

DATA PROCESSING AGREEMENT (DPA)

Versione 1.0 — In vigore dal 1° luglio 2026 — Allegato ai Termini di Servizio

Il presente Accordo ("DPA") integra il contratto principale tra il **Cliente** (Titolare del trattamento) e la ditta individuale **Michele Milazzo**, P.IVA 01425370531 (Responsabile del trattamento) ed è redatto in conformità all'art. 28 del Regolamento UE 2016/679 (GDPR).

1. Oggetto e durata

Il Responsabile tratta i dati personali del Cliente esclusivamente per erogare i Servizi descritti nei Termini di Servizio, per la durata del contratto principale e per il periodo di retention necessario all'adempimento degli obblighi legali.

2. Natura, finalità e categorie

Voce	Descrizione
Natura del trattamento	Hosting, storage, elaborazione, backup, supporto tecnico.
Finalità	Erogazione dei servizi cloud OneKeyCo e dei moduli (App) acquistati.
Categorie di interessati	Dipendenti, clienti, fornitori, contatti del Cliente.
Categorie di dati comuni	Anagrafiche, dati di contatto, dati commerciali, di fatturazione, log applicativi.
Categorie di dati particolari	Eventuali dati sanitari (HRMS), dati su condanne (KYC/KYB), trattati solo se l'App attivata lo richiede e con base giuridica del Cliente.

3. Obblighi del Responsabile

trattare i dati solo su istruzione documentata del Cliente (istruzioni iniziali = Termini di Servizio + configurazione tenant);

garantire la riservatezza del personale autorizzato;

adottare le misure di sicurezza descritte all'Allegato A;

non ricorrere a sub-responsabili senza autorizzazione (vedi Allegato B);

assistere il Cliente nell'evasione delle richieste degli interessati;

assistere il Cliente in caso di data breach, DPIA e consultazione preventiva;

al termine del contratto, restituire o cancellare tutti i dati a scelta del Cliente, entro 90 giorni;

mettere a disposizione tutte le informazioni necessarie a dimostrare il rispetto del DPA e consentire audit (con preavviso 30gg, max 1 volta/anno).

4. Sub-responsabili

Il Cliente autorizza in via generale i sub-responsabili elencati nell'Allegato B. Il Responsabile comunicherà eventuali nuovi sub-responsabili con preavviso di 30 giorni; il Cliente può obiettare per motivi sostanziali, nel qual caso il Responsabile si impegna a trovare una soluzione alternativa o, in difetto, il Cliente può recedere senza penali.

5. Data breach

Il Responsabile notifica al Cliente ogni violazione di dati personali senza ingiustificato ritardo (**entro 24 ore** dalla scoperta), fornendo le informazioni utili al Cliente per la notifica al Garante entro 72 ore (art. 33 GDPR).

6. Trasferimenti extra-UE

I dati restano nello SEE (Hetzner DE/FI). Eventuali trasferimenti extra-UE (Cloudflare CDN, AI provider USA solo se Cliente attiva MMOS AI cloud) avvengono con Clausole Contrattuali Standard 2021/914 + EU-US DPF dove applicabile.

7. Limitazione di responsabilità

La responsabilità del Responsabile per violazione del presente DPA è limitata secondo quanto previsto dai Termini di Servizio, salvo dolo o colpa grave e ferma restando la responsabilità solidale prevista dall'art. 82 GDPR verso gli interessati.

Allegato A — Misure tecniche e organizzative

Crittografia: TLS 1.3 in-transit; LUKS at-rest sui dischi; backup AES-256.

Controllo accessi: MFA per accesso amministrativo; principio least-privilege; audit log centralizzato (Elasticsearch).

Segregazione: tenant isolati a livello di database, file storage e network.
Backup & DR: backup giornalieri offsite (Hetzner StorageBox), retention 30gg, test DR semestrale.
Monitoring: VictoriaMetrics + alert email h24.
Patching: aggiornamenti di sicurezza entro 7gg dalla disclosure.
Pentest: scansione automatica continua.

Allegato B — Sub-responsabili autorizzati

Soggetto	Ruolo	Sede
Hetzner Online GmbH	Hosting infrastruttura	DE/FI
Cloudflare Inc.	CDN, DNS, anti-DDoS	USA (SCC+DPF)
Stripe Payments Europe Ltd	Gateway pagamenti	IE
Anthropic PBC	LLM (solo se Cliente attiva MMOS AI cloud)	USA (SCC+DPF)
OpenAI LLC	LLM (solo se Cliente attiva MMOS AI cloud)	USA (SCC+DPF)
Meta Platforms Ireland	WhatsApp Business API (solo se attivato)	IE