

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/EIN 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, Portale);
- Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA (Hosting der Website; DPF-zertifiziert,

DPA mit EU-Standardvertragsklauseln);

- freie Mitarbeiter des Auftragnehmers mit Sitz in der EU, jeweils schriftlich auf Vertraulichkeit und Datenschutz verpflichtet.

§ 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 – Mandant

Ort, Datum – Digitally Done EOOD

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;
- Verfügbarkeitskontrolle: regelmäßige Backups, Wiederherstellungskonzept;
- Trennungskontrolle: mandantengetrennte Verarbeitung;
- Organisatorisches: Vertraulichkeitsverpflichtungen aller Mitarbeiter und freien Mitarbeiter, dokumentierte Löschprozesse, regelmäßige Sensibilisierung.