Vereinbarung über eine Auftragsverarbeitung nach Art. 28 DSGVO

abgeschlossen zwischen dem Anwender (Verantwortlicher):		und dem Hersteller (Auftragsverarbeiter):
Name:	_____	Deutner Lohnverrechnung &
Name 2:	_____	Business Software e.U.
Adresse:	_____	Rathausstraße 23
PLZ/Ort:	_____	A-2151 Asparn an der Zaya
(im Folgenden Auftraggeber)		(im Folgenden Auftragnehmer)

1. Gegenstand der Vereinbarung

(1) Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben:

Unterstützung bei Problemen mit der Lohnsoftware per Fernwartung – vertraglich abgesichert durch den Wartungsvertrag werden bei Problemen, die telefonisch nicht lösbar sind, per Fernwartung Lösungen angeboten. Diese Lösungen sind bei Überschreitung der Grenze für kurzfristige Unterstützungen (etwa bis zu 10 Minuten) auch entgeltlich. Es werden aber vom Auftragnehmer keine Daten ohne Zustimmung des Auftraggebers auf den PC des Auftragnehmers übertragen.

(2) Folgende Datenkategorien werden verarbeitet:

Durch die Unterstützung per Fernwartung werden alle im Dokument Winlohn_Datenschutz für die Umsetzung der DSGVO angesprochenen Datenkategorien betroffen sein! Das sind u.a. auch die Adressdaten der Mitarbeiter sowie deren Lohnabrechnungsdaten.

(3) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

Personaldaten sowie deren gesetzeskonforme Abrechnung

2. Dauer der Vereinbarung

Die Vereinbarung wird auf unbestimmte Zeit geschlossen und kann von beiden Parteien per Jahresende mit einer Kündigungsfrist von einem Monat gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der Fernwartung für den Auftraggeber zu verarbeiten. Nachdem über die Dauer der Fernwartung hinaus ohne zusätzliche Einwilligung keine Daten gespeichert werden, können diese auch nicht auf Grund eines behördlichen Auftrages weitergegeben werden. Eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers bedarf eines schriftlichen Auftrages bzw. zumindest einer Zustimmung per e-Mail.

(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage ./1 zu entnehmen).

(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(6) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

(9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. Ort der Durchführung der Datenverarbeitung

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

5. Sub-Auftragsverarbeiter

Der Auftragnehmer ist nicht berechtigt, einen Sub-Auftragsverarbeiter heranzuziehen.

_____	_____, Asparn an der Zaya
Datum, Ort	Datum, Ort
_____	_____
Stampiglie der Firma und Unterschrift des Auftraggebers	Stampiglie der Firma und Unterschrift des Auftragnehmers
_____	Hermann Deutner, Geschäftsführer
Name und Funktion	Name und Funktion

Anlage ./1 – Technisch-organisatorische Maßnahmen

Vertraulichkeit

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch Sicherheitstüren im Außenbereich und verschließbarem Büro;
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung durch Verwendung von Passwörtern und Verschlüsselung von externen Datenträgern;
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, da nicht in einem Netzwerk sondern Standalone-PC und einziger Benutzer am PC; keine Mitarbeiter haben Zugang;
- **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

Integrität

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung externer Datenträger und Versand von e-Mails mit personenbezogenen Daten per elektronischer Signatur;
- **Eingabekontrolle**: nicht notwendig, da nur der Auftragnehmer Hermann Deutner Zugang zu den PC's hat;

Verfügbarkeit und Belastbarkeit

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
- Rasche **Wiederherstellbarkeit**; da keine Daten bei einer Fernwartung gespeichert werden, muss auch keine rasche Wiederherstellbarkeit gewährleistet werden!
- **Löschungsfristen**: da im Zuge der Fernwartung keine Daten kopiert werden, außer es erfolgt eine schriftliche Vereinbarung, sind keine Daten nach dem Beenden der Fernwartung zu löschen; sollte ausnahmsweise ein Datenbestand nach schriftlicher Zustimmung beim Auftragnehmer gespeichert werden, dann verpflichtet sich der Auftragnehmer, diese Daten nach Lösung des Problems unverzüglich zu löschen und dem Auftraggeber diese Löschung per e-Mail anzuzeigen;

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen;
- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, Vorabüberzeugungspflicht, Nachkontrollen.