Auftragsverarbeitungsvertrag

gem. Art. 28 DSGVO

zwischen

_____

_____

_____

(im Folgenden: Verantwortlicher)

und

No Isolation GmbH
Innere Wiener Str. 11
81667 München

(im Folgenden: Auftragsverarbeiter)

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 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.

Klausel 5

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.

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

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 Tage 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.

c) Um die Stabilität und Sicherheit seiner Infrastruktur zu erhöhen, kann der Auftragsverarbeiter Dienste eines Unternehmens (bzw. seiner Muttergesellschaft) in Anspruch nehmen, das in den USA ansässig ist. Dies kann zu einer Übermittlung personenbezogener Daten in die USA führen. Diese Übermittlung beruht auf dem Angemessenheitsbeschluss der Europäischen Kommission (Art. 45 (1) GDPR), da der Dienstleister unter dem EU-US Data Privacy Framework (DPF) registriert ist. Auch für den Fall, dass dieser Beschluss geändert oder widerrufen wird, ist die Übermittlung durch vertragliche, technische und organisatorische Maßnahmen gemäß Art. 44 ff. gesichert und legitimiert. 44 ff. GDPR, wie in Ziffer 7.8 b) beschrieben.

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

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

Name: …

Anschrift: …

Name, Funktion und Kontaktdaten der Kontaktperson: …

Unterschrift und Beitrittsdatum: _____

Auftragsverarbeiter:

No Isolation GmbH
Innere Wiener Str. 11
81667 München
vertreten durch den Geschäftsführer Morten Jørgensen
Telefon: +49 89 3803 4115
E-Mail: contact@noisolation.com

Datenschutzbeauftragter des Auftragsverarbeiters:
Manfred Mainka
msecure GmbH
Bajuwarenring 21
82041 Oberhaching
E-Mail: privacy@noisolation.com

Unterschrift und Beitrittsdatum: _____

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Der AV1-Telepräsenzroboter ist ein Werkzeug, das die Integration von Schülern erleichtert, die über einen längeren Zeitraum nicht am Unterricht teilnehmen können. Die Lösung AV1 ist so konzipiert, dass der Schüler das Geschehen im Unterricht von zu Hause aus verfolgen kann. Gleichzeitig soll er es den Mitschülern und Lehrern im Klassenzimmer ermöglichen, die Signale und Beiträge des Schülers wahrzunehmen.

Einzelheiten zu Art und Umfang der Verarbeitung personenbezogener Daten ergeben sich aus den vertraglichen Verpflichtungen, die in der/den Hauptdienstvereinbarung(en) zwischen den Parteien festgelegt sind.

Grundsätzlich ist die Verarbeitung von besonderen Kategorien personenbezogener Daten im Sinne von Artikel 9 Verordnung (EU) 2016/679 (im Folgenden "DSGVO") nicht Bestandteil der vertraglichen Hauptvereinbarungen.

Soweit besondere Kategorien von Daten im Einzelfall verarbeitet werden (z.B. im Rahmen der Übermittlung von Video- und Audioinhalten), ist durch geeignete technische und organisatorische Maßnahmen sichergestellt, dass insbesondere den Anforderungen der Grundsätze der Datenminimierung und der Einhaltung des Grundsatzes der Vertraulichkeit angemessen Rechnung getragen wird.

Die Dauer der Verarbeitung (Ziffer 7.3) richtet sich nach der Laufzeit der jeweiligen Hauptleistungsverträge zwischen den Parteien.

Je nach den darin vereinbarten Vertragsbestandteilen werden personenbezogene Daten grundsätzlich nach Maßgabe der folgenden Bestimmungen verarbeitet:

1. Servicemodul "Bereitstellung von AV1 und AV1-Assistant App" (Infrastruktur)

   Der Zweck der Verarbeitung ist die Erbringung vertraglich vereinbarter Dienstleistungen, insbesondere:

   - Ermöglichung des Einsatzes und der Nutzung von AV1-Robotern zum Zwecke des Live-Video-Streamings
   - die Verwaltung und das Management der entsprechenden Dienste, einschließlich des Onboarding von Kunden
   - Erstellung und Verwaltung von Kundenkonten und Authentifizierung der Kundenbenutzer
   - Verwaltung des AV1-Bestands (z. B. Generierung von Schlüsselwörtern für neue Nutzer; Erstellung einer AV1-Bestandsliste)
   - Versorgung der Kunden mit statistischen und anderen Informationen über die Nutzung der Dienste
   - Nachverfolgung, wann ein AV1 aktiviert ist; Nachverfolgung der Nutzung der AV1-App nach der Aktivierung
   - Implementierung von Sicherheitsmaßnahmen und Problemlösung

   Die Kategorien der in diesem Modul verarbeiteten personenbezogenen Daten sind:

- Kontaktdaten (Titel, Name, Adresse, Funktion, etc.)
- Zugangsdaten (E-Mail-Adresse, Anmeldedaten)
- IT-Verkehrs- und Nutzungsdaten (IP-Adresse, Datum und Uhrzeit des Zugriffs etc.)
- andere personenbezogene Daten, die der für die Verarbeitung Verantwortliche je nach Auftrag zur Verfügung stellt

Deklaratorischer Hinweis:
Zusätzlich werden gegebenenfalls, sofern die Funktion nicht auf explizite Weisung der verantwortlichen Stelle deaktiviert wurde, folgende pseudonymisierte – aus Sicht des Auftragsverarbeiters anonymisierte - Daten verarbeitet:

- Grund für die Nutzung des AV1 (Angabe in kategorisierter Form):

  Körperliche Erkrankung oder Verletzung, psychische Gesundheitszustände, frühzeitige Intervention zur Verhinderung von Schulverweigerung, sonderpädagogischer Förderbedarf, Verhaltensunterstützung und vorübergehender Ausschluss vom Unterricht, besondere Lebenssituationen, Behinderung, Hochbegabtenförderung, alternative Bildungsprogramme, sonstige Gründe)

- Geschlecht der nutzenden Person

  Diese Daten werden dem Auftragsverarbeiter von der verantwortlichen Stelle über die technische Infrastruktur in einer für den Auftragsverarbeiter anonymisierten Form bereitgestellt und dienen dazu, der verantwortlichen Stelle statistische Auswertungen zur Nutzung der eingesetzten AV1-Avatare bereitzustellen.

Ein Rückschluss auf natürliche Personen und damit eine Personenbeziehbarkeit durch den Auftragsverarbeiter ist ausgeschlossen. Insoweit findet für diese Daten keine Auftragsverarbeitung statt.
Die Überprüfung der Rechtmäßigkeit der Verarbeitung zur Anonymisierung (vor Übermittlung der genannten Daten) obliegt allein der verantwortlichen Stelle.

Kategorien betroffener Personen in diesem Modul:
Personenbezogene Daten werden vom "Kundennutzer" (d. h. Mitarbeiter der Bildungseinrichtung, die zur Nutzung des Dienstes berechtigt sind) und "Endnutzer" (d. h. Schüler, die die AV1-App nutzen oder deren Erziehungsberechtigten) erhoben.

2. Servicemodul "Technische Unterstützung"

   Der Zweck der Verarbeitung besteht in der Erbringung vertraglich vereinbarter

Dienstleistungen, insbesondere in der Erbringung technischer Unterstützungsleistungen für Kunden und Endnutzer (einschließlich Untersuchung von Support-Problemen und Fehlerbehebung)

Die in diesem Modul verarbeiteten Kategorien personenbezogener Daten sind:
- Kommunikationsdaten (z. B. Name, E-Mail-Adresse, Telefon)
- Inhaltsdaten der Kommunikation, die im Einzelfall personenbezogene Daten enthalten können
- Metadaten (Länge und Qualität der Videoübertragung, Datum und Uhrzeit, Funknetzinformationen, Verbindungsstärke, Mobilfunknetzinformationen)
- IT-Verkehrs- und Nutzungsdaten

Kategorien von betroffenen Personen in diesen Bereichen sind insbesondere:
- Mitarbeiter des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters
- Vertragspartner, Kunden und Interessenten des für die Datenverarbeitung Verantwortlichen
- Kundennutzer, Endnutzer

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

Einhaltung der Sicherheitsanforderungen an die Datenverarbeitung gemäß Art. 32 DSGVO Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit

1. **Pseudonymisierung, Anonymisierung und Verschlüsselung von personenbezogenen Daten**

- Pseudonymisierung

Der Endnutzer erhält eine pseudonymisierte Benutzerkennung durch den Verantwortlichen. Der Auftragsverarbeiter erhält grundsätzlich keine Kenntnis von der Identität des Nutzers.

- Verschlüsselung

Daten im Transit werden verschlüsselt (Transportverschlüsselung).

Daten im Ruhezustand werden verschlüsselt.

Die Verschlüsselung wird mit TLS 1.2 und AES256-bit realisiert.

- Anonymisierung

Alle Metadaten werden anonymisiert, wenn es kein aktives Abonnement für AV1 mehr gibt.

2. **Vertraulichkeit der Verarbeitungssysteme und -dienste**

- Physische Zugangskontrolle (Zutrittskontrolle)

Alle Räumlichkeiten an sämtlichen No Isolation-Standorten sind mit Einbruchmeldeanlagen und Videoüberwachung an den Ein- und Ausgängen ausgestattet, die von den jeweiligen Vermietern verwaltet und gewartet werden.

Es werden Maßnahmen ergriffen, um zu verhindern, dass Unbefugte Zugang zu den Räumlichkeiten erhalten, in denen sich die Systeme befinden.

Das Personal von No Isolation ist in den Verfahren zum sicheren Ver- und Aufschließen der Räumlichkeiten geschult.

Das Personal von No Isolation muss für den Zugang zu den Räumlichkeiten individuelle PIN-geschützte Schlüsselkarten oder herkömmliche physische Schlüssel (je nach Standort) verwenden. Die berechtigten Mitarbeiter und die jeweils zugeordneten Schlüssel(-karten) werden in einem zentralen Schlüsselbuch dokumentiert, das vom Büroleiter in Norwegen geführt wird. Die Vergabe der Berechtigungen zur Nutzung von Schlüssel(-karten) in Deutschland und im Vereinigten Königreich wird von den dortigen Direktoren/Geschäftsführern verwaltet. Besucher in den Räumlichkeiten müssen jederzeit von No Isolation-Personal begleitet werden.

- System- und Datenzugangskontrolle (Zugangs- und Zugriffskontrolle)

Nur befugte Personen haben Zugang zu Systemen, in denen personenbezogene Daten und Metadaten gespeichert sind. Der Zugang zu den Systemen wird ausschließlich nach dem „Need-to-know“ Prinzip gewährt, überwacht und protokolliert.

Die internen und kundeneigenen Verwaltungssysteme von No Isolation verwenden rollenbasierte Zugangskontrollen, die die Fähigkeit zur Änderung oder Löschung von Daten auf bestimmte Kundenorganisationen und autorisierte Benutzergruppen beschränken.

Der Zugang zu Systemen und Cloud-basierten Konten basiert auf einer zugewiesenen Benutzer-ID und einer Zwei-Faktor-Authentifizierung.

Der Zugriff auf die Infrastruktur von No Isolation unterliegt Sicherheitsregeln und -vorschriften, die nur Datenverkehr von autorisierten Quellen zulassen. Der Zugang zu den Ressourcen der Infrastruktur ist auf No Isolation-Administratoren (Betriebspersonal) beschränkt, die den Zugang benötigen, um Wartungsarbeiten an den Systemen durchzuführen.

3. Integrität der Verarbeitungssysteme und Dienste

- Ereignisprotokollierung (z. B. bei Authentifizierung oder CRUD-Aktionen - Erstellen, Lesen, Aktualisieren, Löschen von Daten)

- Eingabekontrolle (Überprüfung, zu welchem Zeitpunkt und von wem personenbezogene Daten eingegeben, geändert oder gelöscht wurden)

Die Systeme sind nur für eine minimale Anzahl von Endpoints geöffnet, die für die Bereitstellung von Diensten erforderlich sind. Die offenen Endpunkte unterstützen nur HTTPS und alle Clients müssen sich gegenüber dem System authentifizieren, bevor die Endpunkte genutzt werden können. Es werden Maßnahmen ergriffen, um zu überprüfen, wer personenbezogene Daten in die Systeme eingegeben, geändert oder entfernt hat.

Datenbank- und Datenspeichersysteme werden durch kontinuierliche Anwendung von Wartungsmaßnahmen, Empfehlungen und Best Practices der Anbieter gewartet; alle Verfahren, mit denen personenbezogene Daten eingegeben, gespeichert und bearbeitet werden, sind mit eingebauten Integritäts- und Sicherheitsvorkehrungen konzipiert. Alle diese Verfahren werden vor ihrer Einführung gründlich getestet und von Fachleuten begutachtet.

- Übertragungs- und Weiterleitungskontrolle
  (Überprüfung, an welche Stellen personenbezogene Daten übermittelt werden)

Alle Datenübertragungen über das Internet im Zusammenhang mit AV1 sind mindestens nach dem Standard TLS 1.2 verschlüsselt und decken die für die Dienste erforderlichen Übertragungen ab. Alle Signale werden mit starken Schlüsseln verschlüsselt und verwenden das HTTPS-Protokoll.

Datenbanken/Server haben verschlüsselte Festplatten/Backups/Kommunikation. Der gesamte Medienverkehr (d. h. Audio- und Videostreams) verwendet SRTP (mit DTLS für den Schlüsselaustausch) oder DTLS. Die Kommunikation wird Ende-zu-Ende mit diesen Schlüsseln unter Verwendung von SRTP verschlüsselt, unabhängig davon, ob die Kommunikation direkt zwischen dem AV1 und den Anwendungen oder über ein Relais erfolgt.)

Die für den Verbindungsaufbau erforderlichen Metadaten (einschließlich IP-Adresse, Endpunktkennungen und Verschlüsselungsschlüssel) werden mit TLS verschlüsselt zwischen AV1 und den Servern von No Isolation übertragen. Für den Aufbau des Audio- und Videostroms wird der WebRTC-Standard verwendet, und die WebRTC-Signale (d. h. die Metadaten) werden (TLS-verschlüsselt) über die No Isolation-Server übertragen.

4. **Verfügbarkeit von Verarbeitungssystemen und -diensten sowie die Fähigkeit zur Wiederherstellung der Verfügbarkeit und des Datenzugriffs nach einem physischen oder technischen Zwischenfall**

- Wiederherstellbarkeit (Wiederherstellung/Backup)

No Isolation nutzt Cloud-Dienste, um sicherzustellen, dass Daten und Dienste im Bedarfsfall verfügbar sind. Der Anbieter erstellt alle 24 Stunden Backups von kritischen Systemen. Die Backups werden in der Cloud gespeichert, damit die Systeme bei Bedarf an einem anderen Ort schnell wiederhergestellt werden können (z. B. bei Schäden wie Feuer oder Stromausfällen).

No Isolation unterhält einen Geschäftskontinuitätsplan ("BC-Plan"), der Verfahren zum Schutz vor Unterbrechungen durch unerwartete Ereignisse vorsieht und Meldewege, Notfallkontakte, die Bildung von Reaktionsteams und Notfallpläne für kritische Systeme umfasst. Der BC-Plan wird jährlich getestet, wobei die Ergebnisse und Verbesserungen im Rahmen des Informationssicherheitsmanagementsystems von No Isolation verwaltet werden.

Software und Konfigurationsinformationen zu den Systemen und intern entwickelten und verwalteten Anwendungsdiensten werden in einem gesicherten Quellcode-Repository verwaltet. No Isolation kann Anwendungsdienste bei Bedarf schnell wiederherstellen oder neu bereitstellen. Dazu gehört auch die Möglichkeit, die Dienste bei Bedarf an einen anderen Standort zu verlagern.

- Zuverlässigkeitskontrolle (Meldung von Fehlfunktionen, Ausfällen und Bedrohungen)

Vernetzte Systeme sind durch Firewalls, Endpoint-Protection-Dienste, Überwachungs- und Verwaltungstools gegen unbefugtes Eindringen gesichert.

Die Infrastruktur von No Isolation protokolliert Informationen über das Systemverhalten, den empfangenen Datenverkehr, die Systemauthentifizierung und andere Anwendungsanforderungen. Interne Systeme warnen die zuständigen Mitarbeiter vor böswilligen, unbeabsichtigten oder untypischen Aktivitäten. Das

Personal von No Isolation, einschließlich des Sicherheits-, Betriebs- und Support-Personals, ist geschult, um auf erkannte Sicherheitsvorfälle zu reagieren.

Über erkannte Sicherheitsvorfälle werden Aufzeichnungen geführt. Verdächtige und bestätigte Sicherheitsvorfälle werden untersucht und die entsprechenden Lösungsschritte werden dokumentiert. Bei bestätigten Sicherheitsvorfällen wird eine Nachuntersuchung durchgeführt und es werden geeignete Maßnahmen ergriffen, um das Risiko eines Schadens oder einer unbefugten Offenlegung zu minimieren.

Der Supplier überwacht seine Systeme kontinuierlich und benachrichtigt das Betriebspersonal direkt, wenn ein System ausfällt. Es werden Überwachungsanwendungen eingesetzt und konfiguriert, um die Systemkapazität zu überwachen und das Betriebspersonal zu benachrichtigen, wenn vordefinierte Schwellenwerte erreicht werden.

- Verfügbarkeit (redundante Systeme und Infrastruktur)

Der Anbieter der Cloud-Infrastruktur von No Isolation und die SaaS-Provider (die mit wirtschaftlich vertretbarem Aufwand für Betriebszeit, redundante Strom-, Netzwerk- und HVAC-Dienste sorgen) setzen Routinen für Business Continuity, Disaster Recovery und Incident Response ein.

ISO 27001-Richtlinien, z. B. für Schwachstellenmanagement, Backup, Risikomanagement, Patch-Management, gewährleisten einen gemanagten Ansatz für die Erreichung der Informationssicherheitsziele. Die Infrastruktur wird von AWS bereitgestellt, mit getrennten Umgebungen für Entwurf/Test (Staging) und Produktion. Die Verfügbarkeit wird ständig überwacht.

5. Verarbeitung personenbezogener Daten nur auf dokumentierte Weisung des für die Verarbeitung Verantwortlichen und getrennt für die jeweiligen Zwecke

- Auftragskontrolle (personenbezogene Daten werden nur gemäß den Anweisungen des Auftraggebers verarbeitet)

No Isolation hat mit seinem Personal (einschließlich Angestellten, Beratern und Leiharbeitern) Verträge geschlossen, die Vertraulichkeitsverpflichtungen enthalten. Die Vertraulichkeitspflicht besteht auch nach Beendigung des Arbeitsverhältnisses fort, solange die Informationen vertraulich bleiben.

Der Zugang zur Ferndiagnose wird nur nach Zustimmung des Kunden gewährt. Ferndiagnosesitzungen werden protokolliert, und je nach erforderlicher Zugriffsstufe muss das Supportpersonal einen physischen Hardware-Authentifizierungsschlüssel vorlegen, um die Ferndiagnosesitzung zu starten.

No Isolation ist durch einen AV-Vertrag verpflichtet, Daten nur auf dokumentierte Anweisungen hin zu verarbeiten. Das Personal wird entsprechend informiert und geschult. Es wird festgelegt, welche Personen Anweisungen zur Verarbeitung geben und empfangen dürfen.

- Datentrennung (personenbezogene Daten, die für unterschiedliche Zwecke erhoben werden, werden getrennt verarbeitet).

Eine zusätzliche logische Trennung wird innerhalb der Software von No Isolation durch feste und eindeutige Kunden- und Gerätekennungen und sichere temporäre sitzungsbasierte Token, die bei erfolgreich authentifizierten Verbindungen generiert werden, durchgesetzt.

6. Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

No Isolation hat einen Datenschutzbeauftragten (DSB) und einen Informationssicherheitsbeauftragten (ISB) benannt. Ein Information Security Management System (ISMS) gem. ISO 27001 ist eingerichtet.

Die Informationen zu den Kontrollen sind durch dokumentierte Konzepte und Richtlinien im Rahmen der ISO 27001-Zertifizierung glaubwürdig nachprüfbar.

Eine Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO wurde durchgeführt und wird regelmäßig überprüft.

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter gem. Klausel 7.7 Buchstabe a genehmigt:

1. Amazon Web Services EMEA SARL
   38, Avenue John F. Kennedy
   1855 Luxembourg
   Luxemburg

   Gegenstand der Beauftragung:
   Cloudbasierte Infrastrukturdienste

   Verarbeitung in: EU (Luxemburg)
   Standort der genutzten Rechenzentren: EU (Deutschland)

   Amazon Web Services EMEA SARL ist eine Tochtergesellschaft von Amazon Web Services, Inc. mit Sitz in den USA.
   Als angemessene Garantien im Sinne der Artikel 44 ff. DSGVO wurde ein Datenverarbeitungsvertrag unter Verwendung der Standardvertragsklauseln (SCCs) der Europäischen Kommission (Stand Juni 2021) abgeschlossen.
   Als ergänzende Maßnahmen wurden datenschutzfreundliche Konfigurationseinstellungen gewählt (Datenminimierung) und geeignete technische Maßnahmen wie z.B. Pseudonymisierung umgesetzt.

2. No Isolation AS
   Pilestredet 28
   0166 Oslo
   Norwegen

   Gegenstand der Beauftragung:
   Kundenservice

   Verarbeitung in: EWR (Norwegen)

3. No Isolation Ltd.
   201 Borough High Street
   London, SE11JA
   Großbritannien

   Gegenstand der Beauftragung: Kundenservice

   Verarbeitung in: UK

   Drittlandsverarbeitung auf Grundlage eines Angemessenheitsbeschlusses der Kommission gem. Art. 45 DSGVO