AUFTRAGSVERARBEITUNGSVEREINBARUNG

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 DE 4 DE 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

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):

Name: GROW Life Coaching

Anschrift: Seefeldstrasse 210, 8008, Zürich, Schweiz

Name, Funktion und Kontaktdaten der Kontaktperson: Olivia Tschanz

Unterschrift und Beitrittsdatum: In elektronischer Form geleistet.

Auftragsverarbeiter:

Name: KLICK-TIPP LIMITED

Anschrift: 15 Cambridge Court, 210 Shepherd’s Bush Road, London W6 7NJ, Vereinigtes Königreich

Name, Funktion und Kontaktdaten der Kontaktperson: Michael Toohig (Geschäftsführer / Managing Director)

Unterschrift und Beitrittsdatum: In elektronischer Form geleistet.

ANHANG II - BESCHREIBUNG DER VERARBEITUNG

Vorbemerkung

Der Verantwortliche hat mit der Digistore24 GmbH, St.-Godehard-Straße 32, 31139 Hildesheim, Deutschland (nachfolgend “Digistore24“) einen Hauptvertrag geschlossen (nachfolgend Hauptvertrag). Dieser Hauptvertrag verpflichtet Digistore24, dem hiesigen Verantwortlichen Zugang zu den Leistungen zu verschaffen, die der hiesige Auftragsverarbeiter erbringt (nachfolgend Klick- Tipp-Leistungen). Neben diesem Hauptvertrag soll nun zwischen dem Verantwortlichen und dem Auftragsverarbeiter ein Rechtsverhältnis i.S.v. Artikel 28 DSGVO entstehen. Abseits dessen wird kein darüberhinausgehendes Vertragsverhältnis zwischen Verantwortlichen und Auftragsverarbeiter begründet.

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Bewerber
- angestellte Beschäftigte
- ehemalige Beschäftigte
- Interessenten, die natürliche Personen sind
- Ansprechpartner bei Interessenten, die juristische Personen sind
- potentielle Interessenten, die natürliche Personen sind
- Ansprechpartner bei potentiellen Interessenten, die juristische Personen sind
- Kunden, die natürliche Personen sind
- Ansprechpartner bei Kunden, die juristische Personen sind
- ehemalige Kunden, die natürliche Personen sind
- Ansprechpartner bei ehemaligen Kunden, die juristische Personen sind
- potentielle Lieferanten, die natürliche Personen sind
- Ansprechpartner bei potentiellen Lieferanten, die juristische Personen sind
- Lieferanten, die natürliche Personen sind
- Ansprechpartner bei Lieferanten, die juristische Personen sind
- Besucher der Internetseite oder einer Landingpage
- Besucher des Auftritts in sozialen Netzwerken/Medien
- sonstige Personen, mit denen der Auftraggeber automatisiert kommuniziert

Kategorien personenbezogener Daten, die verarbeitet werden

- Kontakt- und Erreichbarkeitsdaten der o.g. betroffenen Personen
- Kommunikationsinhaltsdaten der o.g. betroffenen Personen
- tagbasierte Daten über das Verhalten bzw. Interaktionen der o.g. betroffenen Personen
- tagbasierte Eigenschaften, die der Datenimporteuer im Rahmen von Marketing- Onboarding- und sonstige Automatisierungsmaßnahmen selbst und fortlaufend definiert

Art der Verarbeitung

Die Art der Verarbeitung wird durch die schuldrechtliche Vereinbarung zwischen dem Verantwortlichen und Digistore24 bestimmt. Es werden weisungsgemäß Maßnahmen des Online- Marketings und der Marketingautomation ausgeführt. Das umfasst insbesondere den automatisierten Versand von E-Mails und sonstigen elektronischen Nachrichten, sowie deren Auswertung.

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

Die Zwecke werden ebenfalls durch die schuldrechtliche Vereinbarung zwischen dem Verantwortlichen und Digistore24 bestimmt. Es geht i.d.R. um die vertragsbezogene und werbliche Kommunikation mit den Betroffenen.

Dauer der Verarbeitung

Die Dauer der Verarbeitung ist grundsätzlich an den Bestand der schuldrechtlichen Vereinbarung zwischen dem Verantwortlichen und Digistore24 geknüpft.

Unterauftragsverarbeitung

1. Der Dienstleister Anexia Deutschland GmbH, Konrad Zuse Platz, 81829 München wurde mit der Speicherung von Daten unterbeauftragt.
2. Der Dienstleister Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109 wurde mit der Speicherung von Daten unterbeauftragt, wobei die Weisung erteilt wurde, dass Daten ausschließlich auf dem Gebiet der Europäischen Union gespeichert werden dürfen. Damit liegt keine Übermittlung i.S.v. Artikel 44 DSGVO vor. Vorsorglich wurde der Unterauftragsverarbeiter jedoch gemäß Artikel 46 DSGVO verpflichtet. Dem steht nicht die Rechtsprechung des Europäischen Gerichtshofs entgegen. Denn die erforderliche Einzelfallbetrachtung hat ergeben, dass der Umstand, dass die Daten ausschließlich in Rechenzentren innerhalb der Europäischen Union gespeichert werden, die Risiken hinreichend minimiert.

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

Maßnahmen zur Pseudonymisierung/Anonymisierung

Bei Klick-Tipp werden Daten in unterschiedlichen Tabellen gespeichert. Pseudonyme sind dabei stets IDs, z.B. die User-ID (die ein Klick-Tipp-Kundenkonto eines Klick-Tipp-Kunden identifiziert) oder die Subscriber- ID (die einen Empfänger eines unserer Kunden identifiziert).

Anwendungsfall 1: Alle E-Mail-Adressen sowie weitere Informationen zu einem Opt-in (z.B. Zeitpunkt, IPAdresse etc.) werden in der Subscriber-Tabelle gespeichert. Ohne die Tabelle, in der die User-ID dem Kundenkonto zugeordnet wird, kann man nicht erkennen, welche E-Mail-Adresse zu welchem Benutzerkonto gehört.

Anwendungsfall 2: Alle Tags (virtuelle Notizschilder) werden in einer riesigen Tag-Tabelle gespeichert. Die Tag-Tabelle enthält ausschließlich IDs, u.a. auch die Subscriber-ID. Ohne die Tabelle, in der die Subscriber- ID dem Empfänger zugeordnet wird, kann man nicht erkennen, welches Tag zu welchem Empfänger gehört.

Maßnahmen zur Verschlüsselung personenbezogener Daten

Klick-Tipp speichert Passwörter verschlüsselt. Klick-Tipp Mitarbeiter (z.B. unser Customer Happiness Team) loggt sich in Klick-Tipp-Konten unserer Kunden über einen speziellen Support-Zugang ein – ohne die Nutzung von Passwörtern unserer Kunden.

Die Passwörter unserer Kunden werden also anonymisiert gespeichert. Man kann aus den Schlüsseln nicht auf die Passwörter schließen. Die Datenträger, auf denen die Backups der Datenträger durchgeführt werden, sind verschlüsselt.

Klick-Tipp speichert die Daten ausschließlich bei externen Cloud-Anbietern, die insoweit folgende Maßnahmen ergreifen:

- Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109, United States („AWS“): Der Anbieter ist nach ISO/IEC 27018:2014 Der Anbieter ist nach ISO 27001 zertifiziert. Klick-Tipp wird weitere Zertifizierungen überwachen und dokumentieren. Hierzu ist ergänzend noch auszuführen: Die Daten werden verschlüsselt und zwar im Amazon S3 Advanced Encryption Standard (AES) 256 Verschlüsselungsstandard mit symmetrischen Schlüsseln unter Verwendung von 256-Bit-Verschlüsselungsschlüsseln.
- Anexia Deutschland GmbH, Konrad Zuse Platz, D-81829 München („Anexia“): Alle Prozesse des Anbieters sind nach ISO 9001:2015 zertifiziert und werden jährlich durch den TÜV Nord verifiziert. Seit der Einführung der ISO 9001:2008 Zertifizierung hat der Anbieter die ersten ISO/IEC 27001 konformen Prozesse eingeführt und diese im Laufe der Jahre 2011 und 2012 fortentwickelt. In Zusammenarbeit mit externen IT-Sicherheits-Fachkräften und dem TÜV Nord ist der Anbieter seit September 2012 erfolgreich nach ISO/IEC 27001:2005 und seit November 2015 nach ISO/IEC 27001:2013 zertifiziert. Klick-Tipp wird weitere Zertifizierungen überwachen und dokumentieren.

Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Klick Tipp nimmt anlassbezogen und im Übrigen anlasslos gemäß einem Prüfzyklus von 12 Monaten eine Risikobewertung vor und prüft anschließend, ob die ergriffenen technischen und organisatorischen Maßnahmen noch hinreichend sind, um die Risiken adäquat zu minimieren. Notwendige Änderungen werden vorgenommen.

Ferner gilt noch:

Klick-Tipp verfolgt konsequent den „Infrastructure as Code“-Ansatz. Kern dieses Ansatzes ist, dass Klick- Tipp-Server nicht mehr lokal, sondern über ein zentrales Konfigurationsmanagement konfiguriert und gewartet werden. Durch das zentrale Konfigurationsmanagement und die dadurch mögliche Automatisierung kann Infrastruktur bei Klick-Tipp sehr viel effizienter und sicherer bereitgestellt werden. Es kommt auch zu viel weniger Fehlern, weil Server nicht mehr einzeln konfiguriert werden müssen, sondern durch Skripte automatisiert ausgeliefert werden können.

Ein besonderes Augenmerk hierbei ist der Klick-Tipp Datenbank-Cluster, denn dort sind die Daten unserer Kunden gespeichert. Klick-Tipp hat dabei Sicherheitsmaßnahmen ergriffen, die über das über das übliche Maß einer Datenbankinstallation weit hinausgehen. Der Klick-Tipp Datenbank-Cluster besteht aus drei Servern, die untereinander mithilfe einer SSL-geschützten Replikation in einem eigenen Netzwerk miteinander und über eine SSL-Verbindung mit der Klick-Tipp Anwendung kommunizieren. Der erste Server in diesem Netzwerk beantwortet die Anfragen der Anwendung. Der zweite Server springt im Notfall durch ein automatisches Failover ein, falls der erste Server nicht mehr verfügbar sein sollte. Der dritte Server stellt sicher, dass Klick-Tipp Daten in regelmäßigen Abständen gesichert werden können, ohne dass es dabei zu Einschränkungen im Produktivbetrieb gibt.

Klick-Tipp Datenbank wird dabei wie folgt gesichert:

- Binary-Backup alle drei Stunden in der AWS-Cloud (Aufbewahrung 24 Stunden)
- MySQL-Dump einmal pro Tag in der AWS-Cloud (Aufbewahrung 120 Tage)
- MySQL-Dump einmal pro Tag in der Anexia-Cloud (Aufbewahrung 120 Tage)

Was Klick-Tipp im Rahmen seiner Infrastructure-as-Code-Initiative noch entwickeln wird, ist ein wöchentliches Upgrade-Konzept, in dem alle Infrastrukturkomponenten wöchentlich einmal aktualisiert, getestet und in den Produktivbetrieb verteilt werden.

Maßnahmen zur Zutrittskontrolle

Die Räume von Klick-Tipp sind gegen unberechtigten Zutritt innerhalb der Bürozeiten durch eine verschlossene Eingangstür geschützt, die nur nach Kontrolle durch die Mitarbeiter geöffnet wird. Außerhalb der Geschäftszeiten werden die Büroräume durch hochwertige Schlösser und eine Alarmanlage geschützt.

Hinzukommt, dass sich in diesen Räumen keine lokalen Server oder physische Kundenakten befinden, da diese Daten ausschließlich in Cloud-Systemen gespeichert werden, deren Anbieter entsprechende Sicherheitsmaßnahmen ergriffen haben.

Maßnahmen der Zugriffskontrolle

Klick-Tipp hat ein ausdifferenziertes, tätigkeitsbezogenes Berechtigungskonzept implementiert. Externe Wartungsunternehmen haben nur Zugriff, soweit dies erforderlich ist, und werden sorgfältig ausgewählt und überprüft.

Zum Bereich der Fernwartung ist folgendes auszuführen: Die Einwahl zur Fernwartung wird durch eine Multi-Faktor-Authentifizierung und ein adäquates Passwortmanagement geschützt. Zusätzlich ist eine interne Freigabe durch Klick-Tipp erforderlich.

Die Zugriffsrechte des mit der Wartung betrauten Technikers sind auf das Mindestmaß beschränkt. Nach jeder Fernwartungssitzung verändert sich der Code, der bei der Multi-Faktor-Authentifizierung verwendet wird.

Maßnahmen der Weitergabekontrolle

Der Datenaustausch mit Schwestergesellschaften erfolgt elektronisch. Beim Zugriff auf Kundendaten (vgl. auch Berechtigungskonzept oben) müssen die Mitarbeiter der Schwestergesellschaften ihre IP-Adresse freischalten, bevor das System den Zugriff auf Kundendaten ermöglicht. Die Entwickler und Systemadministratoren können nur über einen speziellen Admin-Server auf die Kundendaten zugreifen. Der Admin-Server ist nur von den Rechnern der Admins aus bedienbar.

Marketing-Tools: Hier überträgt bzw. empfängt Klick-Tipp immer nur diejenigen Daten, die der Klick-Tipp- Kunde in seinem Klick-Tipp-Konto konfiguriert. Die Verbindungen werden über API-Schnittstellen hergestellt, die über die üblichen Branchenstandards abgesichert werden.

Maßnahmen der Eingabekontrolle

Es sind hinreichende Maßnahmen ergriffen worden; u.a. erfolgt eine personalisierte Anmeldung, die protokolliert wird.

Maßnahmen der Auftragskontrolle

Klick-Tipp hat einen externen, fachkundigen und zuverlässigen Datenschutzbeauftragten bestellt, der die Auslagerungsvorgänge anhand einer vordefinierten Prüfmatrix entsprechend den Vorgaben aus Artikel 28 DSGVO prüft, überwacht und das entsprechende Vertragsmanagement sicherstellt.

Maßnahmen der Trennungskontrolle

Die Ordner- und Zugriffsstruktur ist mit dem oben beschriebenen Berechtigungskonzept verknüpft, sodass Daten zu unterschiedlichen Zwecken an unterschiedlichen Orten gespeichert werden.

Maßnahmen der Verfügbarkeitskontrolle

Die Klick-Tipp Datenbank wird dabei wie folgt gesichert:

- Binary-Backup alle drei Stunden in der AWS-Cloud (Aufbewahrung 24 Stunden)
- MySQL-Dump einmal pro Tag in der AWS-Cloud (Aufbewahrung 120 Tage)
- MySQL-Dump einmal pro Tag in der Anexia-Cloud (Aufbewahrung 120 Tage)

Die eingesetzten Cloud-Anbieter gewährleisten folgendes:

- AWS: Der Anbieter ist nach ISO/IEC 27018:2014. Klick-Tipp wird weitere Zertifizierungen überwachen und dokumentieren. Ergänzend ist hierzu folgendes auszuführen: Rechenzentren sind in Clustern in verschiedenen globalen Regionen aufgebaut. Alle Rechenzentren sind online und bedienen Kunden. Kein Rechenzentrum ist "kalt". Im Fehlerfall verlagern automatisierte Prozesse den Kundendatenverkehr aus dem betroffenen Bereich. Es ist sichergestellt, dass im Falle eines Rechenzentrumsausfalls genügend Kapazität zur Verfügung steht, um den Lastausgleich für die verbleibenden Standorte zu kompensieren. Ferner differenziert der Anbieter zwischen verschiedenen Verfügbarkeitszonen. Jede Verfügbarkeitszone ist als unabhängige Fehlerzone ausgelegt. Dies bedeutet, dass die Verfügbarkeitszonen innerhalb einer typischen Metropolregion räumlich getrennt sind und sich in Niedrigwasser-Überschwemmungsgebieten befinden (die spezifische Kategorisierung der Überschwemmungsgebiete variiert je nach Region). Zusätzlich zur unterbrechungsfreien Stromversorgung und zu den Onsite-Backup-Generatoren wird die Energiezufuhr über verschiedene Netze von unabhängigen Versorgungsunternehmen gespeist, um einzelne Fehlerquellen weiter zu reduzieren. Verfügbarkeitszonen sind alle redundant verbunden.
- Anexia:Alle Prozesse des Anbieters sind nach ISO 9001:2015 zertifiziert und werden jährlich durch den TÜV Nord verifiziert. Seit der Einführung der ISO 9001:2008 Zertifizierung hat der Anbieter die ersten ISO/IEC 27001 konformen Prozesse eingeführt und diese im Laufe der Jahre 2011 und 2012 fortentwickelt. In Zusammenarbeit mit externen IT-Sicherheits-Fachkräften und dem TÜV Nord ist der Anbieter seit September 2012 erfolgreich nach ISO/IEC 27001:2005 und seit November 2015 nach ISO/IEC 27001:2013 zertifiziert. Klick-Tipp wird weitere Zertifizierungen überwachen und dokumentieren.

Maßnahmen zur raschen Wiederherstellung der Verfügbarkeit bei einem physischen oder technischen Zwischenfall

Klick-Tipp erstellt in kurzen zeitlichen Intervallen Binary-Backups. Damit können Daten in Minuten wiederhergestellt werden und sie sind v.a. auf einem Stand, der nicht – wie bei einer Wiederherstellung mit einem MySQL-Dump – viele Stunden zurückliegt.

Die eingesetzten Cloud-Anbieter gewährleisten folgendes:

- AWS: Der Anbieter ist nach ISO/IEC 27018:2014. Klick-Tipp wird weitere Zertifizierungen überwachen und dokumentieren. Ergänzend ist hierzu folgendes auszuführen: Die Infrastruktur des Anbieters verfügt über ein hohes Maß an Verfügbarkeit und bietet den Kunden die Funktionen zur Bereitstellung einer ausfallsicheren IT-Architektur. Der Anbieter hat seine Systeme so konzipiert, dass System- oder Hardwarefehler mit minimaler Auswirkung auf den Kunden toleriert werden. Das Betriebskontinuitätsmanagement für Rechenzentren des Anbieters steht unter der Leitung sachkundiger und zuverlässiger Spezialisten. Ein Notfallteam verwendet branchenübliche Diagnoseverfahren, um die Lösung bei geschäftskritischen Ereignissen zu verbessern. Mitarbeiter bieten eine unterbrechungsfreie Abdeckung (24 Stunden/Tag – 7 Tage/Woche – 365 Tage/Jahr), um Vorfälle zu erkennen und die Auswirkungen und die Auflösung zu verwalten.
- Anexia: Alle Prozesse des Anbieters sind nach ISO 9001:2015 zertifiziert und werden jährlich durch den TÜV Nord verifiziert. Seit der Einführung der ISO 9001:2008 Zertifizierung hat der Anbieter die ersten ISO/IEC 27001 konformen Prozesse eingeführt und diese im Laufe der Jahre 2011 und 2012 fortentwickelt. In Zusammenarbeit mit externen IT-Sicherheits-Fachkräften und dem TÜV Nord ist der Anbieter seit September 2012 erfolgreich nach ISO/IEC 27001:2005 und seit November 2015 nach ISO/IEC 27001:2013 zertifiziert. Klick-Tipp wird weitere Zertifizierungen überwachen und dokumentieren.

Maßnahmen zur Sicherstellung der Belastbarkeit der Systeme und Dienste auf Dauer

In diesem Zusammenhang ergreift Klick-Tipp selbst folgende vier Maßnahmen:

- Backup-Policy, vgl. Ausführungen oben.
- Infrastructure-as-Code-Ansatz. Kern dieses Ansatzes ist, dass die Server nicht mehr lokal, sondern über ein zentrales Konfigurationsmanagement konfiguriert und gewartet werden. Durch das zentrale Konfigurationsmanagement und die dadurch mögliche Automatisierung kann Infrastruktur bei Klick-Tipp sehr viel effizienter und sicherer bereitgestellt werden. Es kommt auch zu viel weniger Fehlern, weil Server nicht mehr einzeln konfiguriert werden müssen, sondern durch Skripte automatisiert ausgeliefert werden können. Ohne die Nutzung der AWS-Cloud wäre dieser Ansatz undenkbar.
- Ferner hat Klick-Tipp ein umfangreiches Monitoring- und Alarming-Systems entwickelt. Alle Infrastrukturkomponenten werden 24/7 automatisiert überwacht. Wenn Infrastrukturkomponenten fehlerhaft sind, dann bekommen unsere Techniker auf ihre Handies Nachrichten und greifen ein.
- Klick-Tipp hat einen externen, fachkundigen und zuverlässigen Datenschutzbeauftragten bestellt, der die entsprechenden Maßnahmen alle sechs Monate und anlassbezogen überprüft.

ANHANG IV - LISTE DER UNTERAUFTRAGSVERARBEITER:

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1. Der Dienstleister Anexia Deutschland GmbH, Konrad Zuse Platz, 81829 München wurde mit der Speicherung von Daten unterbeauftragt.
2. Der Dienstleister Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109 wurde mit der Speicherung von Daten unterbeauftragt, wobei die Weisung erteilt wurde, dass Daten ausschließlich auf dem Gebiet der Europäischen Union gespeichert werden dürfen. Damit liegt keine Übermittlung i.S.v. Artikel 44 DSGVO vor. Vorsorglich wurde der Unterauftragsverarbeiter jedoch gemäß Artikel 46 DSGVO verpflichtet. Dem steht nicht die Rechtsprechung des Europäischen Gerichtshofs entgegen. Denn die erforderliche Einzelfallbetrachtung hat ergeben, dass der Umstand, dass die Daten ausschließlich in Rechenzentren innerhalb der Europäischen Union gespeichert werden, die Risiken hinreichend minimiert.

ANHANG V - VERSCHWIEGENHEITSERKLÄRUNG NACH § 203 STGB

Nur sofern der Verantwortlicher ein sog. Berufsgeheimnisträger sind, gilt folgende Zusatzvereinbarung:

Die nach dieser Auftragsverarbeitung zu verarbeitenden Daten lassen auch Rückschlüsse auf Personen zu, die durch eine besondere, berufliche Schweigepflicht geschützt sind. Dies vor Augen schließen die Parteien folgende Verschwiegenheitsvereinbarung:

1. Der Auftragsverarbeiter ist zur Verschwiegenheit über solche Daten und Informationen verpflichtet, die ihm bei der Ausübung seiner Tätigkeit bekannt geworden sind und zu denen. Maßgeblich ist der Privatgeheimnisbegriff des jeweils geltenden Berufsrechts (in Deutschland: § 203 StGB).
2. Der Auftragsverarbeiter darf diese Daten und Informationen nur verwenden, soweit dies für die Erfüllung des Hauptvertrages erforderlich ist.
3. Der Auftragsverarbeiter verpflichtet seine Mitarbeiter (m/w/d) zur selben Verschwiegenheit.
4. Der Auftragsverarbeiter bestätigt, auf die strafrechtlichen Folgen eines Verstoßes gegen diese Vereinbarung hingewiesen worden zu sein.
5. Dieser Vertrag wird durch Zustandekommen der Auftragsverarbeitung wirksam. Dies gilt auch zugunsten der Berufsträger, die diese nicht abgeschlossen haben, die aber zum Verantwortlichen gehören. Die Vereinbarung wird auch als echter Vertrag zugunsten Dritter mit Unterzeichnung nach Satz 1 wirksam.