Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (Art. 28 DSGVO)

zwischen

_____ (Firma, Anschrift) – „Verantwortlicher“ –

und

Pfeifer IT-Systemhaus, Inhaber Jakob Pfeifer, Friesenstolzring 1, 26632 Ihlow – „Auftragsverarbeiter“ –

§ 1 Gegenstand und Dauer

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten für den Verantwortlichen, soweit dies zur Erfüllung des Vertrags über Deichwerk Faktura und/oder IT HUB („Hauptvertrag“) nötig ist. Dieser Vertrag regelt die Rechte und Pflichten der Parteien dabei.
2. Dieser Vertrag gilt, solange der Auftragsverarbeiter Daten des Verantwortlichen verarbeitet, also für die Laufzeit des Hauptvertrags und bis zur vollständigen Löschung oder Rückgabe der Daten.
3. Der Verantwortliche darf diesen Vertrag und den Hauptvertrag fristlos kündigen, wenn der Auftragsverarbeiter schwerwiegend gegen diesen Vertrag oder gegen Datenschutzvorschriften verstößt.

§ 2 Art, Zweck und Umfang der Verarbeitung

Art und Zweck der Verarbeitung, die Art der Daten und die Kategorien betroffener Personen stehen in Anlage 1. Der Auftragsverarbeiter verarbeitet die Daten nur für diese Zwecke und nicht für eigene Zwecke.

§ 3 Weisungen

1. Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen. Das gilt auch für Übermittlungen in ein Land außerhalb der EU oder des EWR. Der Hauptvertrag, dieser Vertrag und die Einstellungen, die der Verantwortliche in der Software vornimmt, sind Weisungen.
2. Einzelne Weisungen erteilt der Verantwortliche in Textform. Mündliche Weisungen bestätigt er unverzüglich in Textform.
3. Ist der Auftragsverarbeiter durch das Recht der EU oder eines Mitgliedstaats zu einer anderen Verarbeitung verpflichtet, teilt er dies dem Verantwortlichen vorher mit, soweit das Recht eine solche Mitteilung nicht verbietet.
4. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, weist er den Verantwortlichen unverzüglich darauf hin. Er darf die Ausführung aussetzen, bis der Verantwortliche die Weisung bestätigt oder ändert.
5. Weisungen, die über die vereinbarte Leistung hinausgehen, darf der Auftragsverarbeiter nach dem Stundensatz des Hauptvertrags berechnen.

§ 4 Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere dafür, dass er die Daten erheben und dem Auftragsverarbeiter überlassen darf, sowie für die Wahrung der Rechte der betroffenen Personen.
2. Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 5 Vertraulichkeit

Der Auftragsverarbeiter setzt für die Verarbeitung nur Personen ein, die sich zur Vertraulichkeit verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen und die mit den für sie wichtigen Regeln des Datenschutzes vertraut sind. Die Pflicht zur Vertraulichkeit besteht nach Ende dieses Vertrags fort.

§ 6 Sicherheit der Verarbeitung

1. Der Auftragsverarbeiter trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Sie sind in Anlage 2 beschrieben.

2. Der Auftragsverarbeiter darf die Maßnahmen an den Stand der Technik anpassen und durch gleichwertige ersetzen. Das Schutzniveau der Anlage 2 darf er dabei nicht unterschreiten. Wesentliche Änderungen dokumentiert er und teilt sie dem Verantwortlichen mit.

§ 7 Ort der Verarbeitung

Die Verarbeitung findet in der Europäischen Union oder im Europäischen Wirtschaftsraum statt. Eine Verlagerung in ein anderes Land ist nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und der Auftragsverarbeiter den Verantwortlichen vorher nach § 8 informiert hat.

§ 8 Unterauftragsverarbeiter

1. Der Verantwortliche genehmigt allgemein, dass der Auftragsverarbeiter weitere Auftragsverarbeiter einsetzt. Die bei Vertragsschluss eingesetzten stehen in Anlage 3.
2. Will der Auftragsverarbeiter einen weiteren Auftragsverarbeiter neu einsetzen oder einen ersetzen, informiert er den Verantwortlichen mindestens 30 Tage vorher in Textform. Der Verantwortliche kann innerhalb von 14 Tagen nach Zugang aus wichtigem datenschutzrechtlichen Grund Einspruch erheben. Finden die Parteien keine Lösung, darf der Verantwortliche den Hauptvertrag zum Zeitpunkt der Änderung kündigen.
3. Der Auftragsverarbeiter verpflichtet jeden weiteren Auftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten, die in diesem Vertrag festgelegt sind, insbesondere auf hinreichende technische und organisatorische Maßnahmen.
4. Erfüllt ein weiterer Auftragsverarbeiter seine Datenschutzpflichten nicht, haftet der Auftragsverarbeiter dem Verantwortlichen dafür.
5. Keine Unterauftragsverarbeitung sind Nebenleistungen ohne Zugriff auf die Daten des Verantwortlichen im Auftrag, etwa Telekommunikation, Post und Transport oder Bankdienste.

§ 9 Rechte der betroffenen Personen

1. Wendet sich eine betroffene Person mit einem Antrag nach Art. 15 bis 22 DSGVO an den Auftragsverarbeiter, leitet er den Antrag unverzüglich an den Verantwortlichen weiter. Er beantwortet ihn nicht selbst, außer der Verantwortliche weist ihn dazu an.
2. Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, solche Anträge zu erfüllen, insbesondere durch Auskunft, Berichtigung, Löschung und Export der Daten.

§ 10 Weitere Unterstützung

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm vorliegenden Informationen bei dessen Pflichten aus Art. 32 bis 36 DSGVO, also bei der Sicherheit der Verarbeitung, bei Meldungen von Datenschutzverletzungen, bei Datenschutz-Folgenabschätzungen und bei Konsultationen der Aufsichtsbehörde.

§ 11 Verletzungen des Schutzes personenbezogener Daten

1. Wird dem Auftragsverarbeiter eine Verletzung des Schutzes der Daten des Verantwortlichen bekannt, meldet er sie dem Verantwortlichen unverzüglich, spätestens innerhalb von 48 Stunden.
2. Die Meldung enthält, soweit bekannt: die Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen, die ergriffenen und vorgeschlagenen Maßnahmen und eine Kontaktstelle. Fehlende Angaben reicht er unverzüglich nach.
3. Der Auftragsverarbeiter ergreift unverzüglich die nötigen Maßnahmen, um die Daten zu sichern und Folgen für die betroffenen Personen zu mindern.
4. Meldungen an die Aufsichtsbehörde und an betroffene Personen gibt der Verantwortliche ab.

§ 12 Nachweise und Kontrollen

1. Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die nötig sind, um die Einhaltung der Pflichten aus Art. 28 DSGVO und aus diesem Vertrag nachzuweisen.
2. Der Verantwortliche darf die Einhaltung selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer kontrollieren, auch vor Ort. Der Auftragsverarbeiter ermöglicht die Kontrolle und wirkt daran mit. Der Prüfer darf kein Wettbewerber des Auftragsverarbeiters sein.

3. Kontrollen vor Ort kündigt der Verantwortliche in der Regel 14 Tage vorher an. Sie finden zu den üblichen Geschäftszeiten statt und stören den Betrieb nicht mehr als nötig. Daten anderer Kunden bleiben dabei geschützt. Bei einem konkreten Anlass, etwa nach einer Datenschutzverletzung, ist eine kürzere Ankündigung zulässig.
4. Unterstützung bei Kontrollen, die über einen halben Arbeitstag im Kalenderjahr hinausgeht, darf der Auftragsverarbeiter nach dem Stundensatz des Hauptvertrags berechnen. Das gilt nicht, wenn die Kontrolle durch einen Verstoß des Auftragsverarbeiters veranlasst war oder einen solchen ergibt.
5. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen einer Aufsichtsbehörde, soweit sie diesen Auftrag betreffen.

§ 13 Löschung und Rückgabe

1. Nach Ende des Hauptvertrags gibt der Auftragsverarbeiter dem Verantwortlichen nach dessen Wahl alle Daten zurück oder löscht sie. Ohne andere Weisung löscht er sie 30 Tage nach Vertragsende; bis dahin kann der Verantwortliche sie exportieren.
2. Kopien in Datensicherungen werden mit Ablauf der Aufbewahrungszeit der Sicherung überschrieben und bis dahin nicht mehr verwendet.
3. Die Löschung unterbleibt, soweit das Recht der EU oder eines Mitgliedstaats den Auftragsverarbeiter zur Speicherung verpflichtet.
4. Auf Wunsch bestätigt der Auftragsverarbeiter die Löschung in Textform.

§ 14 Haftung

1. Gegenüber betroffenen Personen haften die Parteien nach Art. 82 DSGVO.
2. Zwischen den Parteien gelten die Haftungsregeln des Hauptvertrags, soweit dieser Vertrag nichts anderes bestimmt.

§ 15 Ansprechpartner für den Datenschutz

Der Auftragsverarbeiter ist gesetzlich nicht verpflichtet, einen Datenschutzbeauftragten zu benennen. Ansprechpartner für den Datenschutz ist der Inhaber, Jakob Pfeifer, info@pfeifer-systemhaus.de, Telefon 04928 8489052. Der Verantwortliche nennt seinen Ansprechpartner: _____ (Name, E-Mail).

§ 16 Schlussbestimmungen

1. In Fragen des Datenschutzes geht dieser Vertrag dem Hauptvertrag und den Allgemeinen Geschäftsbedingungen vor.
2. Sind die Daten des Verantwortlichen beim Auftragsverarbeiter durch Pfändung, Beschlagnahme, ein Insolvenzverfahren oder andere Maßnahmen Dritter gefährdet, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich und weist die Dritten darauf hin, dass die Daten dem Verantwortlichen zustehen.
3. Änderungen und Ergänzungen dieses Vertrags und seiner Anlagen bedürfen der Textform. § 8 Absatz 2 bleibt unberührt.
4. Ist eine Bestimmung unwirksam, bleiben die übrigen wirksam.
5. Die Anlagen 1 bis 3 sind Bestandteil dieses Vertrags.

Ort, Datum: _____ Verantwortlicher: _____

Ort, Datum: _____ Auftragsverarbeiter: _____

Anlage 1 – Beschreibung der Verarbeitung

Nicht gebuchte Produkte werden gestrichen.

	IT HUB	Deichwerk Faktura
Gegenstand	Betrieb und Pflege des IT-Betriebshandbuchs des Verantwortlichen	Betrieb beim Anbieter: Bereitstellung des Programms samt Datensicherung. Betrieb beim Kunden: nur Support und Fernwartung mit möglichem Einblick in die Daten

	IT HUB	Deichwerk Faktura
Betroffene Personen	Beschäftigte und Ansprechpartner des Verantwortlichen, Ansprechpartner seiner Dienstleister	Kunden, Interessenten und Lieferanten des Verantwortlichen und deren Ansprechpartner; Beschäftigte des Verantwortlichen
Art der Daten	Name, dienstliche E-Mail-Adresse und Telefonnummer, Abteilung, Standort, zugeordnete Geräte, Konten und Berechtigungen, Anmeldeprotokolle	Name, Anschrift, Kontaktdaten, Angebots-, Auftrags-, Rechnungs- und Zahlungsdaten, Bankverbindung; bei Zeiterfassung: Arbeitszeiten, Pausen, Urlaub und andere Abwesenheiten, Anmeldeprotokolle
Besondere Kategorien (Art. 9 DSGVO)	keine	Krankheitstage als Abwesenheit, ohne Diagnose
Art der Verarbeitung	Speichern, Anzeigen, Ändern, Sichern, Löschen; Abgleich mit Gerätedaten aus dem Netzwerk des Verantwortlichen, soweit eingerichtet	Speichern, Anzeigen, Ändern, Sichern, Löschen; Versand von Dokumenten per E-Mail, soweit der Verantwortliche ihn auslöst
Zweck	Dokumentation und Betreuung der IT des Verantwortlichen	Auftragsabwicklung, Rechnungsstellung und Zeiterfassung des Verantwortlichen
Dauer	Laufzeit des Hauptvertrags, Löschung 30 Tage nach Ende	Laufzeit des Hauptvertrags, Löschung 30 Tage nach Ende

Anlage 2 – Technische und organisatorische Maßnahmen

- **Zutritt:** Die Server stehen in den abgeschlossenen Geschäftsräumen des Auftragsverarbeiters in Ihlow. Zutritt hat nur der Inhaber.
- **Zugang zum Server:** Verwaltung nur durch den Inhaber, nur über SSH mit Schlüssel, Firewall mit Freigabe nur der nötigen Ports, Sicherheitsupdates des Betriebssystems zeitnah. Die Datenträger des Servers sind verschlüsselt.
- **Zugriff auf die Programme:** persönliche Benutzerkonten, Passwörter nur als Hash gespeichert, Zwei-Faktor-Anmeldung für Konten mit Verwaltungsrechten, Sperre nach wiederholten Fehlversuchen, automatische Abmeldung bei Inaktivität, Rechte nach Rollen.
- **Trennung:** Deichwerk Faktura läuft je Kunde in einer eigenen Instanz mit eigener Datenbank. Im IT HUB sieht jeder Kunde nur seine eigenen Daten (Mandantentrennung). Vorführ- und Testdaten sind von echten Daten getrennt.
- **Übertragung:** Zugriff nur über verschlüsselte Verbindungen (HTTPS/TLS).
- **Verschlüsselung gespeicherter Geheimnisse:** Zugangsdaten zu Drittsystemen und Geheimnisse der Zwei-Faktor-Anmeldung sind verschlüsselt gespeichert. Datensicherungen, die den Server verlassen, sind verschlüsselt (AES-256).
- **Nachvollziehbarkeit:** Protokoll über Anmeldungen und Änderungen. In der Zeiterfassung wird jede Korrektur mit altem und neuem Wert, Benutzer, Zeitpunkt und Begründung festgehalten.
- **Verfügbarkeit:** Datensicherung mindestens täglich, Aufbewahrung mindestens 30 Tage. Zusätzlich wird der Server auf einen zweiten Server gespiegelt und täglich verschlüsselt an einem zweiten Standort gesichert (georedundant, siehe Anlage 3). Die Wiederherstellung wird halbjährlich getestet.
- **Organisation:** Zugriff auf die Daten hat nur der Inhaber. Er ist zur Vertraulichkeit verpflichtet. Kundendaten werden nicht auf privaten Geräten und nicht in Cloud-Speichern außerhalb der Anlage 3 abgelegt.
- **Fernwartung:** Zugriffe auf Systeme des Verantwortlichen nur mit dessen Zustimmung; Datum, Dauer und Zweck werden festgehalten.
- **Umgang mit Vorfällen:** Sicherheitsvorfälle werden dokumentiert und dem Verantwortlichen nach § 11 gemeldet.
- **Löschung:** 30 Tage nach Vertragsende; Datensicherungen mit Ablauf ihrer Aufbewahrungszeit.
- **Überprüfung:** Der Auftragsverarbeiter prüft diese Maßnahmen mindestens einmal im Jahr.

Anlage 3 – Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
Microsoft Ireland Operations Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	Speicherung der verschlüsselten Datensicherungen (OneDrive); E-Mail-Versand über Microsoft 365, soweit der Auftragsverarbeiter E-Mails für den Verantwortlichen versendet	EU
Anbieter der KI-Funktion – nur wenn der Verantwortliche die KI-Funktion über einen Zugang des Auftragsverarbeiters nutzt; wird vorher in Textform mitgeteilt	Auslesen von Belegen	wird vorher mitgeteilt

Der Server selbst wird vom Auftragsverarbeiter in eigenen Räumen betrieben; ein Rechenzentrumsbetreiber ist nicht beteiligt.