Vertrag zur Auftragsverarbeitung

zwischen

-nachstehend Auftraggeber oder Verantwortlicher genannt –

und

I TRUST IT Computer Technik & Handel
Langer Brink 33, D-33790 Halle Westfalen
-nachstehend Auftragnehmer oder Auftragsverarbeiter genannt –

§ 1 Gegenstand und Dauer des Auftrags

1.1 Der Auftragnehmer führt die im Anhang 1 beschriebenen Dienstleistungen für den Auftraggeber durch.

1.2 Da der Auftragnehmer in Erfüllung seiner Aufgaben, Daten im Auftrag, nach Weisung und im Interesse des Auftraggebers verarbeitet bzw. ein Zugriff auf personenbezogene Daten bei der Auftragserfüllung nicht ausgeschlossen werden kann, erfolgt die Dienstleistung als Auftragsdatenverarbeitung, bzw. Auftragsdatenverwaltung gemäß der jeweils geltenden datenschutzrechtlichen Rechtsgrundlagen.

1.3 Dieser Vertrag tritt, solange keine anderweitigen Regelungen vereinbart wurden, mit Unterzeichnung beider Parteien in Kraft und gilt, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten im Auftrag verarbeitet.

§ 2 Umfang, Art und Zweck der Datenverarbeitung, Datenarten und Betroffenenkreis

Umfang, Art und Zweck der Datenverarbeitung, die Art der Daten sowie der Kreis der Betroffenen werden in Anhang 1 beschrieben.

§ 3 Technische und organisatorische Maßnahmen

3.1 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. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen als Anlage 3 Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

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 derVertraulichkeit, 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
[Einzelheiten in Anlage 1].

3.3 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, Einschränkung und Löschung von 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, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

5.1 Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau … bestellt/***Trifft nicht zu!***

5.2 Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO.

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 Datenausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

5.3 Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].

5.4 Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5.5 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.

5.6 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.

5.7 Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

5.8 Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

§ 6 Unterauftragsverhältnisse

6.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung bezeichnen. Nicht hierzu gehören 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. 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.

6.2 Der Auftragnehmer darf Unterauftragnehmer nur beauftragen, wenn durch einen schriftlichen Vertrag sichergestellt wurde, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Unterauftragnehmern gelten und der Auftraggeber hiervon informiert wird.

6.3 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

6.4 Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers ist nur zulässig, wenn

a) der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt,

b) der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftraggeber schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

c) der Unterbeauftragte eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

6.5 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen im Sinne des §6.4 für eine Unterbeauftragung gestattet.

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

6.7 Zum Zeitpunkt der Vertragsunterzeichnung beauftragte Unterauftragnehmer werden ebenfalls in Anhang 2 einschließlich der Verarbeitungsstandorte und der Art der Dienstleistung dokumentiert. Die in Anhang 2 genannten Unterauftragnehmer gelten als von Anfang an rechtmäßig beauftragt im Sinne von § 6.1 und 6.2, sofern die Umsetzung der dort genannten Voraussetzungen durch den Auftragnehmer gewährleistet wird.

§ 7 Kontrollrechte des Auftraggebers

7.1 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.

7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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.

7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVOaktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen wie z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

§ 8 Mitteilung bei Verstößen des Auftragnehmers

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32

bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten,

Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige

Konsultationen. Hierzu gehören u.a.

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

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an denAuftraggeber zu melden

c) 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

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) 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 (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 solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 10 Löschung und Rückgabe von personenbezogenen Daten

10.1 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.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit demAuftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 11 Schlussbestimmungen

11.1 Die Parteien sind sich darüber einig, dass diese Vereinbarung mit sofortiger Wirkung wirksam wird. Sofern in dieser Vereinbarung ausdrücklich auf die Bestimmungen der DSGVO Bezug genommen wird, gelten bis zur Wirksamkeit die entsprechenden Bestimmungen des BDSG.

11.2 Gerichtsstand für sämtliche Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist Gütersloh, sofern nicht gesetzlich zwingend ein anderer Gerichtsstand vorgeschrieben ist,

11.3 Sollte eine Bestimmung dieses Vertrags oder eine später in ihn aufgenommene Bestimmung ganz oder teilweise nichtig sein oder werden oder sollte sich eine Lücke in diesem Vertrag herausstellen, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An Stelle der nichtigen Bestimmung oder zur Ausfüllung derLücke gilt mit Rückwirkung diejenige wirksame und durchführbare Regelung als vereinbart die rechtlich und wirtschaftlich dem am nächsten kommt, wenn sie diesen Punkt beim Abschluss des Vertrages bedacht hätten. Beruht die Nichtigkeit einer Bestimmung auf einem darin festgelegten Maß der Leistung oder der Zeit (Frist oder Termin), so gilt die Bestimmung mit einem dem ursprünglichen Maß am nächsten kommenden rechtlichen zulässigen Maß als vereinbart.

Ort, Datum	Ort, Datum
Unterschrift/Stempel	Unterschrift/Stempel
Auftraggeber	Auftragnehmer

Anhang 1:
Auflistung der beauftragten Dienstleistungen (Umfang, Art, Zweck der Erhebung, Verarbeitung, Nutzung von Daten, Art der Daten, Kreis der Betroffenen)

Dienstleistungen	IT-Technik, Softwaresupport …
Datenart	Alle Daten, die in der Software JTL vom Auftraggeber gespeichert werden. Datenarten z.B. Personenstammdaten, Einsatzzeiten und Einsatzorte, Gehaltsabrechnungen der Gehalts-/Heuerempfänger, Nutzungsdaten der Angestellten.
Kreis der Betroffenen	Kunden, Mitarbeiter der Kunden (Gehalts-/Heuerempfänger) und Beschäftigte des Auftraggebers.

Umfang, Art, Zweck der Erhebung, Verarbeitung, Nutzung der Daten

Die Daten werden durch den Auftragnehmer ausschließlich für Supportanfragen des Auftraggebers genutzt. Nur in Ausnahmefallen ist hierbei ein Zugriff auf personenbezogene Daten erforderlich.

Der Auftragnehmer wird ausdrücklich in jedem einzelnen Fall darauf hinweisen, ob und in welchem Umfang ein Datenzugriff erforderlich sein sollte. Eine proaktive Daten Übermittlung durch den Auftraggeber ist nicht geboten. Ein Zugriff auf Daten erfolgt zumeist mittels einer Fernwartungssoftware (z.B. Team Viewer) und ausschließlich mit Kenntnis und Willen des Auftraggebers.

Eine Kopie (gesamt oder teilweise) der Daten des Auftraggebers durch den Auftragnehmer auf die Systeme des Auftragnehmers ist nicht gestattet. Sollte dies in speziellen Fällen erforderlich sein, ist die schriftliche Zustimmung (unter Angabe von Gründen, Umfang, Speicherdauer und verantwortlichen Mitarbeiter beim Auftragnehmer) des Auftraggebers erforderlich.

Anhang 2:
Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

Unterauftragnehmer (Name, Rechtsform, Sitz der Gesellschaft)	Verarbeitungsstandort	Art der Dienstleistung

Anhang 3:
Technische und organisatorische Maßnahmen (TOM)