Vereinbarung über die Auftragsverarbeitung gemäß Art. 28 DSGVO (AVV)

zwischen [Name der Firma], [Rechtsform], [Anschrift], vertreten durch [Vertretungsberechtigte/r] (nachfolgend „Mandant“ bzw. „Verantwortlicher“) und Digitally Done EOOD, j.k. Bratya Miladinovi 88, ent. 4, fl. 1, ap. 1, 8000 Burgas, Bulgarien, UIC/ЕИК 208857359, vertreten durch den Geschäftsführer Alexander Lienau (nachfolgend „Auftragnehmer“) als Auftragsverarbeiter.

§ 1 Gegenstand und Dauer

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Rahmen des Mandatsvertrages über Buchhaltungsdienstleistungen. Die Dauer dieser Vereinbarung entspricht der Laufzeit des Mandatsvertrages.

§ 2 Art, Zweck und Umfang der Verarbeitung

Erhebung, Speicherung, Ordnung und Verwendung personenbezogener Daten zum Zweck der laufenden Finanzbuchhaltung, der Lohn- und Gehaltsabrechnung, des Melde- und Bescheinigungswesens sowie des Personalmanagements – ausschließlich innerhalb der Europäischen Union.

§ 3 Kategorien betroffener Personen und Datenarten

- Beschäftigte des Verantwortlichen: Stammdaten, Kontaktdaten, Steuer- und Sozialversicherungsdaten, Bankverbindungen, Entgeltdaten, Fehl- und Urlaubszeiten, ggf. Gesundheitsdaten (z. B. Arbeitsunfähigkeitszeiten) als besondere Kategorien nach Art. 9 DSGVO;
- Geschäftspartner des Verantwortlichen (Debitoren/Kreditoren): Namen, Kontaktdaten, Bankverbindungen, Rechnungs- und Zahlungsdaten.

§ 4 Pflichten des Auftragsverarbeiters

- Verarbeitung ausschließlich auf dokumentierte Weisung des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO);
- Verpflichtung aller mit der Verarbeitung befassten Personen – einschließlich freier Mitarbeiter – auf Vertraulichkeit;
- Umsetzung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO (Anlage TOM);
- Unterstützung des Verantwortlichen bei der Beantwortung von Betroffenenanfragen sowie bei den Pflichten aus Art. 32–36 DSGVO;
- unverzügliche Meldung von Verletzungen des Schutzes personenbezogener Daten an den Verantwortlichen;
- Bereitstellung aller für den Nachweis der Pflichten erforderlichen Informationen; Duldung und Unterstützung von Kontrollen.

§ 5 Unterauftragsverhältnisse

(1) Der Verantwortliche erteilt die allgemeine Genehmigung zur Einschaltung von Unterauftragsverarbeitern innerhalb der EU. Der Auftragnehmer informiert über beabsichtigte Änderungen; der Verantwortliche kann aus wichtigem Grund widersprechen.

(2) Derzeit eingesetzte Unterauftragsverarbeiter:

- Agenda Informationssysteme GmbH & Co. KG, Oberaustraße 14, 83026 Rosenheim, Deutschland (Buchhaltungs- und Lohnsoftware sowie das Agenda Unternehmensportal und das Agenda Personal Portal, über die der Verantwortliche und seine Beschäftigten Unterlagen abrufen);

- IONOS SE, Elgendorfer Straße 57, 56410 Montabaur, Deutschland (Serverhosting der Agenda-Installation);
- Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Deutschland (Serverhosting der Belegerfassung und Vorverarbeitung);
- Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg (KI-gestützte Erkennung von Belegen über Amazon Bedrock, Verarbeitung in einer EU-Region). Nach den Servicebedingungen für Amazon Bedrock werden die übermittelten Inhalte weder zum Training von Modellen verwendet noch an Modellanbieter weitergegeben.
- freie Mitarbeiter des Auftragnehmers mit Sitz in der EU, jeweils schriftlich auf Vertraulichkeit und Datenschutz verpflichtet.

(3) Die Server der unter Absatz 2 genannten Dienstleister stehen in der Europäischen Union. Eine aktuelle Fassung dieser Liste stellt der Auftragnehmer auf Anforderung in Textform zur Verfügung.

(4) Die KI-gestützte Belegerkennung dient der Vorerfassung. Jeder daraus abgeleitete Buchungssatz wird vor der Verbuchung durch den Auftragnehmer geprüft; eine ausschließlich auf automatisierter Verarbeitung beruhende Entscheidung im Sinne des Art. 22 DSGVO findet nicht statt.

§ 6 Löschung und Rückgabe

Nach Beendigung des Mandats gibt der Auftragnehmer alle personenbezogenen Daten in einem gängigen Format zurück und löscht vorhandene Kopien, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

§ 7 Schlussbestimmungen

Im Übrigen gelten die Bestimmungen des Mandatsvertrages. Bei Widersprüchen geht diese Vereinbarung hinsichtlich des Datenschutzes vor. Änderungen bedürfen der Textform.

Ort, Datum	Burgas, 17.10.2026
Mandant	Digitally Done EOOD
Name, Funktion	Alexander Lienau, Geschäftsführer

Anlage: Technische und organisatorische Maßnahmen (TOM) – Übersicht

- Zutritts-/Zugangskontrolle: passwortgeschützte Systeme, Zwei-Faktor-Authentifizierung, rollenbasierte Berechtigungen;
- Übertragungskontrolle: verschlüsselte Übertragung (TLS), Datenaustausch über gesicherte Portale statt unverschlüsselter E-Mail;
- Verarbeitung ausschließlich innerhalb der EU; keine Draufsicht durch Drittstaaten-Dienstleister;
- Eingabekontrolle: revisionssichere Protokollierung in der Buchhaltungssoftware;
- KI-gestützte Belegerkennung: Verarbeitung in einer EU-Region, keine Verwendung der Inhalte zum Training von Modellen, Prüfung jedes Ergebnisses durch den Auftragnehmer vor der Verbuchung;
- Verfügbarkeitskontrolle: regelmäßige Backups, Wiederherstellungskonzept;
- Trennungskontrolle: mandantengetrennte Verarbeitung;
- Organisatorisches: Vertraulichkeitsverpflichtungen aller Mitarbeiter und freien Mitarbeiter, dokumentierte Löschprozesse, regelmäßige Sensibilisierung.