Auftragsverarbeitungsvertrag (AVV)

Struktur

Dieser AVV ist wie folgt aufgebaut:

Abschnitt	Inhalt
Abschnitt A - Details der Datenverarbeitung	Die wichtigsten Definitionen und Details der Datenverarbeitung im Rahmen dieser AVV sind in Abschnitt A festgelegt.
Abschnitt B - Geltungsbereich	Enthält die für die Vereinbarung geltenden allgemeinen rechtlichen Bestimmungen.
Abschnitt C – TOMs	Die anwendbaren technischen und organisatorischen Massnahmen.

Abschnitt A - Details der Datenverarbeitung

Verantwortlicher	<Adresse Kunde> Kontakt: <Kontaktperson Kunde> (<Email>)
Auftragsverarbeiter	Moodtalk AG, Reussstrasse 5, 6468 Attinghausen, Schweiz Kontakt: Jonas Purtschert (jonas@moodtalk.ch) (gemeinsam mit dem Verantwortlichen **"die Parteien"**)
Zweck der Verarbeitung	Verarbeitung im Zusammenhang mit <Name Basisvertrag> (der "Basisvertrag")
Dauer der Verarbeitung	So lange wie für den Basisvertrag notwendig
Kategorie von betroffenen Personen	• Freiberufler • Mitarbeiter
Kategorie von Personendaten	• Benutzerdaten (z.B.: IP-Adresse, Logfiles, Geräte ID, Gerätedetails, Metadaten, Datum, Uhrzeit) • Benutzerkontendaten (z.B.: Name, E-Mail, Telefonnummer) • Nutzungs- und Analysedaten • Arbeitsbedingungen, Beanspruchung durch die Arbeit, Einstellung zur Arbeit und stellenbezogene Angaben (z.B. Abteilung)
Ort der Speicherung und Verarbeitung	An der Geschäftsadresse des Auftragsverarbeiters und seiner zugelassenen Unterauftragsverarbeiter, wie in dieser Vereinbarung zur Auftragsverarbeitung angegeben
Vor-Ort-Prüfungen	Nein
Unter-Auftragsverarbeiter	Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland - Zweck: Cloudspeicher, Cloud Infrastruktur, Cloud Datenverarbeitung - Speicherung und Verarbeitung in Datenzentren in der Schweiz und EU Weitere Informationen unter: https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn#how-to-configure-services-for-use-in-the-eu-data-boundary

	Hubspot Ireland Limited, 2nd Floor, 30 North Wall Quay, Dublin 1, Ireland
	- Zweck: CRM tool
	- Bearbeitete Personendaten: Auc
	  ○ E-Mail-Kommunikation mit Kundenbetreuung
	  ○ Teamnamen
	  ○ Teilnahmequoten der Teams
	  ○ Datum der Moodtalks der Teams
	  ○ E-Mail-Adressen der Teamleads
	- Speicherung im AWS-Datenzentrum in Frankfurt
	- Verarbeitung wie im Hubspot-DPA beschrieben: https://legal.hubspot.com/dpa

Die in Abschnitt A definierten Variablen dienen als Definitionen in Abschnitt B.

Abschnitt B - Geltungsbereich

1 Zweck und Anwendungsbereich

a) Zweck dieses Auftragsverarbeitungsvertrags (AVV) ist es, die Einhaltung von Art. 28 Abs. 3 und 4 der EU-Datenschutz-Grundverordnung (DSGVO) und Art. 9 des Schweizerischen Bundesgesetz über den Datenschutz (DSG) zu gewährleisten, und zwar nur in dem Umfang, der auf die jeweilige Verarbeitungstätigkeit anwendbar ist.

b) Dieser AVV gilt für die Verarbeitung von personenbezogenen Daten gemäss Abschnitt A.

2 Auslegung

a) Wo in diesem AVV Begriffe verwendet werden, die in der DSGVO oder dem DSG definiert sind, haben diese Begriffe dieselbe Bedeutung wie in dem betreffenden Gesetz.

b) Dieser AVV ist im Lichte der Bestimmungen der DSGVO oder des DSG zu lesen und auszulegen, soweit diese anwendbar sind.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die im Widerspruch zu den Rechten und Pflichten steht, die in der DSGVO oder dem DSG vorgesehen sind, oder die Grundrechte oder -freiheiten der betroffenen Personen beeinträchtigt.

3 Hierarchie

Im Falle eines Widerspruchs zwischen diesem AVV und den Bestimmungen einer anderen Vereinbarung zwischen den Parteien, die zum Zeitpunkt der Vereinbarung dieses AVV besteht oder danach abgeschlossen wird, hat dieser AVV Vorrang, es sei denn, es wurde ausdrücklich etwas anderes in Textform vereinbart.

4 Beschreibung der Verarbeitung(en)

Die Einzelheiten der Verarbeitungen, insbesondere die Kategorien von personenbezogenen Daten und die Zwecke der Verarbeitung, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Abschnitt A aufgeführt.

5 Verpflichtungen der Vertragsparteien

5.1 Allgemein

a) Der Auftragsverarbeiter verarbeitet personenbezogenen Daten nur auf dokumentierte Weisung des für die Verarbeitung Verantwortlichen, es sei denn, er ist aufgrund von Rechtsvorschriften der EU, der Mitgliedstaaten oder der Schweiz, denen der Auftragsverarbeiter unterliegt, hierzu verpflichtet. Solche Weisungen sind in Abschnitt A aufgeführt. In diesem Fall unterrichtet der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung über diese rechtliche Verpflichtung, es sei denn, das Gesetz verbietet dies aus wichtigen Gründen des öffentlichen Interesses. Der Verantwortliche kann während der gesamten Dauer der Verarbeiter von personenbezogenen Daten auch nachträgliche Weisungen erteilen. Solche Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn die Anweisungen des Verantwortlichen nach Ansicht des Auftragsverarbeiter gegen geltende Datenschutzvorschriften der EU, der Mitgliedstaaten oder der Schweiz verstossen.

5.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Abschnitt A genannten Zweck(e) der Verarbeitung.

5.3 Löschung oder Rückgabe von Daten

a) Die Verarbeitung durch den Auftragsverarbeiter darf nur für die in Abschnitt A angegebene Dauer erfolgen.

b) Bei Beendigung der Erbringung von Dienstleistungen zur Verarbeitung von personenbezogenen Daten oder bei Beendigung gemäss Klausel 8 hat der Auftragsverarbeiter alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten zu löschen und dem Verantwortlichen zu bescheinigen, dass er dies getan hat sowie vorhandene Kopien zu löschen, es sei denn, das Schweizer Recht, das EU-Recht oder das Recht der Mitgliedstaaten schreibt die Aufbewahrung der personenbezogenen Daten vor.

5.4 Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift die in Abschnitt C genannten technischen und organisatorischen Massnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten, einschliesslich des Schutzes vor zufälliger oder unrechtmässiger Zerstörung, Verlust, Veränderung, unbefugter Weitergabe oder unbefugtem Zugriff auf diese Daten (Verletzung des Schutzes von personenbezogenen Daten) gemäss Art. 5, 28 Abs. 3. Bst. c und 32 GDPR sowie Art. 8 DSG.

b) Im Falle einer Verletzung des Schutzes von personenbezogenen Daten in Bezug auf Daten, die vom Auftragsverarbeiter verarbeitet werden, benachrichtigt dieser den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von 48 Stunden, nachdem er von der Verletzung Kenntnis erhalten hat. Diese Benachrichtigung enthält die Angaben zu einer Kontaktstelle, bei der weitere Informationen über die Verletzung des Schutzes von personenbezogenen Daten eingeholt werden können, eine Beschreibung der Art der Verletzung (einschliesslich, soweit möglich, der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze), ihrer wahrscheinlichen Folgen und der Massnahmen, die zur Minderung ihrer möglichen nachteiligen Auswirkungen ergriffen wurden oder ergriffen werden sollen. Ist es nicht möglich, alle Informationen gleichzeitig zur Verfügung zu stellen, so enthält die erste Benachrichtigung die zu diesem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden ohne unangemessene Verzögerung bereitgestellt, sobald sie verfügbar sind.

c) Der Auftragsverarbeiter arbeitet nach Treu und Glauben mit dem Verantwortlichen zusammen und unterstützt ihn in jeder erforderlichen Weise, damit der Verantwortliche gegebenenfalls die zuständige Datenschutzbehörde und die betroffenen Personen benachrichtigen kann, wobei die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt werden.

d) Der Auftragsverarbeiter gewährt seinen Mitarbeitern nur insoweit Zugang zu den Daten, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter stellt sicher, dass die Personen, die zur Verarbeitung der erhaltenen personenbezogenen Daten befugt sind, sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen.

e) Betrifft die Verarbeitung personenbezogenen Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten über Gesundheit oder das Sexualleben oder die sexuelle Ausrichtung einer Person, Daten über Massnahmen der sozialen Hilfe oder Daten über strafrechtliche Verurteilungen und Straftaten (besondere Datenkategorien), so wendet der Auftragsverarbeiter besondere Beschränkungen und/oder zusätzliche Garantien an, die der Verantwortliche angemessenerweise verlangt.

5.5 Dokumentation und Einhaltung der Vorschriften

a) Die Parteien müssen in der Lage sein, die Einhaltung dieses AVV nachzuweisen.

b) Der Auftragsverarbeiter ist verpflichtet, alle angemessenen Anfragen des Verantwortlichen, die sich auf die Verarbeitung im Rahmen dieses Vertrags beziehen, unverzüglich und ordnungsgemäss zu beantworten.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in diesem AVV festgelegten und sich unmittelbar aus der DSGVO oder dem DSG ergebenden Verpflichtungen nachzuweisen, und ermöglicht auf Verlangen des Verantwortlichen die Überprüfung von Dateien und Unterlagen oder von Audits der unter diese Klauseln fallenden Verarbeitungstätigkeiten und trägt dazu bei, insbesondere wenn es Anzeichen für eine Nichteinhaltung gibt.

d) Der Verantwortliche hat die Wahl, das Audit selbst durchzuführen, auf eigene Kosten einen unabhängigen Prüfer zu beauftragen oder sich auf ein vom Auftragsverarbeiter beauftragtes unabhängiges Audit zu verlassen. Beauftragt der Auftragsverarbeiter ein Audit, so hat er die Kosten für den unabhängigen Prüfer zu tragen. Der Auftragsverarbeiter hat die Kosten des Audits jedoch zu tragen, falls das Audit aufgrund von Verschulden des Auftragsverarbeiters oder Verdachts auf Nichteinhaltung der Vereinbarung durchgeführt werden muss. Die Audit-, Zugangs- und Inspektionsrechte des Verantwortlichen gemäss dieser Klausel beschränken sich ausschliesslich auf die Aufzeichnungen des Auftragsverarbeiter (einschliesslich u. a. der Verzeichnisse der Tätigkeiten zur Verarbeitung von personenbezogenen Daten und der Verzeichnisse der Empfänger von personenbezogenen Daten) und gelten nicht für die physischen Räumlichkeiten des Auftragsverarbeiter. Jede Prüfung und jedes Auskunftsersuchen ist auf die Informationen zu beschränken, die für die Zwecke dieses AVV erforderlich sind, und hat den Vertraulichkeitsverpflichtungen des Auftragsverarbeiter und seinem berechtigten Interesse am Schutz von Geschäftsgeheimnissen gebührend Rechnung zu tragen.

e) Der Auftragsverarbeiter und der Verantwortliche stellen die in dieser Klausel genannten Informationen, einschliesslich der Ergebnisse etwaiger Audits, der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung, wenn und soweit dies nach der DSGVO oder dem DSG erforderlich ist.

5.6 Einsatz von Unter-Auftragsverarbeitern

a) Der Auftragsverarbeiter verfügt über die allgemeine Ermächtigung des Verantwortlichen für die Beauftragung von Unter-Auftragsverarbeitern. Die Liste der Unter-Auftragsverarbeiter ist in Abschnitt A zu finden. Der Auftragsverarbeiter unterrichtet den Verantwortlichen in Textform mindestens 30 Tage im Voraus über beabsichtigte Änderungen dieser Liste durch Hinzufügung oder Ersetzung von Unter-Auftragsverarbeitern, so dass der Verantwortliche die Möglichkeit hat, vor der Beauftragung des/der betreffenden Unter-Auftragsverarbeiter(s) Einspruch gegen diese Änderungen einzulegen. Ein solcher Einspruch darf nicht unangemessen erhoben werden. Die Parteien halten die Liste auf dem neuesten Stand.

b) Beauftragt der Auftragsverarbeiter einen Unter-Auftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so erfolgt dies im Rahmen eines Vertrags, der dem Unter-Auftragsverarbeiter dieselben Pflichten auferlegt wie dem

Auftragsverarbeiter gemäss dieses AVV. Der Auftragsverarbeiter stellt sicher, dass der Unter-Auftragsverarbeiter die Verpflichtungen einhält, denen der Auftragsverarbeiter gemäss dieses AVV, Art. 28 Abs. 2 bis 4 DSGVO und Art. 9 Abs. 3 DSG.

c) Der Auftragsverarbeiter legt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Unter-Auftragsverarbeitungsvereinbarung und späterer Änderungen vor.

d) Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen in vollem Umfang für die Erfüllung der Verpflichtungen des Unter-Auftragsverarbeiters aus seinem Vertrag mit dem Auftragsverarbeiter verantwortlich. Der Auftragsverarbeiter meldet dem Verantwortlichen, wenn der Unter-Auftragsverarbeiter seinen Verpflichtungen aus diesem Vertrag nicht nachkommt.

5.7 Internationale Übermittlungen

a) Jegliche Übermittlung von personenbezogenen Daten in ein "Drittland" (jedes Land ausserhalb der EU/des EWR und der Schweiz) oder an eine internationale Organisation durch den Auftragsverarbeiter darf nur erfolgen, wenn sie gemäss Abschnitt A genehmigt wurde, und muss, soweit anwendbar, in Übereinstimmung mit Kapitel V der DSGVO und dem 2. Abschnitt des DSG erfolgen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass, wenn der Auftragsverarbeiter einen Unter-Auftragsverarbeiter gemäss Klausel 5.6 mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in einem Drittland beauftragt und diese Verarbeitungstätigkeiten die Übermittlung von personenbezogenen Daten im Sinne der DSGVO oder des DSG beinhalten, der Auftragsverarbeiter und der Unter-Auftragsverarbeiter Standardvertragsklauseln verwenden können, die von der EU-Kommission auf der Grundlage von Art. 46 Abs. 2 DSGVO angenommen wurden (inkl. den vom EDÖB aus Schweizer Sicht vorgeschlagenen Anpassungen), um die Anforderungen von Kapitel V der DSGVO bzw. des DSG zu erfüllen, sofern die Bedingungen für die Verwendung dieser Klauseln erfüllt sind und eine interne Bewertung zu dem Ergebnis geführt hat, dass eine solche Übermittlung dem Datenschutzniveau der DSGVO oder dem DSG entspricht. Bei Bedarf sind zusätzliche Massnahmen (z.B. Verschlüsselung der Daten) zu treffen.

6 Rechte der betroffenen Person

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über alle direkt von der betroffenen Person gestellten Anträge. Er antwortet nicht selbst auf diese Anfrage, es sei denn, er wurde von dem Verantwortlichen dazu ermächtigt.

b) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Verpflichtungen, auf die Anträge der betroffenen Personen auf Ausübung ihrer Rechte gemäss Kapitel III der DSGVO und dem 4. Kapitel des DSG zu reagieren, und zwar

1) das Recht, informiert zu werden, wenn personenbezogenen Daten von der betroffenen Person erhoben werden,
2) das Recht, informiert zu werden, wenn personenbezogenen Daten nicht von der betroffenen Person erhalten wurden,
3) das Recht auf Auskunft durch die betroffene Person,
4) das Recht auf Berichtigung,
5) das Recht auf Löschung ("das Recht auf Vergessenwerden"),
6) das Recht auf Einschränkung der Verarbeitung,
7) die Meldepflicht zur Berichtigung oder Löschung von personenbezogenen Daten oder zur Einschränkung der Verarbeitung,
8) das Recht auf Datenübertragbarkeit,
9) das Recht, Einspruch zu erheben,
10) das Recht, keiner Entscheidung unterworfen zu werden, die ausschliesslich auf einer automatisierten Verarbeitung, einschliesslich Profiling, beruht,
11) das Recht, die Einwilligung zu widerrufen.

c) Der Auftragsverarbeiter unterstützt den Verantwortlichen, wenn eine betroffene Person bei der zuständigen Aufsichtsbehörde eine Beschwerde eingereicht hat, die Daten betrifft, die auf der Grundlage dieses AVV verarbeitet werden.

d) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Informationspflicht, indem er dem Verantwortlichen eine Datenschutzerklärung zur Verfügung stellt, die vom Verantwortlichen, gemäss der im Rahmen des Basisvertrags erbrachten Dienstleistungen, zu ergänzen ist. Bei Gebrauch der genannten Datenschutzerklärung, wird diese vom Verantwortlichen in seinem eigenen Namen und nicht im Namen des Auftragsverarbeiters herausgeben. Jegliche Gewährleistung und Haftung der Auftragsverarbeiters im Zusammenhang mit dieser Datenschutzerklärung ist ausgeschlossen.

e) Zusätzlich zu der Verpflichtung des Auftragsverarbeiter, den Verantwortlichen gemäss Art. 6 Bst. b zu unterstützen, unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der folgenden Verpflichtungen, wobei die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt werden:

1) Die Verpflichtung, eine Verletzung des Schutzes von personenbezogenen Daten unverzüglich nach Bekanntwerden der zuständigen Aufsichtsbehörde mitzuteilen (es sei denn, die Verletzung des Schutzes von personenbezogenen Daten führt wahrscheinlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen), in Übereinstimmung mit Art. 33 DSGVO und Art. 24 Abs. 1 bis 3 DSG;

2) die Verpflichtung, der betroffenen Person die Verletzung des Schutzes von personenbezogenen Daten unverzüglich mitzuteilen, wenn die Verletzung des Schutzes von personenbezogenen Daten wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt, gemäss Art. 34 DSGVO und Art. 24 Abs. 2 DSG;

3) die Verpflichtung zur Durchführung einer Abschätzung der Folgen der geplanten Verarbeitungen für den Schutz von personenbezogenen Daten (eine "Datenschutz-Folgenabschätzung"), wenn eine Art der Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, gemäss Art. 35 DSGVO und Art. 22 DSG;

4) die Verpflichtung, die zuständige Aufsichtsbehörde vor der Verarbeitung zu konsultieren, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung zu einem hohen Risiko führen würde, wenn der Verantwortliche keine Massnahmen zur Risikominderung ergreift, gemäss Art. 36 DSGVO und Art. 23 DSG.

f) Die Vertragsparteien legen in Abschnitt C die geeigneten technischen und organisatorischen Massnahmen fest, durch die der Auftragsverarbeiter den Verantwortlichen bei der Anwendung dieser Klausel zu unterstützen hat, sowie den Umfang und das Ausmass der erforderlichen Unterstützung.

7 Meldung von Verletzungen des Schutzes von personenbezogenen Daten

a) Im Falle einer Verletzung des Schutzes von personenbezogenen Daten arbeitet der Auftragsverarbeiter nach Treu und Glauben mit dem Verantwortlichen zusammen und unterstützt ihn in jeder Weise, die für den Verantwortlichen erforderlich ist, um seinen Verpflichtungen gemäss Art. 33 und 34 DSGVO und Art. 24 DSG nachzukommen, wobei die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt werden.

b) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Meldung der Verletzung des Schutzes von personenbezogenen Daten an die zuständige Aufsichtsbehörde, sofern zutreffend. Der Auftragsverarbeiter ist verpflichtet, insbesondere bei der Beschaffung der folgenden Informationen behilflich zu sein, die gemäss Art. 33 Abs. 3 DSGVO und Art. 24 Abs. 2 DSG in der Meldung des Verantwortlichen angegeben werden müssen:

1) Die Art der personenbezogenen Daten, einschliesslich, soweit möglich, die Kategorien und die ungefähre Anzahl der betroffenen Personen sowie die Kategorien und die ungefähre Anzahl der betroffenen personenbezogenen Daten;

2) die wahrscheinlichen Folgen der Verletzung des Schutzes von personenbezogenen Daten;

3) die Massnahmen, die der Verantwortliche ergriffen hat oder zu ergreifen gedenkt, um die Verletzung des Schutzes von personenbezogenen Daten zu beheben, gegebenenfalls einschliesslich Massnahmen zur Abschwächung möglicher negativer Auswirkungen.

8 Beendigung

a) Unbeschadet der Bestimmungen der DSGVO oder des DSG kann der Verantwortliche den Auftragsverarbeiter anweisen, die Verarbeitung von personenbezogenen Daten vorübergehend einzustellen, bis dieser diesen AVV einhält oder der Vertrag gekündigt wird, falls der Auftragsverarbeiter gegen seine Verpflichtungen aus diesem AVV verstösst. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, falls er aus irgendeinem Grund nicht in der Lage ist, diesen AVV einzuhalten.

b) Der Verantwortliche ist berechtigt, diesen AVV zu kündigen, wenn:

1) die Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter von dem Verantwortlichen gemäss Buchstabe a vorübergehend ausgesetzt wurde, der Verstoss des Auftragsverarbeiter erheblich ist und die Einhaltung dieses AVV nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats, wiederhergestellt wird;

2) Der Auftragsverarbeiter verstösst in erheblichem Masse oder dauerhaft gegen diesen AVV oder gegen seine Verpflichtungen nach der DSGVO oder dem DSG und es ist nicht zu erwarten, dass dieser Verstoss behoben wird;

3) der Auftragsverarbeiter einer verbindlichen Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde in Bezug auf seine Verpflichtungen aus diesem AVV, der DSGVO oder dem DSG nicht nachkommt.

c) Diese Vereinbarung bleibt in vollem Umfang in Kraft, solange der Basisvertrag in Kraft bleibt. Alle Bestimmungen dieses AVV, die ausdrücklich oder stillschweigend bei oder nach Beendigung des Basisvertrags zum Schutz von personenbezogenen Daten in Kraft treten oder fortbestehen sollen, bleiben in vollem Umfang in Kraft.

9 Haftung und Schadenersatz

Die Haftung jeder Partei, die sich aus oder im Zusammenhang mit diesem AVV ergibt, unterliegt den Haftungsbeschränkungen und -ausschlüssen, die im Basisvertrag festgelegt sind.

Abschnitt C - TOMs

Beschreibung der technischen und organisatorischen Massnahmen, die von dem/den Auftragsverarbeiter(n) durchgeführt werden:

1 Organisatorische Sicherheitsmassnahmen

1.1 Sicherheitsmanagement

a) Sicherheitskonzept und -verfahren: Der Auftragsverarbeiter verfügt über ein dokumentiertes Sicherheitskonzept für die Verarbeitung von personenbezogenen Daten.

b) Rollen und Verantwortlichkeiten:

   1) Die Rollen und Verantwortlichkeiten im Zusammenhang mit der Verarbeitung von personenbezogenen Daten sind klar definiert und im Einklang mit dem Sicherheitskonzept zugewiesen.

   2) Bei internen Umstrukturierungen oder Kündigungen und beim Wechsel des Arbeitsplatzes ist der Widerruf von Rechten und Zuständigkeiten mit entsprechenden Übergabeverfahren klar definiert.

c) Politik der Zugangskontrolle: Jeder Rolle, die an der Verarbeitung von personenbezogenen Daten beteiligt ist, werden nach dem Need-to-know-Prinzip spezifische Zugriffskontrollrechte zugewiesen.

d) Verwaltung der Ressourcen/Vermögenswerte: Der Auftragsverarbeiter verfügt über ein Register der für die Verarbeitung von personenbezogenen Daten verwendeten IT-Ressourcen (Hardware, Software und Netzwerk). Eine bestimmte Person ist mit der Pflege und Aktualisierung des Registers betraut (z.B. der IT-Beauftragte).

e) Änderungsmanagement: Der Auftragsverarbeiter stellt sicher, dass alle Änderungen am IT-System von einer bestimmten Person (z. B. dem IT- oder Sicherheitsbeauftragten) registriert und überwacht werden. Dieser Prozess wird regelmässig überwacht.

1.2 Reaktion auf Zwischenfälle und Geschäftskontinuität

a) Umgang mit Zwischenfällen / Verletzungen des Schutzes von personenbezogenen Daten:

   1) Es wird ein Plan für die Reaktion auf Zwischenfälle mit detaillierten Verfahren festgelegt, um eine wirksame und ordnungsgemässe Reaktion auf Zwischenfälle im Zusammenhang mit personenbezogenen Daten zu gewährleisten.

2) Der Auftragsverarbeiter meldet dem Verantwortlichen unverzüglich jeden Sicherheitsvorfall, der zu einem Verlust, einem Missbrauch oder einer unbefugten Kenntnisnahme von personenbezogenen Daten geführt hat.

b) Geschäftskontinuität: Der Auftragsverarbeiter hat die wichtigsten Verfahren und Kontrollen festgelegt, die zu befolgen sind, um das erforderliche Mass an Kontinuität und Verfügbarkeit des IT-Systems zur Verarbeitung von personenbezogenen Daten (im Falle eines Zwischenfalls/einer Verletzung des Schutzes von personenbezogenen Daten) zu gewährleisten.

1.3 HR

a) Vertraulichkeit des Personals: Der Auftragsverarbeiter stellt sicher, dass alle Mitarbeiter ihre Verantwortlichkeiten und Pflichten im Zusammenhang mit der Verarbeitung von personenbezogenen Daten kennen und das Personal zur Vertraulichkeit verpflichtet wurde. Die Rollen und Zuständigkeiten werden während des Verfahrens vor der Einstellung und/oder bei der Einarbeitung klar kommuniziert.

b) Schulung: Der Auftragsverarbeiter stellt sicher, dass alle Mitarbeiter angemessen über die Sicherheitskontrollen des IT-Systems informiert sind, die sich auf ihre tägliche Arbeit beziehen. Die mit der Verarbeitung von personenbezogenen Daten befassten Mitarbeiter werden durch regelmässige Sensibilisierungskampagnen auch angemessen über die einschlägigen Datenschutzanforderungen und rechtlichen Verpflichtungen informiert.

2 Technische Sicherheitsmassnahmen

2.1 Zugangskontrolle und Authentifizierung

a) Ein Zugangskontrollsystem, das für alle Benutzer, die auf das IT-System zugreifen, gilt, wurde eingeführt. Das System ermöglicht das Anlegen, Genehmigen, Überprüfen und Löschen von Benutzerkonten.

b) Es werden keine gemeinsamen Benutzerkonten verwendet, um die Nachvollziehbarkeit zu garantieren.

c) Bei der Gewährung des Zugangs oder der Zuweisung von Nutzerrollen ist der Grundsatz "Need-To-Know" zu beachten, um die Zahl der Nutzer, die Zugang zu personenbezogenen Daten haben, auf diejenigen zu beschränken, die diesen Zugang für die Erfüllung der Verarbeitungszwecke des Auftragsverarbeiter benötigen.

d) Wenn die Authentifizierungsmechanismen auf Passwörtern beruhen, verlangt der Auftragsverarbeiter, dass das Passwort mindestens acht Zeichen lang ist und sehr strengen

Passwortkontrollparametern entspricht, einschliesslich Länge, Zeichenkomplexität und Nichtwiederholbarkeit.

e) Die Authentifizierungsdaten (z. B. Benutzer-ID und Passwort) dürfen niemals ungeschützt über das Netz übertragen werden.

2.2 Protokollierung und Überwachung

Für jedes System/jede Anwendung, das/die für die Verarbeitung von personenbezogenen Daten verwendet wird, werden Protokolldateien aktiviert. Sie umfassen alle Arten des Zugriffs auf Daten (Ansicht, Änderung, Löschung).

2.3 Sicherheit von Daten im Ruhezustand

a) Server-/Datenbank-Sicherheit

1) Datenbank- und Anwendungsserver sind so konfiguriert, dass sie unter einem separaten Konto mit minimalen Betriebssystemprivilegien laufen, um korrekt zu funktionieren, oder in einer abgetrennten Container-Umgebung laufen.

2) Datenbank- und Anwendungsserver verarbeiten nur die personenbezogenen Daten, deren Verarbeitung zur Erreichung des Verarbeitungszwecks tatsächlich erforderlich ist.

2.4 Netz-/Kommunikationssicherheit

a) Bei jedem Zugriff über das Internet wird die Kommunikation durch kryptographische Protokolle verschlüsselt.

b) Der Verkehr zum und vom IT-System wird durch Firewalls überwacht und kontrolliert.

c) Vertrauliche Informationen werden klassifiziert und ausschliesslich verschlüsselt übertragen.

2.5 Backups

a) Sicherungs- und Datenwiederherstellungsverfahren sind definiert, dokumentiert und klar mit Rollen und Verantwortlichkeiten verknüpft.

b) Datenwiederherstellungsverfahren werden jährlich getestet.

c) Backups werden in angemessenem Umfang physisch und ökologisch geschützt, entsprechend den Standards, die für die ursprünglichen Daten gelten.

d) Die Ausführung der Backups wird auf Vollständigkeit überwacht.

2.6 Sicherheit im Lebenszyklus von Anwendungen

Während des Entwicklungszyklus werden bewährte Praktiken, der neueste Stand der Technik und anerkannte sichere Entwicklungsverfahren oder -standards befolgt.

2.7 Löschung/Entsorgung von Daten

a) Die Datenträger werden vor ihrer Entsorgung mit Software überschrieben. In Fällen, in denen dies nicht möglich ist (CDs, DVDs usw.), werden sie physisch vernichtet.

b) Papier und tragbare Datenträger, die zur Speicherung von personenbezogenen Daten verwendet werden, werden vernichtet.

2.8 Physische Sicherheit

Die physische Umgebung der IT-Systeminfrastruktur ist für nicht autorisiertes Personal nicht zugänglich. Durch geeignete technische Massnahmen (z.B. Einbruchmeldeanlage, chipkartengesteuertes Drehkreuz, Ein-Personen-Sicherheitszugangssystem, Schliessanlage) oder organisatorische Massnahmen (z.B. Wachdienst) sind die Sicherheitsbereiche und deren Zugänge gegen das Betreten durch Unbefugte zu schützen.

* * *

(Unterschriftsseite folgt)

Unterschriften

(E-Signatur ist ausreichend)

<Kunde>

Name: <Person 1>
Funktion: <Person 1 Funk.>

Name: <Person 1>
Funktion: <Person 2 Funk.>

Moodtalk AG

Name: Loris Niederberger
Funktion: Co-CEO

Name: Jonas Purtschert
Funktion: CTO