Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen (der)

Muster GmbH
Musterstraße 5
12345 Musterstadt
muster@muster.de

- nachstehend Auftraggeber genannt -

und der

Coachy OOD
104 Simeonovsko shose Blvd
1700 Sofia, Bulgarien

- nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

Gegenstand und Dauer des Auftrags bestimmen sich vollumfänglich nach den im jeweiligen Hauptvertragsverhältnis gemachten Angaben.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber i.S.v. Art.4 Nr.2 und Art.28 DS-GVO auf Grundlage dieses Auftrags.

2. Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten

Der Umfang, die Art und der Zweck einer etwaigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, die Art der Daten und der Kreis der Betroffenen werden dem Auftragnehmer durch den Auftraggeber gemäß der vom Auftraggeber ausgefüllten Anlage 1 beschrieben, soweit sich das nicht aus dem Vertragsinhalt der in Ziffer 1 beschriebenen Vertragsverhältnisse ergibt.

Der Auftragnehmer wird die vertraglichen Leistungen im Gebiet der Bundesrepublik Deutschland erbringen. Etwaige Unterauftragnehmer erbringen die sie betreffenden Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR).

3. Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO (Art.28 Abs.3 Satz 2 lit.c DS-GVO)

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben (siehe Anlage 2). Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs.3 Satz 2 lit.c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung.

Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Sperrung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Der Auftragnehmer verpflichtet sich zu einer schriftlichen Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 37, 38 DS-GVO ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber auf Anforderung, zum Zweck der direkten Kontaktaufnahme, mitgeteilt.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechen Art. 28 Abs. 3 Satz 2 lit. c, 32 DS-GVO und Anlage 2.
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer setzt Dritte als Dienstleister im Unterauftrag ein. Mit diesen ist jeweils eine Vereinbarung über die Verarbeitung von Daten im Auftrag abgeschlossen. Bei Abschluss des Auftrages sind dies diejenigen Dienstleister, die in Anlage 3 dieser Vereinbarung aufgeführt sind. Die Einschaltung dieser Dienstleister wird durch den Auftraggeber ausdrücklich gestattet. Bei Änderung in Bezug auf die Hinzuziehung oder Ersetzung von weiteren Subunternehmern ergeht hierüber eine Information an den Auftraggeber. Die Änderungen gelten als vom Auftraggeber akzeptiert, wenn dieser nicht innerhalb von 4 Wochen nach Veröffentlichung widerspricht.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann wahlweise erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) und/oder eine geeignete Zertifizierung durch IT- Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Verarbeitungstätigkeit löscht der Auftragsnehmer nach Wahl des Auftraggebers entweder alle personenbezogenen Daten oder gibt sie dem Verantwortlichen zurück, sofern nicht nach dem Unionsrecht oder nach dem anwendbaren Recht eines Mitgliedstaates eine Verpflichtung zur Speicherung der

personenbezogenen Daten besteht oder sich aus jeweiligen vertraglichen Vereinbarungen etwas anderes ergibt. Macht der Auftraggeber von diesem Wahlrecht keinen Gebrauch, gilt die Löschung als vereinbart. Wählt der Auftraggeber die Rückgabe, kann der Auftragsnehmer eine angemessene Vergütung verlangen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Sonstige Vereinbarungen

11.1. Entgelte

Ein Entgelt für diesen Auftrag wird nicht gefordert.

Soweit der Auftraggeber Unterstützung nach Ziffer 4 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten.

Soweit der Auftraggeber nach Ziffer 7 Kontrollrechte ausüben wird, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an einem festzulegenden Stundensatz des für die Betreuung vom Auftragnehmer abgestellten Mitarbeiters.

Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach Ziffer 9, so hat er durch diese Weisung entstehende Kosten zu erstatten.

11.2. Vertragsdauer

Diese Vereinbarung ist abhängig vom Bestand eines Hauptvertragsverhältnisses gemäß Ziffer 1. Die Kündigung oder anderweitige Beendigung des Hauptvertragsverhältnisses gemäß Ziffer 1 beendet gleichzeitig diese Vereinbarung.

Das Recht zur isolierten, außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte konkret für die Vereinbarung bleiben hierdurch unberührt.

Unterschriften

_____ , den _____	Sofia, den 28.03.2023
	
_____	_____
Auftraggeber	Auftragnehmer

Anlage 1 zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO:
Auflistung der personenbezogenen Daten und Zweck ihrer Verarbeitung

Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung der Daten des Auftraggebers sind folgende Datenarten:

- Personenstammdaten (z.B. Vorname, Nachname)
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Statistikdaten (z.B. Abrufe Kurse, Lektionen)

Kategorien der betroffenen Personen

Der Kreis der durch den Umgang mit den Daten Betroffenen umfasst:

- Beschäftigte des Auftraggebers
- Kunden des Auftraggebers

Anlage 2 zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO:
Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

1. Pseudonymisierung

Wie wird die Pseudonymisierung der Daten gewährleistet?

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- Pseudonymisierung mittels einer eindeutigen Identifikationsnummer (ID).
  Diese ID wird im System bei der Erstellung von Protokollierungen verwendet.

2. Verschlüsselung

Wie wird die Verschlüsselung gewährleistet?

Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.

- Nutzung von kryptografischen Tools
- Data Hashing
- Verschlüsselung von Speichermedien
- Verschlüsselung der Kommunikation

3. Fähigkeit der Vertraulichkeit

Wie wird die Fähigkeit der Vertraulichkeit der Daten dauerhaft gewährleistet?

Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.

- Sicherheitstüren und/oder -fenster
- Alarmanlage
- Spezielle Schutzvorkehrungen für den Serverraum
- Individueller Log-In und Kennwortverfahren
- Zusätzlicher Log-In für bestimmte Anwendungen
- Automatische Sperrung der Clients (Zeitablauf)
- Verwaltung von Berechtigungen
- Dokumentationen von Berechtigungen
- Verschlüsselung von Systemen
- Verschlüsselung von Kommunikation
- Verschlüsselung von Datenträgern
- VPN (Virtual Private Network)
- Gesichertes WLAN
- SSL-Verschlüsselung bei Web-Access

4. Fähigkeit der Integrität

Wie wird die Fähigkeit der Integration der Daten dauerhaft gewährleistet?

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, das Daten vollständig und unverändert sind.

- Maßnahmen werden ergriffen, die die Beschädigung/Veränderung der geschützten Daten während der Verarbeitung oder Übertragung verhindern
- Verwendung von Zugriffsrechten
- Systemseitige Protokollierungen

- Funktionelle Verantwortlichen

5. Fähigkeit der Verfügbarkeit

Wie wird die Fähigkeit der Verfügbarkeit der Daten dauerhaft gewährleistet?

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

- Backup und Recovery-Konzept mit täglichen Sicherungen aller relevanten Daten
- Spiegeln von Festplatten
- Unterbrechungsfreie Stromversorgung (USV)
- Virenschutz / Firewall
- Monitoring aller relevanten Server
- Notfallplan
- Klimaanlage
- Alarmanlage

6. Fähigkeit der Belastbarkeit

Wie wird die Fähigkeit der Belastbarkeit der Daten dauerhaft gewährleistet?

Systeme sind belastbar, wenn sie so widerstandfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.

- Penetrationstests

7. Wiederherstellbarkeit der Verfügbarkeit und des Zugangs

Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?

- Backup und Recovery-Konzept mit täglichen Sicherungen aller relevanten Daten
- Unterbrechungsfreie Stromversorgung (USV)
- Notfallplan
- Vertreterregelungen

8. Verfahren zur regelmäßigen Überprüfung

Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

- Es existiert eine festgelegte Prüfroutine
- Prüfberichte werden evaluiert
- Implementierung von Verbesserungsvorschlägen

9. Unrechtmäßiger Zugang zu personenbezogenen Daten

Wie wird verhindert, dass Datenverarbeitungssystem von Unbefugten genutzt werden können?

- Individueller Log-In mit Kennwortverfahren
- Zusätzlicher Log-In für bestimmte Anwendungen
- Automatische Sperrung der Clients (Zeitablauf)
- Verwaltung von Berechtigungen
- Dokumentationen von Berechtigungen
- Verschlüsselung von Systemen

10. Verarbeitung personenbezogener Daten nur nach Anweisung

Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?

- Mitarbeiter sind zu Verhaltensregeln verpflichtet

- Implementierung unternehmensinterner Datenschutz-Richtlinien
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Schulungen aller zugriffsberechtigter Mitarbeiter
- Bestimmungen von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag

Anlage 3 zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO:
Unterauftragsnehmerliste

1. Hetzner Online GmbH, Deutschland
   Zweck: Hosting der Coachy Server Infrastruktur
   Ort der Leistungserbringung: Serverstandort Deutschland

2. D10 Solutions AG, Deutschland
   Zweck: Technische Unterstützung und allgemeine Betreuung
   Ort der Leistungserbringung: Deutschland

3. BUNNYWAY, informacijske storitve d.o.o
   Zweck: Content Delivery Network
   Ort der Leistungserbringung: Serverstandorte Deutschland und Schweden

4. Amazon AWS
   Zweck: Content Delivery Network
   Orte der Leistungserbringung: Serverstandorte Deutschland und Irland