Anlage zur AGB – Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

TYCT GmbH
Richard-Wagner-Straße 65
82049 Pullach i. Isartal
(im Folgenden „Auftragsverarbeiter“ oder „TYCT“)

und

dem Kunden, der die Plattform tyct.io gemäß den AGB nutzt
(im Folgenden „Verantwortlicher“)

– gemeinsam nachfolgend auch „Parteien“ genannt –

1. Gegenstand und Dauer der Verarbeitung
    a. Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Nutzung der Plattform tyct.io durch den Verantwortlichen.
    b. Die Verarbeitung erfolgt ausschließlich zur Erfüllung der im Hauptvertrag (AGB von TYCT GmbH) vereinbarten Leistungen.
    c. Diese Vereinbarung zur Auftragsverarbeitung (Anlage 1) ist Bestandteil des Vertrags.
    d. Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags. Sie endet automatisch mit dessen Beendigung.
2. Art und Zweck der Verarbeitung
    a. TYCT verarbeitet personenbezogene Daten ausschließlich zur Bereitstellung, Wartung, Sicherung und Weiterentwicklung der SaaS-Plattform „tyct.io“.
    b. Zwecke der Verarbeitung sind insbesondere:
        i. Bereitstellung von Nutzerkonten und Zugriffsverwaltung
        ii. Speicherung und Verwaltung von Kunden- und Projektdaten
        iii. Kommunikationsmanagement (z. B. Benachrichtigungen, Systemmeldungen)
        iv. Protokollierung und Fehleranalyse
        v. Sicherheits- und Leistungsoptimierung
3. Art der personenbezogenen Daten und Kategorien betroffener Personen
    a. Art der verarbeiteten Daten:
        i. Bestandsdaten (Name, Firma, E-Mail-Adresse, Kontaktdaten)
        ii. Nutzungsdaten (Login-Daten, Rollen, Berechtigungen)
        iii. Kommunikationsdaten (Nachrichten, Supportanfragen)
        iv. Logdaten und technische Metadaten (IP-Adresse, Browser, Zeitstempel)
    b. Kategorien betroffener Personen:

   i. Mitarbeiter, Kunden, Lieferanten und Geschäftspartner des Verantwortlichen
   ii. Endnutzer, die durch den Verantwortlichen Zugriff auf die Plattform erhalten

4. Rechte und Pflichten des Verantwortlichen
   a. Der Verantwortliche ist für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich.
   b. Der Verantwortliche ist berechtigt, Weisungen hinsichtlich Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Weisungen sind schriftlich oder in Textform zu erteilen.
   c. Erteilt der Verantwortliche eine Weisung, die nach Ansicht des Auftragsverarbeiters gegen Datenschutzrecht verstößt, informiert TYCT den Verantwortlichen unverzüglich. Die Umsetzung wird bis zur Klärung ausgesetzt.
5. Pflichten des Auftragsverarbeiters (TYCT)
   TYCT verpflichtet sich:
   a. personenbezogene Daten ausschließlich im Rahmen der dokumentierten Weisungen des Verantwortlichen zu verarbeiten;
   b. die zur Verarbeitung befugten Mitarbeiter und sonstigen Beschäftigten auf Vertraulichkeit zu verpflichten;
   c. die gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (TOM) zu treffen;
   d. den Verantwortlichen unverzüglich zu informieren, wenn eine Verletzung des Schutzes personenbezogener Daten („Data Breach“) bekannt wird;
   e. den Verantwortlichen bei der Erfüllung seiner Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung, Datenschutz-Folgenabschätzung) zu unterstützen;
   f. nach Beendigung der Auftragsverarbeitung sämtliche personenbezogenen Daten entweder zu löschen oder auf Wunsch an den Verantwortlichen herauszugeben.
6. Technische und organisatorische Maßnahmen (TOM)
   TYCT hat geeignete technische und organisatorische Maßnahmen getroffen, um personenbezogene Daten vor unbefugtem Zugriff, Verlust, Zerstörung oder Veränderung zu schützen. Diese umfassen insbesondere:
   a. Zugriffsbeschränkung (Passwortschutz, 2FA, Rollenkonzept)
   b. Verschlüsselung von Daten während der Übertragung (TLS/SSL)
   c. Firewall- und Intrusion-Detection-Systeme
   d. Regelmäßige Backups und Wiederherstellungstests
   e. Protokollierung von Zugriffs- und Administrationsvorgängen
   f. Datenschutzfreundliche Standardeinstellungen („Privacy by Default“)

   Eine aktuelle TOM-Liste ist auf Anfrage erhältlich.
7. Unterauftragsverhältnisse
   a. TYCT ist berechtigt, Unterauftragsverarbeiter einzusetzen. Eine Liste der aktuellen Unterauftragsverarbeiter ist auf Anfrage erhältlich bzw. unter https://tyct.io/datenschutz einsehbar.

b. TYCT informiert den Verantwortlichen über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern. Der Verantwortliche kann der Änderung aus wichtigem Grund widersprechen. Der Widerspruch ist innerhalb von 14 Tagen nach Mitteilung in Textform zu erheben.
c. TYCT verpflichtet Unterauftragsverarbeiter vertraglich zur Einhaltung der in dieser Vereinbarung festgelegten Pflichten.
d. Der Auftragnehmer ist berechtigt, zur Einholung von Unbedenklichkeitsbescheinigungen gesetzlich vorgesehene Übermittlungsportale (z. B. ITSG / SV.net) zu nutzen.
Diese Systeme gelten nicht als freie Subunternehmer, sondern als rechtlich verpflichtende Kommunikationsschnittstellen gemäß § 28a SGB IV.
Die Nutzung erfolgt ausschließlich zweckgebunden und nach Maßgabe der DSGVO.
e. Automatisierte Abfrage und Validierung von Unbedenklichkeitsbescheinigungen bei Sozialversicherungsträgern und Behörden im Auftrag des Verantwortlichen
f. Aggregation von Beitrags- und Meldedaten zur Erstellung von Risikoprofilen (Scoring).

8. Kontrollrechte des Verantwortlichen
   a. Der Verantwortliche ist berechtigt, die Einhaltung dieser Vereinbarung regelmäßig zu überprüfen, insbesondere durch Stichproben, Fragebögen oder Audits.
   b. TYCT verpflichtet sich, dem Verantwortlichen alle erforderlichen Auskünfte zu erteilen und Nachweise (z. B. Zertifikate, Sicherheitsberichte) zur Verfügung zu stellen.
   c. Audits vor Ort sind mit angemessener Ankündigungsfrist (mind. 14 Tage) durchzuführen und dürfen den Betriebsablauf nicht unangemessen stören.
9. Mitteilungspflichten bei Datenschutzverstößen
   TYCT informiert den Verantwortlichen unverzüglich, sobald eine Verletzung des Schutzes personenbezogener Daten festgestellt wird.
   Die Mitteilung enthält mindestens:
   a. Art des Verstoßes
   b. betroffene Datensätze und Personen
   c. mögliche Folgen
   d. ergriffene oder geplante Abhilfemaßnahmen
10. Löschung und Rückgabe von Daten
    Nach Beendigung der Auftragsverarbeitung:
    a. werden alle personenbezogenen Daten innerhalb von 30 Tagen gelöscht, sofern keine gesetzliche Aufbewahrungspflicht besteht, oder
    b. auf schriftliche Anforderung an den Verantwortlichen in einem gängigen Format übergeben.

    Nach erfolgter Löschung wird dies schriftlich bestätigt.
11. Haftung
    Für Schäden, die durch Verstöße gegen diese Vereinbarung entstehen, gelten die Haftungsregelungen des Hauptvertrags (AGB).

Die Regelungen der Art. 82 ff. DSGVO bleiben hiervon unberührt.

12. Schlussbestimmungen
    a. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.
    b. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt.
    c. Diese Vereinbarung kann elektronisch abgeschlossen werden (Art 28 Abs. 9 DSGVO).
    d. Es gilt deutsches Recht. Gerichtsstand ist München.