AUFTRAGSVERARBEITUNGSVEREINBARUNG

Hinweis 1: Alle der nachfolgenden Personenbezeichnungen beziehen sich auf alle Geschlechter und ihre Sprachformen und verstehen sich stets mit dem Zusatz „(w/m/d)“.

Hinweis 2: Die nachfolgende Vertragsurkunde beruht auf einem Muster der EU-Kommission, die exakt diese Vertragsurkunde als rechtmäßig ansieht. Dazu hat die EU-Kommission extra einen Durchführungsbeschluss über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28(7) DS-GVO und Artikel 29(7) der Verordnung (EU) 2018/1725 gefasst. Der Durchführungsbeschluss kann hier eingesehen werden: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021D0915. Er darf nicht mit den Standardvertragsklauseln i.S.v. Artikel 46 DSGVO, die eine Drittlandübermittlung regeln, verwechselt werden.

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 drei 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 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

Verantwortliche(r):

Verantwortliche und Auftragsverarbeiterin sind unabhängig von dieser Auftragsverarbeitungsvereinbarung Vertragsparteien eines schuldrechtlichen Hauptvertrages über die Bereitstellung des Dienstes „Optimind“ (vgl. https://www.optimind.so). Verantwortliche ist das Unternehmen, das diesen Dienst bucht, egal, ob kostenfreie Testversion oder kostenpflichtige Version. Das Beitrittsdatum ist identisch mit dem Datum der ersten Buchung des Dienstes.

Auftragsverarbeiter:

Name: Optimind GmbH

Anschrift: Unionstraße 3, 4020 Linz, Österreich

Name, Funktion und Kontaktdaten der Kontaktperson: Johannes Fladenhofer, Geschäftsführung, erreichbar unter office@optimind.so

Das Beitrittsdatum ist identisch mit dem Datum der ersten Buchung des Dienstes.

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Vorbemerkung

Die Auftragsverarbeiterin stellt ihren unternehmerischen Kunden die SaaS-Plattform „Optimind“ zur Verfügung. Mithilfe dieser Plattform ist es möglich, KI-gestützte A/B-Tests auf Webseiten der Kunden durchzuführen, fortlaufend zu konfigurieren und auszuwerten. Hierfür stellt sie ihren Kunden ein Webportal zur browserbasierten Nutzung in einem ausschließlich für registrierte Nutzer zugänglichen Bereich zur Verfügung, ebenso wie Speicherplatz auf Servern der Unterauftragsverarbeiter (ANHANG IV), die sich in der EU befinden bzw. – im Fall

von Drittlandbezug – auf Grundlage geeigneter Garantien gemäß Kapitel V DSGVO eingesetzt werden. Die Verantwortliche ist Kundin und somit Nutzerin der Plattform.

Dies vorausgeschickt kann die Auftragsverarbeitung wie folgt beschrieben werden:

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- aktuelle und ehemalige Besucher*innen der mit Optimind getesteten Internetseiten der Verantwortlichen (Endkunden der Verantwortlichen)
- Beschäftigte und Nutzer*innen der Verantwortlichen, die das Optimind-Backend bedienen (z. B. zur Verwaltung von A/B-Tests, Anlage von Logins, Auswertung)

Kategorien personenbezogener Daten, die verarbeitet werden

Daten der Beschäftigten/Nutzer*innen der Verantwortlichen (Backend-Nutzung):

- Stammdaten und Login-Daten: Name, E-Mail-Adresse, Passwort (verschlüsselt gespeichert), Rollen-/Berechtigungsangaben
- Nutzungsdaten im Backend: Login-Zeiten, durchgeführte Aktionen, angelegte/bearbeitete A/B-Tests, Auswertungs- und Konfigurationsdaten
- Technische Zugriffsdaten: IP-Adresse, Datum/Uhrzeit des Zugriffs, Browsertyp und -version, Betriebssystem, Gerätetyp

Daten der Besucher*innen der mit Optimind getesteten Internetseiten:

- Pseudonymisierte Identifikatoren: Browser-Fingerprints sowie in localStorage abgelegte IDs zur Wiedererkennung von Besucher*innen über Sessions hinweg, ausschließlich zum Zweck der A/B-Test-Zuordnung
- Gekürzte IP-Adresse (das letzte Oktett der IP-Adresse wird vor der Speicherung entfernt)
- Test- und Variantendaten: Zuordnung zu einer A/B-Testvariante, Interaktionsereignisse innerhalb des getesteten Bereichs (z. B. Klicks, Scrollen, Conversions), Verweildauer
- Technische Kontextdaten: Browsertyp und -version, Betriebssystem, Gerätetyp, Spracheinstellung, Referrer-URL, abgerufene URL/Seite

Hinweis: *Browser-Fingerprints, in localStorage abgelegte IDs und gekürzte IP-Adressen werden – in Übereinstimmung mit der herrschenden Auffassung der Aufsichtsbehörden – sicherheitshalber als personenbezogene bzw. pseudonyme Daten i.S.d. DSGVO behandelt.*

Sensible Daten

Die Verarbeitung sensibler Daten i.S.v. Artikel 9 und 10 DSGVO ist nicht Gegenstand dieser Auftragsverarbeitung.

Art der Verarbeitung

Die Daten werden bei den Beschäftigten/Nutzer*innen der Verantwortlichen über das Optimind-Webportal erhoben und verarbeitet. Die Daten der Besucher*innen der mit Optimind getesteten Internetseiten werden über ein von der Verantwortlichen eingebundenes Skript erhoben, in einer Cloudumgebung der Unterauftragsverarbeiter gespeichert und der

Verantwortlichen zum Abruf, zur Auswertung und zur Steuerung der A/B-Tests bereitgestellt. Bei Weisung und/oder Ende des Hauptvertrages werden die Daten gelöscht oder zurückgegeben (siehe „Dauer der Verarbeitung“).

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

Die Verarbeitung dient der Durchführung KI-gestützter A/B-Tests auf den Internetseiten der Verantwortlichen, einschließlich der Zuteilung von Testvarianten, der Erfassung und Auswertung von Interaktions- und Conversion-Daten sowie der Bereitstellung der zugehörigen Auswertungs- und Steuerungsfunktionen im Backend für die Verantwortliche.

Dauer der Verarbeitung

Die Verarbeitung erfolgt für die Laufzeit des Hauptvertrages. 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 III – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

I

Allgemeine Maßnahmen

Maßnahmen zur dauerhaften Gewährleistung der Sicherheit (Nachhaltigkeitskontrolle)

Datenschutz als Compliance-Ziel

Die Achtung kern- und nebendatenschutzrechtlicher Regelungen ist ein formuliertes Compliance-Ziel der Auftragsverarbeiterin. Die organisatorische Hoheit zur Sicherstellung der Datenschutzkonformität liegt qua Amt bei der Geschäftsleitung.

Revisionsfrequenz 18 Monate

Es wird im Abstand von 18 Monaten anlasslos kontrolliert, ob die hier dokumentierten Maßnahmen noch ergriffen werden (Prüfungspunkt 1) und ob die Maßnahmen noch genügen, um die festgestellten Risiken hinreichend zu minimieren (Prüfungspunkt 2). Es wird dokumentiert, ob die Prüfungspunkte bejaht oder verneint werden. Sollte mindestens einer der beiden Prüfungspunkte zu verneinen sein, werden neue Maßnahmen definiert und umgesetzt. Anlassbezogene Kontrollen sind jederzeit möglich und werden ebenfalls dokumentiert.

Schulungs- und Awareness-Maßnahmen

Die Beschäftigten werden regelmäßig (i.d.R. einmal jährlich) im Bereich Datenschutz geschult und sind vertraglich zur Vertraulichkeit verpflichtet. Inhalt der Schulungen sind insbesondere:

- Grundlagen und Grundbegriffe des Datenschutzrechts (DSGVO, österreichisches DSG), insbesondere die Begriffe „personenbezogene Daten“, „Verarbeitung“, „Einwilligung“, „Rechtsvorschrift“, das Verbot mit Erlaubnisvorbehalt sowie die wichtigsten Rechtsgrundlagen (insb. Art. 6 Abs. 1 lit. b und f DSGVO, Beschäftigtendatenschutz);
- technische und organisatorische Maßnahmen nach Artikel 32 DSGVO sowie Mitwirkungspflichten der Beschäftigten bei deren Umsetzung;
- Belehrung über das Datengeheimnis sowie Pflichten im Umgang mit personenbezogenen Daten der Kunden und deren Endkunden;
- Spezifische Fragen des Datenschutzrechts im Anwendungsbereich der Auftragsverarbeitung.

Ansprechpartner für Datenschutz

Die Auftragsverarbeiterin hat einen internen Ansprechpartner für Datenschutz benannt: Peter Jedinger, erreichbar unter office@optimind.so. Eine förmliche Bestellung als Datenschutzbeauftragter im Sinne von Art. 37 DSGVO liegt nicht vor; nach Einschätzung der Auftragsverarbeiterin sind die Voraussetzungen für eine zwingende Bestellung derzeit nicht gegeben. Die Bestellpflicht wird regelmäßig überprüft.

Organisatorische Maßnahmen, Dokumentation und Rechtmäßigkeit von Weisungen

Die Auftragsverarbeiterin führt ein umfassendes Verzeichnis von Verarbeitungstätigkeiten i.S.v. Artikel 30 Absatz 2 DSGVO mit allen gesetzlichen Pflichtangaben. Kommen Beschäftigte zum Ergebnis, dass eine Weisung gegen die DSGVO verstößt, konsultieren sie den internen Ansprechpartner für Datenschutz, der erforderlichenfalls mit dem Verantwortlichen Kontakt aufnimmt und die Rechtmäßigkeit der Weisung klärt. Die Auftragsverarbeiterin unterstützt den Verantwortlichen bei Datenschutz-Folgenabschätzungen in Erfüllung ihrer Pflichten als Auftragsverarbeiterin; sie erbringt jedoch keine Rechtsberatung. Weisungen des Verantwortlichen werden in Textform dokumentiert.

II

Vertraulichkeit

Maßnahmen der Pseudonymisierung und Anonymisierung

Datenminimierung im Tracking

Bei der Erhebung von Daten der Besucher*innen der getesteten Internetseiten werden IP-Adressen vor der Speicherung um das letzte Oktett gekürzt. Es kommen ausschließlich pseudonyme Identifikatoren (localStorage-IDs, Browser-Fingerprints) zur Test-Zuordnung zum Einsatz.

Technik der Löschung

Daten, die zur Löschung anstehen, werden gelöscht oder anonymisiert.

Maßnahmen der Verschlüsselung

Allgemein
Die auftragsgegenständliche Verarbeitung (Speicherung der Test- und Backend-Daten) findet auf Servern der Unterauftragsverarbeiter (siehe Anhang IV) statt, nicht auf eigenen Servern der Auftragsverarbeiterin.

Daten in Übertragung („in transit“) werden mit Transportverschlüsselung nach aktuellem Stand der Technik (TLS 1.3) geschützt. Alle Schnittstellen und API-Endpunkte unterstützen ausschließlich HTTPS (TLS). Daten im Ruhezustand („at rest“) werden mit branchenüblichen Algorithmen (AES-256) verschlüsselt.

Verschlüsselung bei Microsoft Azure
Der Hauptdienstleister für die Speicherung und Verarbeitung der personenbezogenen Daten ist Microsoft Azure (Region Frankfurt/Deutschland). Microsoft Azure verschlüsselt Daten im Ruhezustand standardmäßig mit AES-256 (Azure Storage Service Encryption, Azure SQL Transparent Data Encryption etc.) und Daten in Übertragung mit TLS. Die Schlüsselverwaltung erfolgt über Azure Key Vault. Ohne die erforderlichen Zugangsschlüssel sind gespeicherte Daten für Dritte nicht im Klartext zugänglich.

Verschlüsselung bei Google (Google Workspace)
Soweit Google Workspace zum Einsatz kommt (interne Kommunikations-, Office- und Speicherwerkzeuge der Auftragsverarbeiterin), verschlüsselt der Anbieter sämtliche Kundendaten im Ruhezustand mit Algorithmen wie AES-128 oder AES-256. Die Verschlüsselung erfolgt automatisch ohne Zutun der Nutzer*innen. Für Daten in Übertragung kommt Transportverschlüsselung nach Industriestandard (HTTPS/TLS) zum Einsatz.

Maßnahmen der Zutrittskontrolle
Innerhalb der Büroräume der Auftragsverarbeiterin befinden sich keine permanenten Server-Hardware-Komponenten. Die auftragsgegenständliche Datenverarbeitung selbst findet bei den Unterauftragsverarbeitern statt. Gleichwohl werden für die Räumlichkeiten der Auftragsverarbeiterin folgende Maßnahmen ergriffen:

Gebäude und Büro, verschlossene Türen
Das Gebäude, in dem sich die Betriebsstätte befindet, sowie die Büroräume sind verschlossen. Der Zutritt ist nur über mechanische Schlüssel oder durch Öffnen von innen durch berechtigte Personen möglich. Es besteht eine physische Zugangskontrolle.

Dienstanweisung, Meldung Zutrittsverletzung
Die Beschäftigten sind per Dienstanweisung verpflichtet, den Verdacht auf meldepflichtige Fälle i.S.d. Artikel 33, 34 DSGVO im Zusammenhang mit Zutrittsverletzungen zu melden. Die gleiche Verpflichtung gilt, wenn nicht nur ein Verdacht, sondern Gewissheit hierüber herrscht.

Maßnahmen der Zugangskontrolle

Dienstanweisung, eingeschränkter Zugang
Die Beschäftigten sind per Dienstanweisung verpflichtet, Dritten – einschließlich Familienangehörigen – keinen oder nur einen unbedingt notwendigen Zugriff auf die Datenverarbeitungsmittel im Betriebseigentum zu gewähren.

Dienstanweisung, Meldung Zugangsverletzung
Die Beschäftigten sind per Dienstanweisung verpflichtet, den Verdacht auf meldepflichtige Fälle i.S.d. Artikel 33, 34 DSGVO im Zusammenhang mit Zugangsverletzungen zu melden. Die gleiche Verpflichtung gilt bei Gewissheit.

Übergreifende technische Maßnahmen
Folgende Maßnahmen werden ergriffen, unabhängig davon, ob die Datenverarbeitung remote oder in Präsenz erfolgt:

- Änderung von Standard- und Leerpasswörtern: Nach Installation neuer Software bzw. Inbetriebnahme neuer Hardware werden Standard- und Leerpasswörter geändert.
- Passwortgeschützte Clients: Alle Clients sind passwortgeschützt.
- Individuelle Passwörter: Alle Berechtigten haben individuelle Passwörter.
- Eingeschränkte Nutzung von Admin-Zugängen: Admin-Zugänge werden nur für Admin-Tätigkeiten genutzt; für Nicht-Admin-Tätigkeiten werden gesonderte Zugänge verwendet.
- Eingeschränkter Gesamtzugriff auf Passwörter: Nur ein eng begrenzter Personenkreis hat einen Gesamtzugriff auf alle Zugangsdaten.
- Betriebssysteme und Web-Browser: Alle verfügbaren Sicherheitspatches und Updates werden zeitnah eingespielt.
- Virenschutz auf allen Clients: Alle Clients verfügen über Virenschutz; es werden automatisierte, regelmäßige Virenprüfungen durchgeführt; Updates werden zeitnah installiert.
- Freigabeerfordernis für neue Software/Hardware: Neue Software bzw. Hardware kann nur installiert bzw. in Betrieb genommen werden, wenn sie zentral freigegeben wurde und das jeweilige Handbuch bekannt ist oder gelesen wurde.

Maßnahmen der Zugriffskontrolle

- Zentrale Rechtevergabe: Die Zugriffsrechte auf personenbezogene Daten werden zentral vergeben.
- Need-to-know-Prinzip: Die Zugriffsrechte werden nach dem Need-to-know-Prinzip vergeben.
- Anpassungen bei Rechtevergabe: Verändern sich die Aufgaben einer berechtigten Person, werden die Zugriffsrechte – soweit erforderlich – nach dem Need-to-know-Prinzip angepasst.
- Entzug der Rechte: Endet die Tätigkeit einer berechtigten Person, werden die Zugriffsrechte umgehend und vollständig entzogen.

Maßnahmen der Weitergabekontrolle

Es wird auf die oben beschriebenen Maßnahmen zur Verschlüsselung Bezug genommen. Eine Weitergabe personenbezogener Daten an Dritte erfolgt ausschließlich an die in Anhang IV genannten Unterauftragsverarbeiter und nur nach Maßgabe dieser Vereinbarung.

Maßnahmen der Eingabekontrolle

Eingaben in den auftragsrelevanten Bereichen, soweit sie überhaupt manuell getätigt werden, werden geloggt. Im Backend werden die wesentlichen Aktionen der berechtigten Nutzer*innen (z. B. Anlage, Änderung und Löschung von A/B-Tests) protokolliert.

Maßnahmen der Auftragskontrolle

Artikel 28 DSGVO

Vor jeder Unterbeauftragung wird geprüft, ob die gesetzlichen Voraussetzungen erfüllt sind, insbesondere, ob eine Vertragsurkunde nach Artikel 28 Absatz 3 DSGVO vorhanden ist und ob das zu beauftragende Unternehmen hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Nur bei positivem Ergebnis erfolgt die Beauftragung. Das Ergebnis wird in jedem Fall protokolliert.

Artikel 44 DSGVO

Für den Fall, dass die Unterbeauftragung eine Übermittlung in ein Drittland i.S.v. Artikel 44 DSGVO mit sich bringt, wird geprüft, ob das zu beauftragende Unternehmen die im 5. Kapitel der DSGVO (Artikel 44 bis 50 DSGVO) niedergelegten Bedingungen einhält und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten aus dem betreffenden Drittland an ein anderes Drittland oder eine internationale Organisation. Nur bei positivem Ergebnis erfolgt die Beauftragung. Das Ergebnis wird in jedem Fall protokolliert.

Artikel 46 DSGVO – Transfer Impact Assessment (TIA)

Für den Fall, dass die Beauftragung eine Übermittlung in ein Drittland i.S.v. Artikel 44 DSGVO mit sich bringt und das zu beauftragende Unternehmen sich gemäß den Standardvertragsklauseln i.S.v. Artikel 46 DSGVO verpflichtet, wird ein Transfer Impact Assessment durchgeführt. Nur bei positivem Ergebnis erfolgt die Beauftragung. Das Ergebnis wird in jedem Fall protokolliert.

Artikel 35 DSGVO

Für den Fall, dass die Beauftragung selbst oder die beauftragte Datenverarbeitung in den Anwendungsbereich des Artikels 35 DSGVO fällt, wird eine Datenschutz-Folgenabschätzung durchgeführt. Nur bei positivem Ergebnis erfolgt die Beauftragung. Das Ergebnis wird in jedem Fall protokolliert.

Nachkontrollen

Die vorgenannten Kontrollen werden in regelmäßigen Abständen anlasslos wiederholt, solange die Beauftragung andauert.

Zuständigkeiten
Für die vorgenannten Maßnahmen gelten folgende Zuständigkeiten:

- Geschäftsleitung der Auftragsverarbeiterin
- Interner Ansprechpartner für Datenschutz
- Soweit nach der AVV erforderlich, auch der Verantwortliche (Auftraggeber)

Maßnahmen der Trennungskontrolle

Logische Mandantentrennung
Die Daten verschiedener Verantwortlicher (Kunden) werden logisch getrennt verarbeitet und gespeichert. Über ein ausdifferenziertes Rollen- und Berechtigungsmodell ist sichergestellt, dass die jeweiligen Nutzer*innen ausschließlich auf die Daten ihres eigenen Mandanten zugreifen können.

III

Verfügbarkeit, Wiederherstellbarkeit, Belastbarkeit

Maßnahmen der Verfügbarkeitskontrolle
Die auftragsgegenständliche Verarbeitung findet auf der Infrastruktur der Unterauftragsverarbeiter statt, primär auf Microsoft Azure (Region Frankfurt/Deutschland).

Verfügbarkeit bei Microsoft Azure
Microsoft Azure betreibt geografisch verteilte Rechenzentren mit redundanten Verfügbarkeitszonen innerhalb einer Region. Jede Verfügbarkeitszone ist als unabhängige Fehlerzone mit eigener Strom-, Kühlungs- und Netzwerkversorgung ausgelegt. Im Fehlerfall verlagern automatisierte Prozesse den Datenverkehr aus dem betroffenen Bereich. Microsoft Azure setzt unterbrechungsfreie Stromversorgungen, redundante Energieleitungen sowie Notstromaggregate ein, um Stromausfälle zu überbrücken. Microsoft ist u. a. nach ISO/IEC 27001 zertifiziert.

Verfügbarkeit bei Google (Google Workspace)
Google ist u. a. nach ISO/IEC 27001 zertifiziert. Die Daten werden in einer geschützten Umgebung von eigenen Servern gespeichert und zwischen mehreren geografisch verteilten Rechenzentren repliziert. Die Stromversorgungssysteme der Rechenzentren sind redundant und mit unterbrechungsfreien Stromversorgungen sowie Notstromaggregaten ausgestattet, um einen kontinuierlichen Betrieb sicherzustellen.

Maßnahmen für die rasche Wiederherstellbarkeit
Es ist ein Notfallkonzept für Vorfälle des Datenverlustes oder der eingeschränkten Verfügbarkeit implementiert. Durch die oben genannten Maßnahmen der Verfügbarkeitskontrolle der eingesetzten Cloud-Anbieter (insb. Replikation, Backups, redundante Infrastruktur) sowie eigene Backup- und Wiederherstellungsprozesse ist eine rasche Wiederherstellbarkeit gewährleistet.

Maßnahmen für die Sicherstellung der Belastbarkeit

Es findet ein durchgehendes Systemmonitoring der eingesetzten Anwendungen und Infrastrukturkomponenten statt.

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Microsoft Azure

Name: Microsoft Österreich GmbH (Vertragspartner für die EU-Cloud-Region: Microsoft Ireland Operations Limited)

Anschrift: Am Euro Platz 3, 1120 Wien, Österreich

Name, Funktion und Kontaktdaten der Kontaktperson: Microsoft Datenschutzteam, erreichbar über https://www.microsoft.com/de-at/concern/privacy

Drittlandstatus: n/a; Verarbeitung erfolgt in der Azure-Region Frankfurt (Deutschland, EU). Es wird nicht verkannt, dass die Microsoft-Konzernmutter ihren Sitz in den USA hat. Microsoft hat jedoch vertraglich zugesichert, die Daten in der gewählten EU-Region zu verarbeiten. Soweit Verwaltungs- oder Supportzugriffe aus Drittländern technisch nicht ausgeschlossen werden können, gelten die zwischen Microsoft und der Auftragsverarbeiterin vereinbarten EU-Standardvertragsklauseln gemäß Artikel 46 DSGVO.

Beschreibung der Verarbeitung: Speicherung und Verarbeitung personenbezogener Daten im Auftrag der Auftragsverarbeiterin (Cloud-Storage, Compute, Datenbank- und Infrastrukturleistungen) als Hauptinfrastruktur des Optimind-Dienstes.

Google Workspace

Name: Google Cloud EMEA Limited

Anschrift: 70 Sir John Rogerson’s Quay, Dublin 2, Irland

Name, Funktion und Kontaktdaten der Kontaktperson: Google Datenschutzteam, erreichbar über https://support.google.com/a/contact/googlecloud_dpr; allgemeine Kontaktstelle: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland.

Drittlandstatus: n/a, da Irland (EU). Es wird nicht verkannt, dass dieser Unterauftragsverarbeiter eine Muttergesellschaft in den USA hat. Soweit Verwaltungszugriffe aus Drittländern technisch nicht ausgeschlossen werden können, gelten die zwischen Google und der Auftragsverarbeiterin vereinbarten EU-Standardvertragsklauseln gemäß Artikel 46 DSGVO. Google ist zudem unter dem EU-U.S. Data Privacy Framework (Art. 45 DSGVO) zertifiziert.

Beschreibung der Verarbeitung: Bereitstellung interner Office-, Kommunikations- und Speicherwerkzeuge der Auftragsverarbeiterin (Gmail, Drive, Docs, Meet u. ä.). Es werden keine produktiv-auftragsgegenständlichen Test- oder Trackingdaten in Google Workspace gespeichert; eine Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen

erfolgt mittelbar nur, soweit etwa Support-Korrespondenz oder Kontaktdaten dort verarbeitet werden.

Stripe

Name: Stripe Payments Europe, Limited

Anschrift: 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Irland

Name, Funktion und Kontaktdaten der Kontaktperson: Datenschutzbeauftragter, dpo@stripe.com; allgemeine Datenschutzanfragen: privacy@stripe.com

Drittlandstatus: n/a, da Irland (EU). Soweit Verwaltungszugriffe aus Drittländern (insb. USA durch die Konzernmutter Stripe, Inc.) technisch nicht ausgeschlossen werden können, gelten die zwischen Stripe und der Auftragsverarbeiterin vereinbarten EU-Standardvertragsklauseln gemäß Artikel 46 DSGVO.

Beschreibung der Verarbeitung: Abwicklung der Zahlungsvorgänge zwischen Auftragsverarbeiterin und Verantwortlichen (Rechnungslegung, Zahlungsabwicklung). Eine Verarbeitung von Daten im Auftrag der Verantwortlichen über die hierzu erforderlichen Stamm- und Zahlungsdaten der Verantwortlichen hinaus findet nicht statt. Stripe agiert hinsichtlich der Zahlungsdaten teilweise als eigener Verantwortlicher; siehe hierzu die Stripe-Datenschutzbestimmungen.

Intercom

Name: Intercom R&D Unlimited Company

Anschrift: 124 St. Stephen’s Green, Dublin 2, Irland

Name, Funktion und Kontaktdaten der Kontaktperson: Datenschutzteam, privacy@intercom.io

Drittlandstatus: n/a, da Irland (EU). Soweit Verwaltungszugriffe aus Drittländern (insb. USA durch die Konzernmutter Intercom, Inc.) technisch nicht ausgeschlossen werden können, gelten die zwischen Intercom und der Auftragsverarbeiterin vereinbarten EU-Standardvertragsklauseln gemäß Artikel 46 DSGVO.

Beschreibung der Verarbeitung: Bereitstellung eines Helpdesk- und In-App-Messaging-Systems für die Kommunikation zwischen der Auftragsverarbeiterin und den Beschäftigten/Nutzer*innen der Verantwortlichen (Support, Onboarding, Produktankündigungen). Verarbeitet werden insb. Stammdaten der Backend-Nutzer*innen sowie Inhalte der ausgetauschten Nachrichten.

Mixpanel

Name: Mixpanel, Inc.

Anschrift: One Front Street, 28th Floor, San Francisco, CA 94111, USA

Name, Funktion und Kontaktdaten der Kontaktperson: Datenschutzteam, privacy@mixpanel.com

Drittlandstatus: USA. Die Übermittlung erfolgt auf Grundlage des EU-U.S. Data Privacy Framework gemäß Artikel 45 DSGVO (Mixpanel, Inc. ist unter dem DPF zertifiziert).

Ergänzend wurden mit Mixpanel die EU-Standardvertragsklauseln gemäß Artikel 46 DSGVO als zusätzliche Garantie vereinbart. Sollte die DPF-Zertifizierung wegfallen, beruht die Übermittlung ausschließlich auf den Standardvertragsklauseln; die Auftragsverarbeiterin führt hierzu ein Transfer Impact Assessment.

Beschreibung der Verarbeitung: Produktanalyse-Dienstleistungen zur Auswertung der Nutzung des Optimind-Backends (Funktionsnutzung, Klick- und Eventdaten der Backend-Nutzer*innen) zur Produktverbesserung.

Sentry

Name: Functional Software, Inc. d/b/a Sentry – EU-Region (sentry.io EU)

Anschrift Vertragspartner: 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA; Datenverarbeitung erfolgt in der EU-Region (Rechenzentren in Frankfurt/Deutschland)

Name, Funktion und Kontaktdaten der Kontaktperson: Datenschutzteam, compliance@sentry.io

Drittlandstatus: Vertragspartner mit Sitz in den USA; die Datenverarbeitung erfolgt jedoch ausschließlich in der EU-Region (Frankfurt/Deutschland) gemäß vertraglicher Zusicherung. Soweit Verwaltungszugriffe aus den USA technisch nicht ausgeschlossen werden können, gelten die zwischen Sentry und der Auftragsverarbeiterin vereinbarten EU-Standardvertragsklauseln gemäß Artikel 46 DSGVO; Sentry ist zudem unter dem EU-U.S. Data Privacy Framework zertifiziert.

Beschreibung der Verarbeitung: Fehler- und Performance-Monitoring der Optimind-Anwendung (Erfassung von Anwendungsfehlern, Stack Traces, Kontextinformationen). Personenbezogene Daten werden nach Möglichkeit gefiltert oder pseudonymisiert; eine Verarbeitung kann sich aber nicht vollständig ausschließen lassen (z. B. IP-Adressen, IDs).

Cloudflare

Name: Cloudflare, Inc.

Anschrift: 101 Townsend Street, San Francisco, CA 94107, USA

Name, Funktion und Kontaktdaten der Kontaktperson: Datenschutzbeauftragter, privacyquestions@cloudflare.com

Drittlandstatus: USA. Die Übermittlung erfolgt auf Grundlage des EU-U.S. Data Privacy Framework gemäß Artikel 45 DSGVO. Ergänzend wurden mit Cloudflare die EU-Standardvertragsklauseln gemäß Artikel 46 DSGVO als zusätzliche Garantie vereinbart.

Beschreibung der Verarbeitung: Erbringung von DNS-Diensten für Optimind-Domains. Im Rahmen von DNS-Anfragen werden technische Verbindungsdaten (insb. IP-Adressen) verarbeitet.

Hinweis zur Aktualisierung: *Diese Liste wird durch die Auftragsverarbeiterin laufend aktualisiert. Änderungen werden dem Verantwortlichen mindestens drei Wochen im Voraus in Textform mitgeteilt (vgl. Klausel 7.7 Buchstabe a).*