Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

zwischen

_____

_____

_____

Verantwortlicher – nachfolgend „Auftraggeber“ genannt

und der

Rahn Datenschutz GmbH

Heinz-Nixdorf-Straße 12

41179 Mönchengladbach

Auftragsverarbeiter – nachfolgend „Auftragnehmer“ genannt

1. Gegenstand und Dauer des Auftrags

1.1. Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung und der Beschreibung unter 2.1.

1.2. Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftrags

2.1. Auftragsgegenstand im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers sind nachfolgend beschrieben:

Der Auftragnehmer stellt ein Datenschutz-Management-Konzept in Form eines Online-Portals mit Vorlagen zur Verfügung. Zur Nutzung der Vorlagen muss sich der Auftraggeber kostenpflichtig registrieren und kann im Anschluss fünf weiteren Mitarbeitern, durch Eingabe von: Name, Vorname und E-Mail-Adresse zur Mitarbeit auf das Portal einladen. Zusätzlich kann der Auftraggeber seine Verarbeitungen über eine Eingabemaske im Online-Portal erfassen und hinterlegen, um daraus benötigte Reports für die Umsetzung eines eigenen Datenschutz-Management-Systems zu erstellen.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau ist hierbei festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art.

45 Abs. 3 DSGVO) oder wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO), möglich ist auch die Festlegung durch Standardvertragsklauseln (Art. 46 Abs. 2 lit. c und d DSGVO) oder genehmigten Verhaltensregeln (Art 46 Abs. 2 lit. e i.V.m. 40 DSGVO), durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO) kann ebenfalls ein Nachweis erfolgen.

2.2. Die Art der verwendeten personenbezogenen Daten (Datenkategorien) erstreckt sich auf: Name und Kontaktdaten von Mitarbeitern, sowie alles, was üblicherweise bei der Dokumentation von Verarbeitungen anfällt (Name und Kontaktdaten von Mitarbeitern, Dienstleistern, etc.) und Logfiles. Die Kategorien betroffener Personen sind üblicherweise: Mitarbeiter; Dienstleister; Kunden, Lieferanten.

3. Technische und organisatorische Maßnahmen

3.1. Der Auftragnehmer hat die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und dem Auftraggeber auf Anfrage zur Prüfung zu übergeben.

3.2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen.

3.3. Die technischen und organisatorischen Maßnahmen werden weiterentwickelt und den Anforderungen und dem aktuellen Stand der Technik angepasst. Das Sicherheitsniveau der festgelegten Maßnahmen darf dadurch aber nicht herabgesetzt oder unterschritten werden. Alle Änderungen sind nachweislich zu dokumentieren.

4. Berichtigung, Löschung und Einschränkung von personenbezogenen Daten

4.1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, 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.

4.2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Daten Portabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer gewährleistet, neben den durch diesen Vertrag und das Gesetz festgelegte Pflichten, insbesondere die Einhaltung folgender Vorgaben:

- Der Auftragnehmer hat schriftlich einen Datenschutzbeauftragten zu benennen, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt, sofern die gesetzliche Verpflichtung besteht. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

- Zur Durchführung der Arbeiten werden nur Beschäftigte eingesetzt, welche mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden und die auf die Vertraulichkeit verpflichtet 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. Der Auftragnehmer stellt die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29 und 32 Abs. 4 DSGVO sicher.

- Der Auftragnehmer gewährleistet die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c und Art. 32 DSGVO.

- Der Auftragnehmer unterstützt den Auftraggeber auf Anfrage bei der Erfüllung der Betroffenenrechte nach Art. 12-22 DSGVO nach seinen Möglichkeiten.

- Der Auftragnehmer hat den Auftraggeber unverzüglich darüber zu informieren, wenn es durch eine Aufsichtsbehörde zu Kontrollhandlungen oder anderen Maßnahmen kommt, welche sich auf diesen Vertrag beziehen. Dies gilt gleichfalls, sofern Maßnahmen anderer Behörden die Verarbeitung personenbezogener Daten des Auftraggebers betreffen. Ferner unterstützt der Auftragnehmer den Auftraggeber bei oben genannten Szenarien, welche beim Auftraggeber auftreten, sofern sie diesen Auftrag betreffen, im Rahmen seiner Möglichkeiten. Auf Anfrage verpflichten sich Auftraggeber und Auftragnehmer zur Zusammenarbeit mit der Aufsichtsbehörde, um der Erfüllung Ihrer Aufgaben gerecht zu werden.

6. Unterauftragnehmer

6.1. Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt, sind nicht als Unterauftragnehmer angesehen Als Unterauftragsverhältnisse sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Der Auftraggeber stimmt der Beauftragung, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO, den in **Anlage 1** genannten Unterauftragnehmern zu.

6.2. Der Auftragnehmer informiert den Auftraggeber laut Art. 28 Abs. 2 DSGVO schriftlich oder in elektronischer Textform über jede beabsichtigte Änderung in Bezug auf die Ersetzung bisheriger oder hinzuziehen neuer Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen diese Änderungen begründeten Einspruch zu erheben.

6.3. Sämtliche hier getroffenen vertraglichen Regelungen sind auch den weiteren Unterauftragnehmern aufzuerlegen.

6.4. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

6.5. Unterauftragnehmer dürfen personenbezogene Daten des Auftraggebers erst erhalten und tätig werden, wenn alle Voraussetzungen für eine Unterbeauftragung erfüllt sind.

7. Kontrollrechte des Auftraggebers

7.1. Der Auftraggeber hat das Recht Stichprobenkontrollen durchzuführen, um sich von der Einhaltung dieser Vereinbarung durch den Auftragnehmer zu überzeugen. Diese Kontrollen sind grundsätzlich rechtzeitig anzumelden.

7.2. Der Auftragnehmer sichert dem Auftraggeber zu, dass er sich von der Einhaltung der Pflichten nach Artikel 28 DSGVO überzeugen kann, nach auf Aufforderungen die erforderlichen Auskünfte erteilt und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachweist.

7.3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO oder eine andere geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits oder aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Datenschutzauditoren, Qualitätsauditoren).

8. Mitteilung bei Verstößen des Auftragnehmers

8.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören 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. Der Auftragnehmer hat die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden. Ebenso hat der Auftragnehmer dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen, insbesondere die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung oder die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8.2. 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

9.1. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich schriftlich (mind. Textform).

9.2. 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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

10.1. Im Rahmen der Gewährleistung einer ordnungsgemäßen Datenverarbeitung dürfen Sicherheitskopien erstellt werden. Daten die zur Einhaltung gesetzlicher Aufbewahrungsfristen erforderlich sind dürfen vorgehalten werden. Duplikate oder Kopien darüber hinaus dürfen nicht ohne Kenntnis des Auftraggebers erstellt werden.

10.2. Der Auftraggeber erhält nach Abschluss der vereinbarten Arbeiten, Beendigung der Vereinbarung oder vorher durch Aufforderung sämtliche Datenbestände, sowie im Zusammenhang mit der Auftragsverarbeitung stehende Unterlagen, Verarbeitungs- oder Nutzungsergebnisse zurück. Bei Zustimmung des Auftraggebers kann die Rückgabe auch durch eine datenschutzgerechte Vernichtung mit Nachweis ersetzt werden.

10.3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11. Schlussbestimmungen

11.1. Für Nebenabreden gilt grundsätzlich Schriftform.

11.2. Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Gez. Sven Rahn Geschäftsführer Rahn Datenschutz GmbH

[Diese Vereinbarung ist ohne Unterschrift gültig]

Stand: 08.08.2024

Anlage 1: Unterauftragsverhältnisse

Unterauftragnehmer	Anschrift/Land	Leistung
compleasy UG (haftungsbeschränkt)	An der Müllerwiese 10 51069 Köln	Bereitstellung der Anwendung