Vereinbarung zur Auftragsverarbeitung

gem. Art. 28 DSGVO

zwischen

JoMoCo UG (haftungsbeschränkt) i. G.
Wiesenblick 5
87466 Oy Mittelberg
Deutschland

– nachfolgend „Auftragsverarbeiter“ –

und

dem jeweiligen Kunden, der als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO handelt

– nachfolgend „Verantwortlicher“ –

gemeinsam auch „Vertragsparteien“

Als Anlage zu den jeweils geltenden Nutzungsbedingungen beziehungsweise zum Hauptvertrag über die Nutzung der vom Auftragsverarbeiter bereitgestellten cloudbasierten Plattform „Jomoco-Solutions“ wird folgende Vereinbarung zur Auftragsverarbeitung geschlossen.

Inhalt

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (*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* - DSGVO) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich und Gegenstand der Verarbeitung

(1) Diese Vereinbarung findet Anwendung auf die Erhebung, Verarbeitung und Löschung sämtlicher personenbezogener Daten, die Gegenstand des Hauptvertrages sind, im Rahmen seiner Durchführung anfallen oder dem Auftragsverarbeiter im Zusammenhang mit der Nutzung der Plattform „Jomoco-Solutions“ bekannt werden.

(2) Gegenstand der Verarbeitung ist die Bereitstellung und Nutzung der cloudbasierten Plattform „Jomoco-Solutions“ des Auftragsverarbeiters einschließlich der damit verbundenen Funktionen zur Konfiguration, Verwaltung, Analyse und dem technischen Betrieb der Plattform sowie aller darüber bereitgestellten digitalen Funktionen

(3) Nicht unter den Anwendungsbereich fallen Daten von Mitarbeitern des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

§ 2 Dauer und Konkretisierung des Auftragsinhalts

(1) Die Dauer der Verarbeitung personenbezogener Daten ergibt sich aus dem Hauptvertrag beziehungsweise den jeweils geltenden Nutzungsbedingungen. Die Verarbeitung beginnt mit Beginn des Vertragsverhältnisses und endet mit dessen Beendigung.

(2) Diese Vereinbarung gilt unbeschadet des Absatzes 1 so lange, wie der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen verarbeitet, einschließlich etwaiger Sicherungskopien.

(3) Im Fall eines Widerspruchs zwischen dieser Vereinbarung und Bestimmungen des Hauptvertrages geht diese Vereinbarung den widersprechenden Bestimmungen des Hauptvertrages vor, soweit es um die Regelung der Auftragsverarbeitung im Sinne von Art. 28 DSGVO geht.

(4) Umfang, Art und Zweck der Verarbeitung

> Zweck der Verarbeitung ist die Bereitstellung, Nutzung, Konfiguration, Verwaltung, Analyse und der technische Betrieb der Plattform „Jomoco-Solutions“ sowie aller darüber bereitgestellten digitalen Funktionen. Die Verarbeitung umfasst insbesondere CRM, Kundenmanagement, Kommunikation, Messaging, Automation, Workflows, Telefonie, Kampagnen, Marketing, Terminverwaltung, Analyse, Reporting, Benutzerverwaltung und systemtechnische Sicherheits- und Betriebsprozesse.

(5) Art der personenbezogenen Daten

Im Rahmen der Nutzung der Plattform „Jomoco-Solutions“ können insbesondere folgende Kategorien personenbezogener Daten verarbeitet werden

– Namen
– E Mail Adressen
– Telefonnummern
– Account, Profil und Zugangsdaten
– CRM und Kontaktdaten
– Kommunikationsinhalte wie Nachrichten, E Mails, Chatverläufe, Gesprächs und Interaktionsmetadaten
– Social Media Daten (Accounts, Inhalte, Interaktionen)
– Marketing , Tracking und Kampagnendaten
– Automations , Workflow und Prozessdaten
– Nutzungs , Meta , Analyse und Protokolldaten
– gegebenenfalls Sprach , Audio oder Kommunikationsmetadaten

(6) Kategorien betroffener Personen

Von der Datenverarbeitung können insbesondere folgende Gruppen betroffener Personen erfasst sein

– Kunden des Verantwortlichen

– Interessenten und Leads

– Mitarbeiter des Verantwortlichen

– Kommunikationspartner

– sonstige vom Verantwortlichen eingebundene Dritte

§ 3 Verantwortlichkeit und Weisungsbefugnis

(1) Die Vertragsparteien sind jeweils für die Einhaltung der sie betreffenden datenschutzrechtlichen Bestimmungen verantwortlich. Der Verantwortliche bleibt im Verhältnis der Parteien zueinander die für die Verarbeitung personenbezogener Daten verantwortliche Stelle im Sinne von Art. 4 Nr. 7 DSGVO. Er kann jederzeit die Berichtigung, Anpassung, Löschung, Einschränkung der Verarbeitung oder Herausgabe der Daten verlangen, soweit dem keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

(2) Zur Gewährleistung des Schutzes der Rechte betroffener Personen unterstützt der Auftragsverarbeiter den Verantwortlichen im angemessenen Umfang, insbesondere durch geeignete technische und organisatorische Maßnahmen.

(3) Wendet sich eine betroffene Person zwecks Geltendmachung von Betroffenenrechten unmittelbar an den Auftragsverarbeiter, leitet dieser das Ersuchen unverzüglich an den Verantwortlichen weiter, sofern keine eigene gesetzliche Verpflichtung zur Bearbeitung besteht.

(4) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtliche Verpflichtung vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

Weisungen können in Textform, insbesondere per E Mail oder über die bereitgestellte Plattform, erteilt werden. Die Weisungen werden zunächst durch den Hauptvertrag und diese Vereinbarung festgelegt und können im Verlauf der Zusammenarbeit in dokumentierter Form konkretisiert, geändert oder ergänzt werden.

(5) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt. Der Auftragsverarbeiter ist berechtigt, die entsprechende Weisung bis zu einer Bestätigung oder Abänderung durch den Verantwortlichen auszusetzen.

Verlangt der Verantwortliche die Umsetzung einer Weisung, obwohl der Auftragsverarbeiter ihn auf einen möglichen Verstoß gegen Datenschutzrecht hingewiesen hat, trägt der Verantwortliche die daraus resultierenden rechtlichen Konsequenzen, soweit er die Weisung zu vertreten hat.

(6) Änderungen des Verarbeitungsgegenstandes oder der eingesetzten Verfahren, die wesentliche Auswirkungen auf den Datenschutz haben, werden zwischen den Vertragsparteien abgestimmt und dokumentiert. Auskünfte an Dritte oder an betroffene Personen erteilt der Auftragsverarbeiter nur nach vorheriger ausdrücklicher Zustimmung des Verantwortlichen, soweit nicht eine eigene gesetzliche Verpflichtung zur Auskunft besteht.

(7) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter führt ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt dem Verantwortlichen auf Wunsch die für dessen Verzeichnis erforderlichen Informationen zur Verfügung.

(8) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet grundsätzlich im Gebiet der Europäischen Union oder des Europäischen Wirtschaftsraumes statt. Eine Verarbeitung in einem Drittland ist nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DSGVO, insbesondere angemessene Garantien, erfüllt sind und der Verantwortliche dem zugestimmt hat beziehungsweise dies im Hauptvertrag oder in dieser Vereinbarung vorgesehen ist.

(9) Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Weisung des Verantwortlichen verarbeiten, es sei denn, sie sind gesetzlich hierzu verpflichtet. Erfolgt eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters, stellt dieser durch geeignete technische und organisatorische Maßnahmen sicher, dass ein dem Risiko angemessenes Schutzniveau gewährleistet ist.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen. Dies umfasst auch die Belehrung über die Weisungsgebundenheit und Zweckbindung im Rahmen dieses Auftragsverhältnisses.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und bei der Dokumentation der sie betreffenden Rechenschaftspflichten im Sinne der Art. 5 Abs. 2 und 24 Abs. 1 DSGVO, insbesondere bei der Umsetzung geeigneter technischer und organisatorischer Maßnahmen. Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu auf Anfrage die erforderlichen Informationen zur Verfügung.

(3) Sofern gesetzlich vorgeschrieben, benennt der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten und teilt dem Verantwortlichen auf Anfrage die Kontaktdaten mit.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen der zuständigen Aufsichtsbehörden, soweit diese die Verarbeitung personenbezogener Daten des Verantwortlichen betreffen, sowie über entsprechende Anfragen, Ermittlungen oder Auskunftsersuchen.

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die im Anhang 1 „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang ist Gegenstand dieser Vereinbarung.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der im Anhang 1 „Technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch

- durch Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren),
- durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO,
- einer Zertifizierung nach Art. 42 DSGVO oder
- einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung

gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(4) Der Verantwortliche kann sich im Benehmen mit dem Auftragsverarbeiter jederzeit zu Prüfzwecken in dessen Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

(5) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

(6) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

§ 7 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.

(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 8 Subunternehmen

(1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmen) nur mit vorheriger ausdrücklicher Zustimmung in Textform des Verantwortlichen in Anspruch nehmen. Die zur Erfüllung dieses Vertrages hinzugezogenen Subunternehmen sind im Anhang 2: "Genehmigte Unterauftragsverhältnisse" im Einzelnen bezeichnet. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden. Sofern es sich um eine allgemeine Genehmigung in Schrift- oder Textform handelt, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmen. Der Verantwortliche kann gegen derartige Änderungen Einspruch erheben. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

(3) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortlichen berechtigt, auf schriftliche Anforderung vom Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.

(4) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 9 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, der/dem Datenschutzbeauftragten des Verantwortlichen (sofern benannt) sowie der zuständigen Aufsichtsbehörde zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren. Der Auftragsverarbeiter unterwirft sich zusätzlich zu der für ihn bestehenden gesetzlichen Datenschutzaufsicht der Kontrolle der für den Verantwortlichen bestehenden Datenschutzaufsicht und der Kontrolle durch die/den Datenschutzbeauftragten des Verantwortlichen (sofern benannt) mit Ausnahme der Bereiche, die keinerlei Bezug zur Auftragserfüllung haben. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte der Genannten einschließlich der Einsicht in durch

Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiter anweisen, mit den Genannten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 10 Geheimhaltung

(1) Die Vertragsparteien sind verpflichtet, die ihnen unter diesem Vertrag von der jeweils anderen Partei zugänglich gemachten Informationen sowie Kenntnisse, die sie bei dieser Zusammenarbeit über Angelegenheiten – etwa technischer, kommerzieller oder organisatorischer Art – von der jeweils anderen Vertragspartei erlangen, vertraulich zu behandeln und während der Dauer sowie nach Beendigung dieser Vereinbarung ohne die vorherige Einwilligung in Textform der betroffenen Partei nicht für andere Zwecke als die Durchführung dieser Vereinbarung zu verwerten oder zu nutzen oder Dritten zugänglich zu machen. Eine Nutzung dieser Informationen ist allein auf den Gebrauch zur Durchführung dieser Vereinbarung beschränkt.

(2) Diese Vertraulichkeitsverpflichtung gilt nicht für Informationen, die

- bei Vertragsabschluss bereits allgemein bekannt waren oder
- nachträglich ohne Verstoß gegen die in dieser Vereinbarung enthaltenen Verpflichtungen allgemein bekannt wurden oder
- Gegenstand von Ermittlungen durch Behörden oder Gerichte sind und im Zuge dieser Ermittlungen aufgrund einer Verfügung oder eines Beschlusses herauszugeben sind.

§ 11 Haftung

Für die Haftung aufgrund von Verletzungen der Datenschutzbestimmungen oder dieser Datenschutzvereinbarung gelten die gesetzlichen Vorschriften, sofern in den für die vertragsgegenständlichen Leistungen geltenden Vertragsdokumenten keine abweichende Haftungsvereinbarung getroffen wurde.

§ 12 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - bedürfen einer Vereinbarung in Textform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

_____	_____
Datum, Ort	Datum, Ort
_____	_____
Unterschrift (Verantwortlicher)	Unterschrift (Auftragsverarbeiter)
_____	_____
Name, Vorname, Funktion	Name, Vorname, Funktion

Anhang 1 „Technisch-organisatorische Maßnahmen“

nach Art. 32 DSGVO

Die folgenden Maßnahmen werden vom Auftragsverarbeiter zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus umgesetzt. Sie gelten für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Nutzung der Plattform „Jomoco-Solutions“.

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

Konkrete Beschreibung der technisch-organisatorischen Maßnahmen des Auftragsverarbeiters unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen:

1. Vertraulichkeit (Art. 32 Abs. 1 Buchst. b DSGVO)

1.1 Zutrittskontrolle
Ziel: Verhindern, dass Unbefugte Zugang zu IT-Systemen oder Datenverarbeitungsumgebungen erhalten.

Maßnahmen:

- Räumliche Zugangssicherung durch Schlüssel und Schließsysteme
- Zutritt nur für berechtigte Personen
- Serverstandorte ausschließlich bei zertifizierten Rechenzentrumsbetreibern (z. B. Hetzner / EU)
- Rechenzentren verfügen über professionelle Zutritts- und Überwachungssysteme des jeweiligen Anbieters (z. B. RFID, Zugangskontrollen, Security-Personal)
- Server stehen in abgeschlossenen Serverschränken des Rechenzentrumsbetreibers

1.2 Zugangskontrolle
Ziel: Unbefugte Nutzung von Systemen verhindern.

Maßnahmen:

- Individuelle Benutzerkonten
- Passwortschutz gemäß Stand der Technik (Mindestlänge, Richtlinien)
- 2-Faktor-Authentifizierung, sofern vom Nutzer aktiviert
- Automatische Sperrung bei Fehlversuchen
- Verschlüsselung mobiler Endgeräte, sofern geschäftlich genutzt
- Regelmäßige Aktualisierung von Betriebssystemen und Software
- Sichere Verwaltung der Admin-Zugänge

1.3 Zugriffskontrolle

Ziel: Sicherstellen, dass nur Berechtigte Daten bearbeiten können.

Maßnahmen:

- Rollen- und Berechtigungssystem innerhalb der Plattform
- Trennung von Administrator- und Nutzerrechten
- Protokollierung sicherheitsrelevanter Administrationsvorgänge
- Sichere Löschprozesse für nicht mehr benötigte Daten und Datenträger
- Kein Zugriff durch unberechtigte Dritte

1.4 Trennungskontrolle

Ziel: Verhindern, dass Daten zu unterschiedlichen Zwecken vermischt werden.

Maßnahmen:

- Logische Mandantentrennung innerhalb der Plattform
- Datenverarbeitung getrennt pro Kundenaccount
- Trennung der Produktions- und Testsysteme

1.5 Pseudonymisierung (Art. 32 Abs. 1 Buchst. a DSGVO; Art. 25 Abs. 1 DSGVO)

Ziel: Minimierung von Personenbezug.

Maßnahmen:

- Verarbeitung personenbezogener Daten nur wenn erforderlich
- Pseudonymisierung ausgewählter Nutzungsdaten, wenn technisch vorgesehen
- Trennung der Zuordnungsinformationen

2. Integrität (Art. 32 Abs. 1 Buchst. b DSGVO)

2.1. Weitergabekontrolle

Ziel: Schutz bei Übertragung oder Weitergabe von Daten.

Maßnahmen:

- Verschlüsselte Übertragung über TLS/SSL
- Zugriff von außen nur über gesicherte Verbindung
- Verschlüsselte Kommunikation mit Unterauftragsverarbeitern
- Passwörter und Zugangsinformationen werden nie im Klartext übertragen
- Versand sensibler Informationen ausschließlich verschlüsselt

2.2. Eingabekontrolle

Ziel: Nachvollziehen können, wer Daten eingegeben, verändert oder gelöscht hat.

Maßnahmen:

- Protokollierung wesentlicher Systemvorgänge
- Individuelle Benutzerkonten
- Zugang zu Protokollen nur für berechtigte Administratoren

- Keine Nutzung von Sammelkonten

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Buchst. b DSGVO)

3.1. Verfügbarkeitskontrolle

Ziel: Schutz vor Datenverlust, Störungen und Ausfällen.

Maßnahmen:

- Tägliche Backups durch Rechenzentrumsanbieter
- Verschlüsselte Speicherung der Backups
- Redundante Serverinfrastruktur (z. B. RAID, Cluster)
- 24/7-Überwachung der Systemverfügbarkeit
- Einsatz aktueller Schutzprogramme (Firewall, Virenschutz auf lokalen Systemen)
- Regelmäßige Sicherheitsupdates
- Notfall- und Wiederherstellungsverfahren der Hosting-Provider

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 Buchst. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Datenschutz-Management

- Interne Prozesse zur Prüfung und Umsetzung von Datenschutzanforderungen
- Regelmäßige Überprüfung der eingesetzten Systeme auf Sicherheits- und Datenschutzkonformität
- Schulung der Mitarbeiter im sicheren Umgang mit Daten
- Verpflichtung der Mitarbeitenden auf Vertraulichkeit
- Führen eines Verzeichnisses der Verarbeitungstätigkeiten
- Prüfung der Auftragsverarbeiter (Subunternehmer)

4.2 Incident-Response-Management

- Verfahren zur Erkennung und Meldung von Datenschutzvorfällen
- Verpflichtung zur unverzüglichen internen Meldung von Störungen
- Dokumentation von Vorfällen
- Ablaufplan zur Bewertung und Behandlung von Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

- Rollen- und Rechtekonzept nach dem Need-to-know-Prinzip
- Standardmäßig eingeschränkte Datenzugriffe
- Minimaldatenerhebung innerhalb der Plattform

4.4 Auftragskontrolle

- Schriftliche Verträge mit Subdienstleistern
- Regelmäßige Prüfung ihrer Datenschutz- und Sicherheitsmaßnahmen
- Dokumentation aller wesentlichen Änderungen

Anhang 2 „Genehmigte Unterauftragsverhältnisse“

Unterauftragsverarbeiter	Anschrift / Land	Datenverarbeitung	Serverstandort
Bluesky Social PBC	USA	Dezentrale Social Media Plattform für textbasierte Kommunikation	USA
CleverReach GmbH & Co. KG	Deutschland	E Mail Marketing und Kommunikationsdienste	Deutschland
Google Ireland Ltd. (YouTube / YouTube Creative Studio)	Irland / EU	Video Verwaltung Analyse und Monetarisierungsfunktionen	EU und ggf. weitere Regionen gemäß Google Infrastruktur
Hetzner Online GmbH	Deutschland	Hosting und Infrastrukturleistungen	Deutschland, ggf. weitere Rechenzentren in der EU
HighLevel Inc.	USA	Betrieb von Teilbereichen der Plattform einschließlich Hosting Automatisierungs und Kommunikationsfunktionen	USA
HubSpot Inc.	USA	CRM System für Marketing Vertrieb und Service Automatisierung	USA / ggf. EU Rechenzentren des Anbieters
Instantly Inc.	USA	E Mail Outreach und Kommunikationsautomatisierung	USA

IONOS SE	Deutschland	Server und Cloud Infrastruktur	Deutschland / EU
LeadConnector	USA	Kommunikations- und Automatisierungsdienste innerhalb der Plattform	USA
LinkedIn Ireland Unlimited Company (LinkedIn Business)	Irland / EU	Social Media Management Unternehmensseiten Werbeanzeigen und Analysefunktionen	EU und internationale LinkedIn Infrastruktur
LinkedIn Ireland Unlimited Company (LinkedIn Campaign Manager)	Irland / EU	Verwaltung Steuerung und Analyse von Werbekampagnen	EU und internationale LinkedIn Infrastruktur
LinkedIn Ireland Unlimited Company (LinkedIn Creator Tool)	Irland / EU	Tools für Creator Inhalte Analyse und Community Management	EU und internationale LinkedIn Infrastruktur
LinkedIn Ireland Unlimited Company (LinkedIn Page Admin Tool)	Irland / EU	Verwaltung von Unternehmensseiten Rollen Berechtigungen und Inhalten	EU und internationale LinkedIn Infrastruktur
Make (Celonis SE / Make.com)	EU	Integrations und Automatisierungsdienste	EU
Mailgun Technologies Inc.	USA	E-Mail-Versanddienst für transaktionale Nachrichten und automatisierte E-Mail-Kommunikation	USA

Meta Platforms Ireland Ltd. (Facebook Studio)	Irland / EU	Social Media Verwaltung Analyse und Content Steuerung	EU und internationale Meta Infrastruktur
Meta Platforms Ireland Ltd. (Meta Business Suite)	Irland / EU	Zentrale Verwaltung von Facebook und Instagram Seiten Nachrichten Inhalten und Anzeigen	EU und internationale Meta Infrastruktur
Meta Platforms Ireland Ltd. (Meta Suite)	Irland / EU	Erweiterte Dienste für Verwaltung Analyse und Werbesteuerung	EU und internationale Meta Infrastruktur
Meta Platforms Ireland Ltd. (Threads)	Irland / EU	Textbasierte Social Media Kommunikation und Community Interaktion	EU und internationale Meta Infrastruktur
n8n GmbH (n8n.io)	Deutschland	Workflow und Prozessautomatisierung	EU
Onepage.io	EU	Landingpage-, Website- und Marketing-Tools zur Erstellung und Verwaltung von Webseiten	EU
OVHcloud	EU (Frankreich)	Europäische Cloud Infrastruktur	EU
Pipedrive OÜ	Estland / EU	CRM System zur Vertriebssteuerung und Pipeline Verwaltung	EU

Pinterest Europe Ltd. (Pinterest)	Irland / EU	Visuelle Social Media Plattform Content Veröffentlichung Reichweitenanalyse und Anzeigen	EU und internationale Pinterest Infrastruktur
Pinterest Europe Ltd. (Pinterest Business Hub)	Irland / EU	Verwaltung von Business Accounts Anzeigenstatistiken und Content Performance	EU und internationale Pinterest Infrastruktur
Reddit Inc.	USA	Community Plattform für Content Diskussion und Reichweitenaufbau	USA
Salesforce Inc.	USA	CRM System für Vertrieb Marketing und Kundenmanagement	USA / EU Rechenzentren des Anbieters
Sentry Inc.	USA	Fehleranalyse und Systemüberwachung	USA / EU (abhängig von gebuchtem Standort)
SendGrid Inc.	USA	Transaktionale E Mails Systembenachrichtigungen und Zustellungsmanagement	USA
Sendinblue GmbH	Deutschland / EU	Transaktionale und Marketing E Mails	EU
Snap Inc.	USA	Social Media Plattform für visuelle Kommunikation Stories und Anzeigen	USA
TikTok Technology Limited (TikTok Business	Irland / EU	Verwaltung von Anzeigen Kampagnen	EU und internationale

Center)		Analyse und Geschäftskonten	TikTok Infrastruktur
TikTok Technology Limited (TikTok Creator Tools)	Irland / EU	Content Erstellung Video Analyse und Community Verwaltung	EU und internationale TikTok Infrastruktur
Twilio Inc.	USA	Kommunikationsdienste für SMS Voice WhatsApp und API basierte Nachrichtenübermittlung	USA / EU je nach Dienst
The Rocket Science Group LLC (Mailchimp)	USA	E Mail Kommunikation und Kampagnen	USA
UptimeRobot Inc.	USA / ggf. international	Verfügbarkeitsüberwachung	Internationale Infrastruktur des Anbieters
X Corp. (ehemals Twitter)	USA	Microblogging Plattform Content Veröffentlichung und Interaktion	USA und internationale X Infrastruktur
Zapier Inc.	USA	Schnittstellen und Automatisierungsdienste	USA
Zoho Corporation Pvt. Ltd.	EU und Drittstaaten	CRM System sowie Geschäfts und Kundenmanagement Anwendungen	EU und weitere Regionen gemäß Zoho Infrastruktur