodelle erhalten nur pseudonymisierte Inhalte, Anhang V Ziff. 2) sowie Löschung im Rahmen eines KI-gestützten Compliance-Audits. Beim Website-Check (§ 5a AGB): automatisierter Abruf der angegebenen Website, Erfassung der geladenen Dienste, Cookies und Verbindungen, Anfertigung von Bildschirmfotos, Anzeige, Speicherung und Löschung des Ergebnisses, ohne Einsatz von Sprachmodellen.

Zweck(e) der Verarbeitung im Auftrag des Verantwortlichen

Durchführung eines KI-gestützten Compliance-Audits nach § 3 AGB: Auswertung der Website, der Stammdaten und der Angaben des Kunden sowie, bei kostenpflichtigen Leistungen, der hochgeladenen Dokumente; Erstellung einer automatisierten Gap-Analyse und, bei kostenpflichtigen Leistungen, eines Detail-Audits mit Bericht. Die Ergebnisse sind keine Rechtsberatung (§ 4 AGB). Zum Einsatz großer Sprachmodelle siehe Anhang V Ziff. 2. Beim Website-Check (§ 5a AGB): technische Prüfung der angegebenen Website und Anzeige des Ergebnisses. Auf Weisung des Verantwortlichen zeigt der Auftragsverarbeiter das Ergebnis

für kurze Zeit auch anderen Nutzern an, die dieselbe Website prüfen, und verwendet die technische Messung ohne Bildschirmfotos für ein Audit derselben Website (§ 5a Abs. 8 AGB).

Dauer der Verarbeitung

Für die Dauer des Nutzungsverhältnisses nach den AGB. Im Einzelnen:

a) Hochgeladene Dokumente und die daraus gewonnenen Volltexte werden nach Maßgabe von Anhang III gelöscht. Die daraus abgeleiteten Analysedaten – Prüfergebnisse mit Begründungen und Auszügen aus den pseudonymisierten Texten sowie die für die Pseudonymisierung gespeicherten zusätzlichen Informationen (Art. 4 Nr. 5 DS-GVO), mit denen die Ergebnisse dem Kunden wieder im Klartext angezeigt werden – werden für die Dauer des Nutzungsverhältnisses gespeichert, damit der Kunde seine Ergebnisse vollständig abrufen kann; ihre Löschung richtet sich nach Buchst. b.

b) Bei Beendigung des Vertrags oder vom Kunden veranlasster Löschung des Kontos werden die im Auftrag verarbeiteten personenbezogenen Daten zunächst für 30 Kalendertage gesperrt archiviert; innerhalb dieser Frist kann der Kunde die Löschung durch Reaktivierung des Kontos rückgängig machen. Diese Aufbewahrung dient dem Schutz des Kunden vor versehentlicher oder unbefugter Löschung und erfolgt als dokumentierte, mit Annahme dieser Klauseln erteilte Weisung des Verantwortlichen (Klausel 7.1 Buchst. a). Nach fruchtlosem Ablauf der Frist werden die Daten gemäß Klausel 10 Buchst. d gelöscht.

c) Kopien in Datensicherungen werden spätestens 30 Kalendertage nach ihrer Erstellung gelöscht. Wird nach einem Zwischenfall eine Sicherung zurückgespielt, führt der Auftragsverarbeiter Löschungen, die nach dem Stand der Sicherung erfolgt sind, erneut aus.

d) Website-Check ohne Anmeldung: Das Ergebnis wird höchstens 24 Stunden zur Anzeige und zur Übernahme in ein Konto vorgehalten, Bildschirmfotos höchstens 60 Minuten, die technische Messung ohne Bildschirmfotos höchstens 72 Stunden; danach wird es gelöscht. Die Rückgabe erfolgt durch die Anzeige des Ergebnisses. Wird der Check angemeldet gestartet oder in ein Konto übernommen, gilt die Dauer des Nutzungsverhältnisses.

e) Daten, die der Auftragsverarbeiter als eigener Verantwortlicher verarbeitet – insbesondere Rechnungs- und Buchungsdaten (Aufbewahrung 8 Jahre, § 147 Abs. 3 AO, § 257 Abs. 4 HGB, § 14b Abs. 1 UStG), Handels- und Geschäftsbriefe (6 Jahre, § 147 Abs. 3 AO, § 257 Abs. 4 HGB) sowie Vertrags- und Abrechnungsdaten zur Geltendmachung oder Abwehr von Rechtsansprüchen (§§ 195, 199 BGB) –, unterliegen nicht diesen Klauseln; Fristbeginn jeweils mit Schluss des Kalenderjahres. Einzelheiten regelt die Datenschutzerklärung des Auftragsverarbeiters.

Anhang III – Technische und organisatorische Maßnahmen (Art. 32 DS-GVO)

Pseudonymisierung und Verschlüsselung

- Hochgeladene Dokumente werden nach dem Upload automatisch pseudonymisiert; der pseudonymisierte Text wird gespeichert und ist Grundlage der weiteren Verarbeitung.
- Mehrstufiges Verfahren: musterbasierte Erkennung, ML-gestützte Eigennamenerkennung und kontextbezogene Prüfung.
- Externen Sprachmodellen werden Dokumenttexte, Website-Inhalte, Stammdaten und Angaben im Audit ausschließlich pseudonymisiert bereitgestellt; die Zuordnungsinformationen verbleiben beim Auftragsverarbeiter. Liegt für einen Inhalt keine pseudonymisierte Fassung vor, unterbleibt seine Auswertung durch ein externes Sprachmodell. Einzelheiten regelt Anhang V Ziff. 2.
- Verschlüsselung bei der Übermittlung (TLS).
- Verschlüsselung ausgewählter personenbezogener Datenbankinhalte im Ruhezustand.
- Originaldokumente werden 30 Kalendertage nach Abschluss des Audits gelöscht (ein Audit ohne Abschluss gilt 365 Kalendertage nach seiner letzten Aktivität als abgeschlossen), nicht in einem Audit verwendete Uploads 30 Kalendertage nach dem Hochladen; die daraus abgeleiteten Volltexte und pseudonymisierten Texte werden zeitgleich gelöscht.

Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

- Authentifizierung mit optionaler Zwei-Faktor-Absicherung (TOTP, E-Mail-Code) sowie Passkeys; Sitzungen mit Inaktivitäts- und absoluter Höchstdauer.
- Rollenbasiertes Berechtigungskonzept nach dem Need-to-know-Prinzip; mandantenbezogene Trennung: jeder Datenzugriff ist auf Anwendungsebene an die Organisation des angemeldeten Nutzers gebunden.
- Protokollierung sicherheitsrelevanter Ereignisse sowie jedes Analyseaufrufs an ein Sprachmodell mit Zeitpunkt, Modell und Umfang.
- Ratenbegrenzung sicherheitskritischer Endpunkte; Schutz vor Anfragen an interne Netzressourcen bei der Verarbeitung vom Kunden angegebener Webadressen.
- Regelmäßige Sicherung der Systeme und Wiederherstellbarkeit nach einem Zwischenfall. Tägliche Sicherung der Datenbanken und der verschlüsselten Dokumentenablage auf einen getrennten Speicher in Deutschland; die Sicherungen werden vor der Übertragung verschlüsselt, der Speicheranbieter erhält keine Schlüssel. Sicherungen werden spätestens nach 30 Kalendertagen gelöscht. Die Wiederherstellung wird mindestens vierteljährlich erprobt.

Hosting / physische Sicherheit

- Hosting bei OVH, ausschließlich Rechenzentren innerhalb der EU/des EWR. Datensicherung bei Hetzner Online GmbH in Rechenzentren in Deutschland (Anhang IV).

Verfahren zur regelmäßigen Überprüfung

- Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen.

Spezifische Maßnahmen zur Unterstützung des Verantwortlichen (Klausel 8 Buchst. d, Klausel 9)

- Bereitstellung der zur Beantwortung von Betroffenenanträgen und zur Erfüllung der Melde- und Benachrichtigungspflichten (Art. 33, 34 DS-GVO) erforderlichen Informationen über den benannten Datenschutzkontakt; Meldung von Verletzungen unverzüglich nach Bekanntwerden mit den in Klausel 9.2 genannten Mindestangaben.

Anhang IV – Liste der Unterauftragsverarbeiter

Vereinbarte Liste der Unterauftragsverarbeiter im Sinne von Klausel 7.7 Buchst. a (Option 2 – allgemeine schriftliche Genehmigung des Verantwortlichen):

Name, Anschrift	**Name, Funktion, und Kontaktdaten der Kontaktperson**	**Beschreibung der Verarbeitung**	**Ort der Datenverarbeitung**
OVH SAS mit einem Kapital von 50 000 000 € RCS Lille Métropole 424 761 419 00045 APE-Code 2620Z USt-IdNr.: FR 22 424 761 419 Geschäftssitz: 2 Rue Kellermann – 59100 Roubaix – Frankreich.	Datenschutzkontakt: Online-Formular unter www.ovh.de/schutz-personenbezogener-daten/rechte-ausueben	Hosting der Plattform und Ablage der im Auftrag verarbeiteten Daten, insbesondere der hochgeladenen Dokumente.	EU/EWR, EU/EWR; Rechenzentrum in Limburg (DE), oder Gravelines, Roubaix, Straßburg (FR).
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland	Datenschutzkontakt: data-protection@hetzner.com	Speicherung der verschlüsselten Datensicherungen (Storage Box). Hetzner erhält keine Schlüssel und kann die Inhalte nicht lesen.	Deutschland; keine Drittlandübermittlung.
OpenAI Ireland Limited, 1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland	Datenschutzkontakt: privacy@openai.com	Auswertung pseudonymisierter Dokumenttexte, Website-Inhalte, Stammdaten und Angaben im Audit durch ein großes Sprachmodell (vgl. Anhang V Ziff. 2); keine Speicherung von Antworten zur Wiederverwendung, keine Nutzung zum Training.	Drittlandübermittlung: nur soweit ein übermittelter Inhalt trotz Pseudonymisierung personenbezogene Daten enthält (Anhang V Ziff. 2.3). Verarbeitung auch in den USA durch verbundene Unternehmen von OpenAI; Grundlage: Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DS-GVO) im Data Processing Addendum von OpenAI.

Anhang V – Ergänzende Vereinbarungen der Parteien

Dieser Anhang enthält ergänzende Regelungen im Sinne von Klausel 2 Buchst. b. Sie treten zu den Standardvertragsklauseln (Abschnitte I–III) hinzu, ändern diese nicht und stehen weder unmittelbar noch mittelbar im Widerspruch zu ihnen. Bei einem etwaigen Widerspruch gehen gemäß Klausel 4 die Standardvertragsklauseln vor.

1. Elektronischer Abschluss, Form, Anwenderkreis, Nachweis

1.1 Diese Klauseln werden elektronisch abgeschlossen. Der Kunde nimmt sie an, indem er die Registrierung abschließt, nachdem ihm diese Klauseln und die AGB unmittelbar vor dem Abschluss als Vertragsbestandteil benannt und zum Abruf und Download bereitgestellt wurden. Beim Website-Check ohne Anmeldung (§ 5a Abs. 2 AGB) nimmt der Nutzer des Checks diese Klauseln an, indem er den Check startet, nachdem ihm diese Klauseln und die AGB unmittelbar vor dem Start benannt und zum Abruf und Download bereitgestellt wurden; er gilt insoweit als Kunde. Einer gesonderten Bestätigung, etwa durch Setzen eines Häkchens, bedarf es nicht. Der Abschluss in elektronischer Form genügt Art. 28 Abs. 9 DS-GVO; eine eigenhändige Unterschrift ist nicht erforderlich.

1.2 Der Auftragsverarbeiter verschafft dem Kunden bei Vertragsschluss die Möglichkeit, diese Klauseln einschließlich der Anhänge abzurufen und in wiedergabefähiger Form zu speichern (§ 312i Abs. 1 S. 1 Nr. 4 BGB), und dokumentiert die angenommene Version, den Zeitpunkt und das Konto, mit dem die Registrierung abgeschlossen wurde. Beim Website-Check ohne Anmeldung dokumentiert er, welche Version zu welchem Zeitpunkt bereitgestellt war, und protokolliert den Check mit Zeitpunkt, ohne Zuordnung zu einer Person oder einem Anschluss.

1.3 Diese Klauseln richten sich ausschließlich an Unternehmer (§ 14 BGB) sowie juristische Personen des öffentlichen Rechts und öffentlich-rechtliche Sondervermögen. Der Kunde bestätigt mit der Annahme, nicht als Verbraucher (§ 13 BGB) zu handeln.

1.4 Individuell zwischen den Parteien getroffene Abreden haben gemäß § 305b BGB unabhängig von ihrer Form Vorrang; Klausel 4 der Standardvertragsklauseln bleibt unberührt.

1.5 Änderungen dieser Klauseln bietet der Auftragsverarbeiter nach dem Verfahren des § 20 Abs. 2 AGB an. Änderungen der Liste der Unterauftragsverarbeiter (Anhang IV) richten sich ausschließlich nach Klausel 7.7 Buchst. a.

1.6 Die Unterrichtung nach Klausel 7.7 Buchst. a erfolgt in Textform (§ 126b BGB), in der Regel per E-Mail an die Organisations-Admins des Kunden. Die Parteien sind sich einig, dass die Textform die schriftliche Form im Sinne der Klausel 7.7 Buchst. a wahrt; Art. 28 Abs. 9 DS-GVO lässt auch insoweit das elektronische Format genügen.

2. Einsatz großer Sprachmodelle (LLM); Pseudonymisierung; Datenstandort

2.1 Hosting und Speicherung der im Auftrag verarbeiteten Daten erfolgen ausschließlich in Rechenzentren innerhalb der EU/des EWR. Eine Übermittlung personenbezogener Daten in Drittländer erfolgt nur an die in Anhang IV als solche gekennzeichneten Unterauftragsverarbeiter und nur unter den Voraussetzungen von Kapitel V DS-GVO (Klausel 7.8).

2.2 Pseudonymisierung vor jeder Übermittlung. Alle Inhalte, die an ein externes Sprachmodell übermittelt werden – Texte hochgeladener Dokumente, Inhalte der Website des Kunden, seine Stammdaten sowie seine Antworten und Freitexte im Audit –, werden zuvor auf Systemen des Auftragsverarbeiters innerhalb der EU/des EWR pseudonymisiert. Ersetzt werden alle Angaben, die eine natürliche Person erkennbar machen, insbesondere Namen, persönliche E-Mail-Adressen und Telefonnummern sowie Firmen, Anschriften, E-Mail-Adressen und Domains, die den Namen einer natürlichen Person enthalten. Erhalten bleiben Angaben ohne Bezug zu einer natürlichen Person, insbesondere Firmen juristischer Personen ohne Personennamen sowie Namen von Diensten, Anbietern und Behörden, weil ihre Prüfung Gegenstand des Audits ist. Die Zuordnungsinformationen verbleiben ausschließlich beim Auftragsverarbeiter und werden dem Anbieter nicht übermittelt; der Anbieter kann einen

Personenbezug daher nicht herstellen. Inhalte, für die keine pseudonymisierte Fassung vorliegt, werden nicht an ein externes Sprachmodell übermittelt.

2.3 Rückführung und Auffangregel. Die Antworten des Sprachmodells werden erst auf Systemen des Auftragsverarbeiters in Klartext zurückgeführt und nur Nutzern des Kunden angezeigt. Die Pseudonymisierung erfolgt automatisiert nach dem Stand der Technik; dass jede personenbezogene Angabe erkannt wird, kann nicht garantiert werden. Lässt sich im Einzelfall nicht ausschließen, dass ein übermittelter Inhalt personenbezogene Daten enthält, ist der Anbieter insoweit Unterauftragsverarbeiter nach Anhang IV; eine Übermittlung in ein Drittland erfolgt dann nur auf der dort genannten Grundlage (Klausel 7.8).

2.4 Der Auftragsverarbeiter setzt nur Anbieter ein, die übermittelte Inhalte nicht zum Training ihrer Modelle verwenden.

2.5 Sprachmodelle, die der Auftragsverarbeiter auf eigenen Servern innerhalb der EU/des EWR betreibt, verarbeiten Inhalte auch ohne Pseudonymisierung, insbesondere um personenbezogene Daten vor der Übermittlung zu erkennen.

3. Zusatzvereinbarung für Berufsgeheimnisträger (§ 203 StGB)

Diese Ziffer 3 gilt ergänzend, soweit der Kunde Berufsgeheimnisträger im Sinne des § 203 Abs. 1 StGB ist und der Verschwiegenheitspflicht über Geheimnisse unterliegt, die ihm in Ausübung seines Berufs anvertraut worden sind oder die er dabei erfahren hat („Geheimnisse“). Maßgeblich ist § 203 StGB in der jeweils geltenden Fassung. Der Auftragsverarbeiter bestätigt, über die Verschwiegenheitspflicht und die strafrechtlichen Folgen ihrer Verletzung belehrt worden zu sein.

3.1 Verschwiegenheitspflicht und Belehrung. Der Auftragsverarbeiter ist zur Verschwiegenheit verpflichtet. Im Hinblick auf § 203 StGB verpflichtet er sich, sich nur insoweit Kenntnis von Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist. Unter „sich Kenntnis verschaffen“ verstehen die Parteien den Vorgang der kognitiven, menschlichen und inhaltlichen Kenntnisnahme. Die Verschwiegenheitspflicht gilt zeitlich unbeschränkt und über die Beendigung des Vertrags hinaus. Dem Auftragsverarbeiter ist bewusst, dass die unbefugte Offenbarung von Geheimnissen strafrechtliche Folgen nach § 203 StGB (Geld- oder Freiheitsstrafe) haben kann.

3.2 Weitere Mitwirkende. Der Auftragsverarbeiter stellt sicher, dass die zur Leistungserbringung herangezogenen Mitwirkenden und Unterauftragsverarbeiter, die Kenntnis von Geheimnissen erlangen oder sich verschaffen könnten, in Textform zur Verschwiegenheit verpflichtet werden (§ 203 Abs. 4 S. 2 Nr. 1 StGB; für Rechtsanwälte zudem § 43e BRAO, für andere Berufsgruppen die jeweiligen berufsrechtlichen Parallelvorschriften).

4. Ausschluss besonderer Kategorien (Art. 9 DS-GVO und Art. 10 DS-GVO)

Der Kunde stellt sicher, dass er weder besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DS-GVO noch personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO in die Plattform einstellt. Die Verarbeitung solcher Daten ist nicht Gegenstand des Auftrags.