Beglaubigte Übersetzung aus dem Englischen

Auftragsverarbeitungsvertrag auf Basis der EU Standardvertragsklauseln

zwischen

ThinkOwl Europe GmbH

Carl-Benz-Straße 10-12
56218 Mülheim-Kärlich

nachfolgend kurz „ThinkOwl" genannt

und

_____

_____

_____

nachfolgend kurz „**Kunde**" genannt

Präambel

Diese Auftragsverarbeitung ("**DPA**" oder "**AVV**") ist Teil des Rahmen-Abonnementvertrags bzw. Master Subscription Agreement („**MSA**" oder „**Hauptvertrag**") zwischen der ThinkOwl Europe GmbH („**Auftragsverarbeiter**") und dem Kunden („**Verantwortlicher**"). Diese Auftragsverarbeitung ist auf Basis der EU Standardvertragsklauseln („**EU SCC**") vom 4. Juni 2021 erstellt worden.

1 Vertragsbestandteile

Vertragsbestandteile sind dieser **Vertragstext** sowie die **EU Standardvertrags-klauseln** bestehend aus:

- Abschnitt I – Allgemeines
- Abschnitt II - Pflichten der Parteien
- Abschnitt III – Schlussbestimmungen
  sowie
- Anhang I – Liste der Parteien
- Anhang II – Beschreibung der Verarbeitung
- Anhang III – Technische und organisatorische Maßnahmen, einschließlich zur Gewährung der Sicherheit der Daten
- Anhang IV – Liste der Unterauftragnehmer

Beglaubigte Übersetzung aus dem Englischen

2 Ergänzungen zu den Standardvertragsklauseln

2.1 *Nachweise und Kosten für Prüfungen*

Gemäß Klausel 7.6 der Standardvertragsklauseln stellt der Auftragsverarbeiter Nachweise zur Einhaltung der Standardvertragsklauseln bereit. ThinkOwl ist berechtigt, hierfür eine Vergütung zu verlangen. Die Vergütung ist im Vorfeld zu vereinbaren. ThinkOwl wird den Kunden vor einem Audit ein Angebot unterbreiten. Die Vergütungssätze dürfen die für IT-Leistungen üblichen Vergütungssätze, jedenfalls den Vergütungssatz nach Ziffer 1.13 des MSA, nicht überschreiten. Externe Kosten der ThinkOwl, wie z.B. Auditkosten bei Dienstleistern, sind vom Kunden vollständig zu übernehmen.

Die folgenden Nachweise zu datenschutzrechtlichen Auditrechten werden kostenfrei zur Verfügung gestellt:

- Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 der Datenschutz-Grundverordnung.
- Zertifizierung gemäß einem genehmigten Zertifizierungsverfahren nach Artikel 42 der Datenschutz-Grundverordnung.
- aktuelle Bescheinigungen, Berichte oder Berichtsauszüge von unabhängigen Stellen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- geeignete Zertifizierungen durch IT-Sicherheits- oder Datenschutzaudit.

Mülheim-Kärlich, 1. August 2025

ThinkOwl

Kunde

Beglaubigte Übersetzung aus dem Englischen

Standardvertragsklauseln

ABSCHNITT I - Allgemeines

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, 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.

Beglaubigte Übersetzung aus dem Englischen

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 zu lesen und 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.

Klausel 5 – fakultativ

Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

Beglaubigte Übersetzung aus dem Englischen

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.

Beglaubigte Übersetzung aus dem Englischen

7.7 Einsatz von Unterauftragsverarbeitern

a) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: 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 4 Wochen 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 dieser 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;

Beglaubigte Übersetzung aus dem Englischen

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.

Beglaubigte Übersetzung aus dem Englischen

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 mindestens 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.

Beglaubigte Übersetzung aus dem Englischen

ANHANG I – LISTE DER PARTEIEN

Verantwortliche(r): [*Name und Kontaktdaten des/der Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten des Verantwortlichen*]

1. Name:

   Anschrift:

   Name, Funktion und Kontaktdaten der Kontaktperson:

   Unterschrift und Beitrittsdatum:

2. Name:

   Anschrift:

   Name, Funktion und Kontaktdaten der Kontaktperson:

   Unterschrift und Beitrittsdatum:

Auftragsverarbeiter: [*Name und Kontaktdaten des Auftragsverarbeiter/der Auftrgverarbeiter und gegebenenfalls des/der Datenschutzbeauftragten des Auftragsverarbeiters/der Auftragsverarbeiter*]

1. Name: ThinkOwl Europe GmbH

   Anschrift: Carl-Benz-Str. 10-12, D-56218 Mülheim-Kärlich

   Name, Funktion und Kontaktdaten der Kontaktperson: Rolf Esau, CEO, rolf.esau@thinkowl.com

   Unterschrift und Beitrittsdatum: 1. August 2025

Beglaubigte Übersetzung aus dem Englischen

2. Name: ThinkOwl Europe GmbH

Anschrift: Carl-Benz-Str. 10-12, D-56218 Mülheim-Kärlich

Name, Funktion und Kontaktdaten der Kontaktperson: Peter Macherey, Datenschutzbeauftragter, privacy@thinkowl.com

Unterschrift und Beitrittsdatum: 1. August 2025

Beglaubigte Übersetzung aus dem Englischen

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

Alle Arten von Kunden, Verbrauchern und Geschäftspartnern des Unternehmens, die eine Dienstleistung des Unternehmens anfordern.

Kategorien personenbezogener Daten, die verarbeitet werden

E-Mail-Adressen und andere Kontaktinformationen können als personenbezogene Daten im Service gespeichert werden. Das Unternehmen ist verpflichtet, nur die personenbezogenen Daten im Service zu speichern oder aufzuzeichnen, die im normalen Geschäftsverlauf und bei der Nutzung des Services benötigt werden.

Art und Zweck der Verarbeitung sowie Informationen zur Verarbeitung von sensiblen Daten

Als Teil einer Cloud-Anwendung werden im Rahmen des Services E-Mails, Dokumente, Sprachaufzeichnungen, Textnachrichten, jegliche Art von Anhängen, Chats, Namen und andere Servicedaten verarbeitet. In diesem Zusammenhang können personenbezogene Daten durch das Unternehmen im Service gespeichert werden.
Das Unternehmen hat selbst die Kontrolle darüber, welche personenbezogenen Daten im Service gespeichert werden. Die genauen Daten, die das Unternehmen im Service speichern möchte, sind ThinkOwl nicht bekannt und werden zudem verschlüsselt gespeichert. ThinkOwl hat keine Informationen darüber:

a) welche Art von Service-Daten im Service gespeichert sind
b) welche Art von personenbezogenen Daten die Servicedaten enthalten
c) ob sensible Daten verarbeitet werden

Dauer der Verarbeitung

Die Dauer der Verarbeitung der personenbezogenen Daten des Unternehmens entspricht der Laufzeit des Hauptvertrags.

Beglaubigte Übersetzung aus dem Englischen

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

ThinkOwl trifft technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust, die den gesetzlichen Anforderungen an Datenschutz und Datensicherheit entsprechen. Hierbei handelt es sich um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Insbesondere gestaltet ThinkOwl seine innerbetriebliche Organisation so, dass diese den besonderen Anforderungen des Datenschutzes gerecht wird. Diese werden im Folgenden näher beschrieben. Wesentliche Vorleistungen werden von Rechenzentrumsbetreibern (Unterauftragnehmern) erbracht. Die genannten Anbieter haben hierfür jeweils ThinkOwl vertraglich zugesichert, ihrerseits entsprechende technische und organisatorische Maßnahmen zum Datenschutz über die Laufzeit des Vertrages aufrecht zu erhalten.

Die nachfolgend dargestellten Maßnahmen werden insbesondere aus Sicherheitsgründen, das heißt zur Minimierung von Sicherheitsrisiken bezüglich des Zugriffs auf Unternehmensdaten und entsprechender Wahrung von Betriebs- und Geschäftsgeheimnissen, nicht im Detail offengelegt, sondern dienen lediglich als grundsätzliche Maßgabe, um den Anforderungen von Artikel 32 DS-GVO zu genügen.

Beglaubigte Übersetzung aus dem Englischen

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a) Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation berechtigter Personen:

Technische Maßnahmen	**Organisatorische Maßnahmen**
Alarmanlage	Schlüsselverwaltung / Dokumentation der Schlüsselvergabe
Biometrische Zutrittskontrolle zum Gebäude, den Büroetagen und separat geschützten Büroräumen	Protokollierung der Besucher
Absicherung der Gebäudeschächte	Besucher in Begleitung durch Mitarbeitende
Klingelanlage mit Kamera	Sorgfalt bei der Auswahl von Dienstleistern und Partnern (Supplier Security Directive)
Sicherheitsverglasung	
Gesicherter Serverraum mit verstärkter Türe und separierter *biometrischer Zutrittsberechtigung* bzw. Schließanlage	
Bewegungsmelder	

Der selbständige Zutritt zum Gebäude ist (auch außerhalb der üblichen Geschäftszeiten, jedoch nicht zur nächtlichen Sperrfrist) nur mit biometrischem Deaktivieren der Alarmanlage und Zugang (Fingerabdruck) mit entsprechender Berechtigung möglich.

Innerhalb der einzelnen Sicherheitsbereiche sind je nach Sicherheitsstufe zusätzliche Fingerabdruckscanner vorhanden.

Während der üblichen Geschäftszeiten werden Besucher durch den Besuchten in Besucherlisten erfasst sowie eine entsprechende Geheimhaltungsvereinbarung durch Unterschrift des Besuchers schriftlich akzeptiert.

Beglaubigte Übersetzung aus dem Englischen

b) Zugangskontrolle

Das Eindringen Unbefugter in die Datenverarbeitungssysteme ist zu verhindern.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Login mit Benutzername + Passwort	Erstellung und Verwaltung von Benutzerprofilen
Anti-Viren-Software Server	Erstellung und Verwaltung von Benutzerberechtigungen
Anti-Viren-Software Clients	User Passwort Management
Firewall	Richtlinie „Sicheres Passwort“
Einsatz von VPN bei Remote-Zugriffen	Richtlinie „Clean Desk / Clear Screen”
Monitoring bei kritischen IT-Systemen	Richtlinie “Nutzung von E-Mail und Internet“
	Information Security Policy
	Datenschutzrichtlinie

Der Zugang zu Client-Systemen im Netz ist nur über eine passwortgeschützte Netzwerk-Authentifizierung möglich. Der direkte Zugang von Extern (d.h. von außerhalb des Netzwerks) ist ausschließlich über gesicherte und verschlüsselte Verbindungen sowie einem vom Unternehmen bereitgestellten Rechner/Laptop (o.ä. Hardware) möglich. Für den sicheren Zugang auf Drittsysteme werden Firewalls und Proxyserver eingesetzt.

c) Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Benutzerkennung + Passwort	Berechtigungskonzepte
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	Verwaltung der Benutzerrechte durch Administratoren
Aktenschredder (mindestens Stufe 3, cross cut)	Regelmäßige Review von Zugriffsrechten

Beglaubigte Übersetzung aus dem Englischen

Externe Aktenvernichtung	Mitarbeiter-Onboarding/Offboarding-Prozesse
	Richtlinie zur Zugangsbeschränkung
	Richtlinie zu lokalen Administratorrechten

Es liegt ein Berechtigungskonzept mit einer entsprechenden Definition von Nutzerprofilen und Rollen hinsichtlich aller IT-Systeme zugrunde. Berechtigungen werden nach dem „least-privileged" Prinzip vergeben. Anwender erhalten also nur die Berechtigungen im jeweiligen IT-System, die sie für die Umsetzung ihrer Aufgaben benötigen. Der Zugang erfolgt immer über einen Benutzer-Account mit Benutzerkennung und Passwort. Die Protokollierung der Zugriffe erfolgt über einen Log-Eintrag auf den entsprechenden Servern.

d) Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Mandantenfähigkeit relevanter Anwendungen	Funktionstrennung
Getrennte Ordnerstrukturen (Auftragsverarbeitung)	Steuerung über Berechtigungskonzept
	Festlegung von Datenbankrechten

Alle Mitarbeitenden sind angewiesen und geschult, personenbezogene Daten nur im Rahmen der Dienstleistungserbringung und unter Wahrung der Zweckbindung zu erheben, zu verarbeiten oder zu nutzen.

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

a) Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der

Beglaubigte Übersetzung aus dem Englischen

elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Tunnelverbindung (VPN)	Richtlinie zur Informationssicherheit
Hybrides Verschlüsselungsprotokoll TLS	Verschlossene Behälter
Firewall	
Protokollierung der Zugriffe und Abrufe	

Eine Weitergabe personenbezogener Daten aus IT-Systemen findet grundsätzlich nicht statt. Sofern nach Maßgabe einer entsprechenden Rechts- oder Vertragsgrundlage eine Weitergabe zulässig ist, kann diese an verbundene Unternehmen, Kunden, Partner oder Lieferanten erfolgen. Die Weitergabe von Daten ist durch einen Abschluss von Vertraulichkeitsvereinbarungen und Auftragsverarbeitungsvereinbarungen mit dem jeweiligen Dritten abzusichern.

b) Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Beglaubigte Übersetzung aus dem Englischen

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a) Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Feuer- und Rauchmeldeanlagen	Notfallplan
Feuerlöscher	Backup-Verfahren
klimatisierter Serverraum	Recovery-Verfahren
USV	
Firewall und Antivirenprogramme	
Regelmäßige Backups	

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Folgende Maßnahmen gewährleisten, dass die Einhaltung der Anforderungen der DS-GVO bezüglich des Schutzes personenbezogener Daten fortlaufend überprüft, bewertet und evaluiert wird.

a) Datenschutz-Management

Technische Maßnahmen	**Organisatorische Maßnahmen**
Software-Lösungen für Datenschutz-Management im Einsatz	Datenschutzbeauftragter
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeitende nach Bedarf / Berechtigung	Regelmäßige Fortbildung des Datenschutzbeauftragten
	Schulung der Mitarbeitenden und Verpflichtung auf Vertraulichkeit/Datengeheimnis
	Regelmäßige Sensibilisierung der Mitarbeitenden

Beglaubigte Übersetzung aus dem Englischen

	Durchführung der Datenschutz-Folgenabschätzung bei Bedarf
	Informationspflichten nach Art. 13 und 14 DS-GVO wird nachgekommen
	Beschäftigte werden auf die Einhaltung der datenschutzrechtlichen Anforderungen nach DS-GVO verpflichtet

b) Incident-Response-Management

Technische Maßnahmen	**Organisatorische Maßnahmen**
Einsatz von Firewall und regelmäßige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen
Einsatz von Spamfiltern und regelmäßige Aktualisierung	Einbindung des Datenschutzbeauftragten bei Sicherheitsvorfällen und Datenpannen
Einsatz von Virenscannern und regelmäßige Aktualisierung	Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Technische Maßnahmen	**Organisatorische Maßnahmen**
Es werden nur die für den jeweiligen Zweck erforderlichen personenbezogenen Daten erhoben	
Einfache Ausübung des Widerrufsrechts der betroffenen Person durch technische Maßnahmen	

Beglaubigte Übersetzung aus dem Englischen

d) Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Technische Maßnahmen	**Organisatorische Maßnahmen**
	Richtlinie zur Lieferantensicherheit
	Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	Sorgfältige Auswahl des Auftragnehmers insbesondere in Bezug auf Datenschutz und Datensicherheit
	Abschluss notwendiger Vereinbarungen zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
	Verpflichtung der Mitarbeitenden des Auftragnehmers auf das Datengeheimnis
	Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Bestellpflicht
	Regelung zum Einsatz weiterer Subunternehmer
	Sicherstellung der Vernichtung oder Rückgabe von Daten nach Auftragsbeendigung

Beglaubigte Übersetzung aus dem Englischen

ANHANG IV – Liste der Unterauftragnehmer

Unterauftragnehmer	Zweck	Datenspeicherung
Oracle Deutschland B.V. & Co. KG Riesstraße 25, 80992 München Deutschland	Oracle Cloud-Infrastruktur für ThinkOwl Europe Anwendungsoperationen	DE
ITyX Labs GmbH Carl-Benz-Straße 10-12, 56218 Mülheim-Kärlich Germany	Software-Support	DE
fileee GmbH Windthorstraße 68, 48143 Münster, Deutschland	Möglichkeit für ThinkOwl Kunden CONVERSATIONS zu nutzen.	DE
Amazon Web Services Inc. 38 avenue John F. Kennedy, L-1855 Luxemburg	Primärer Cloud-Infrastruktur-Anbieter für die Datenspeicherung von ThinkOwl Europe, wo alle Inhalte von Prozessen (z. B. E-Mail-Inhalte einschließlich Anhängen) gespeichert werden. Speicherort für verschlüsselte Backups.	DE
Amazon Web Services Inc. 38 avenue John F. Kennedy, L-1855 Luxemburg	AWS SES (Einfacher E-Mail-Service): Temporärer Speicher für den Empfang und Versand von E-Mails über die ThinkOwl E-Mail Adresse, bis die E-Mails abgeholt werden.	EU

Beglaubigte Übersetzung aus dem Englischen

OpenAI Ireland Limited The Liffey Trust Centre *117-126 Sheriff Street* Uppe Dublin 1 D01 YC43 Irland	Als Option oder auch als Standard für viele KI-Features wie Konversations-Bot, Zusammenfassung, Übersetzung, TTS, STT, etc.)	EU
Bird Trompenburgstraat 2c, Amsterdam, Niederlande	Möglichkeit für ThinkOwl Nutzer, den SMS-Service zu nutzen	EU
OwlSpot Carl-Benz-Straße 10-12, 56218 Mülheim-Kärlich, Deutschland	App-Store + Integrationen	DE
Microsoft Ireland Operations ltd. One Microsoft Place South County Business Park Leopardstown *Dublin 18* D18P521 Irland	Microsoft Voice API mit LLM Bereitstellung von Sprachverarbeitungsdiensten (Speech-to-Speech, Speech-to-Text, Text-to-Speech)	EU
Google Cloud EMEA ltd. 70 Sir John Rogerson´s Quay Dublin 2 Irland	Gemini Flash und Pro LLM für die Verarbeitung von Sprache, Text, Bildern und Videos im Kontext generativer KI-Anwendungen	EU

Die Richtigkeit und Vollständigkeit der Übersetzung wird beglaubigt. Der in englischer Sprache abgefasste Ursprungstext hat als Kopie in nicht beglaubigter Form vorgelegen.

Hünfelden, 20.08.2025