MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO ai sensi del D.Lgs. 8 giugno 2001 n. 231

---

1. DATI SOCIETARI

La società:

OLISTAMI S.R.L.
con sede legale in **Merate (LC), Via San Francesco d'Assisi n. 7, CAP 23807**
Codice Fiscale e Partita IVA **04261130134**
Numero REA **LC – 431944**
domicilio digitale (PEC): **olistamisrl@namirialpec.it**

(d'ora in avanti, anche "Società")

PARTE GENERALE

2. FINALITÀ DEL MODELLO

Il presente Modello di Organizzazione, Gestione e Controllo (di seguito, il "Modello") è adottato dalla Società ai sensi del D.Lgs. 231/2001 al fine di:

- prevenire la commissione dei reati previsti dal decreto nell'interesse o a vantaggio della Società;
- definire un sistema strutturato di procedure e controlli;
- diffondere una cultura aziendale improntata a legalità, correttezza e trasparenza.

---

3. AMBITO DI APPLICAZIONE

Il Modello si applica a:

- tutti i soggetti che operano in nome e per conto della Società;
- collaboratori, partners e terzi coinvolti a qualsivoglia titolo nelle attività aziendali.

---

4. PRINCIPI GENERALI

La Società Olistami S.R.L., nello svolgimento delle proprie attività, si ispira ai principi di:

- legalità
- correttezza e trasparenza
- buona fede
- tracciabilità delle operazioni
- separazione delle funzioni

- controllo e verificabilità dei processi

---

5. SISTEMA DI CONTROLLO

Il sistema di controllo interno è fondato sui seguenti elementi:

- procedure operative formalizzate;
- tracciabilità delle operazioni economiche e decisionali;
- controlli di primo e secondo livello;
- sistemi informatici idonei a garantire sicurezza e integrità dei dati.

PARTE SPECIALE

6. ATTIVITÀ DELLA SOCIETÀ

La Società Olistami S.R.L. opera nei seguenti ambiti:

- organizzazione e promozione di eventi;
- gestione di piattaforme digitali;
- attività di marketing e comunicazione;
- erogazione di servizi e formazione;
- vendita di prodotti on line.

---

7. AREE A RISCHIO

Sono individuate le seguenti aree sensibili:

1. gestione dei flussi economici e dei pagamenti
2. organizzazione e promozione di eventi
3. attività di marketing e comunicazione
4. rapporti con fornitori e partners
5. trattamento dei dati personali
6. gestione amministrativa e contabile
7. raccolta fondi e destinazione degli stessi ad opere inclusive e solidali di cui al Codice Etico

---

8. REATI RILEVANTI

In relazione alle attività svolte, si considerano rilevanti le seguenti categorie di reato:

8.1 Reati contro la Pubblica Amministrazione

- corruzione
- truffa ai danni dello Stato
- indebita percezione di erogazioni pubbliche

8.2 Reati societari

- false comunicazioni sociali
- ostacolo all'attività di vigilanza

8.3 Reati fiscali

- dichiarazione fraudolenta
- omessa dichiarazione
- utilizzo o emissione di fatture per operazioni inesistenti

8.4 Reati informatici

- accesso abusivo a sistemi informatici
- trattamento illecito di dati
- violazioni in materia di sicurezza dei sistemi

8.5 Reati di riciclaggio

- riciclaggio
- autoriciclaggio

8.6 Reati in materia di sicurezza

- lesioni colpose
- violazioni delle norme in materia di sicurezza

8.7 Reati in materia di comunicazione commerciale

- pubblicità ingannevole
- pratiche commerciali scorrette

8.8 Violazioni del diritto d’autore

- utilizzo abusivo di contenuti protetti

---

9. PROTOCOLLI GENERALI DI PREVENZIONE

La Società adotta i seguenti protocolli generali:

9.1 Tracciabilità

- ogni operazione economica deve essere documentata, registrata e verificabile. E’ soggetta a doppio controllo contabile interno e di studio commercialista esterno;

9.2 Separazione delle funzioni

- le attività decisionali, operative e di controllo devono essere distinte;

9.3 Trasparenza delle comunicazioni

- ogni informazione al pubblico deve essere chiara, trasparente e non ingannevole;
- particolare attenzione alla comunicazione viene data in caso di sostegno all’inclusione ed opere di solidarietà e sostegno ad enti ed associazioni così come indicato espressamente nel codice etico.

9.4 Gestione dei pagamenti

- utilizzo esclusivo di strumenti tracciabili (bonifico, paypal);
- coerenza tra incassi, servizi erogati e registrazioni contabili;

9.5 Gestione degli eventi

- definizione chiara dell’offerta;
- verifica minima dei contenuti e dei soggetti coinvolti;

9.6 Protezione dei dati

- trattamento conforme alla normativa vigente;
- limitazione dell’accesso ai dati ai soli soggetti autorizzati.

---

10. SISTEMA DISCIPLINARE

La violazione delle disposizioni del presente Modello comporta:

- l’applicazione di sanzioni proporzionate alla gravità della violazione;
- la risoluzione dei rapporti contrattuali nei casi più gravi;
- eventuale segnalazione alle autorità competenti.

11. AGGIORNAMENTO DEL MODELLO

Il Modello è soggetto a revisione:

- in caso di modifiche normative;
- in caso di cambiamenti organizzativi;
- a seguito di violazioni riscontrate.

Allegati al modello (a,b):

A. ALLEGATO RS-01

MATRICE DEI RISCHI (RISK ASSESSMENT)

ai sensi del D.Lgs. 231/2001

---

1. DATI IDENTIFICATIVI

Società: OLISTAMI S.R.L.
Sede legale: Merate (LC), Via San Francesco d'Assisi n. 7
Codice Fiscale / Partita IVA: 04261130134
Numero REA: LC – 431944

---

2. FINALITÀ DELL'ALLEGATO

La presente matrice è redatta al fine di:

- individuare le **attività sensibili** ai fini del D.Lgs. 231/2001;
- identificare i **reati-presupposto astrattamente configurabili**;
- valutare il **livello di rischio inerente**;
- analizzare i **presidi di controllo esistenti**;
- definire il **rischio residuo** e le **azioni migliorative**.

---

3. METODOLOGIA DI VALUTAZIONE

Scale adottate

- **Probabilità (P):**
  - 1 = Bassa
  - 5 = Alta
- **Impatto (I):**
  - 1 = Basso
  - 5 = Elevato
- **Rischio Inerente (R):**

- R = P × I

- **Rischio Residuo (Rres):**
  - Basso / Medio / Alto (valutazione qualitativa)

---

4. MATRICE DEI RISCHI

4.1 AREA: PAGAMENTI, INCASSI E FATTURAZIONE

Processo	Attività sensibile	Evento di rischio	Reato	P	I	R	Presidi di controllo	Evidenze richieste	Rres
Gestione pagamenti	Incasso PayPal (split)	Disallineamento tra incasso e ripartizione importi	Fiscali / Riciclaggio / Societari	3	5	15	Sistema PayPal multiparty; gestione eventi CAPTURE/REFUND; log e riconciliazioni	ID transazioni, log PayPal, report incassi	Medio
Fatturazione	Emissione TD01/TD04	Errata emissione o mancata trasmissione SdI	Fiscali / Societari	3	5	15	Generazione XML automatizzata; invio via Aruba; numerazione progressiva senza interruzioni	XML fatture, esiti SdI, registro numerazione	Medio
Raccolta dati	Dati fiscali clienti/organizer	Dati incompleti per fatturazione	Fiscali / Privacy	4	4	16	Obbligo CF/P.IVA; validazioni anagrafiche; regole SDI	Database clienti, log validazione	Medio
Payout	Pagamenti agli organizer	Erogazione somme in presenza di anomalie	Fiscali / Riciclaggio	3	5	15	HOLD temporale; blocco payout se errori o refund	Log payout, controlli pre-erogazione	Medio

---

4.2 AREA: EVENTI E PIATTAFORMA

Processo	Attività sensibile	Evento di rischio	Reato	P	I	R	Presidi di controllo	Evidenze richieste	Rres
Gestione eventi	Stato evento	Evento non coerente con pagamento	Fiscali / Societari	3	4	12	Stati automatizzati (confermato/cancellato); audit trail	Log stati evento	Medio
Pricing	Prezzi eventi	Disallineamento prezzo cliente/checkout	Commerciali scorrette	3	4	12	Controllo coerenza prezzo; verifica lato checkout	Log prezzo evento e pagamento	Medio
Split pagamenti	Ripartizione fondi	Mancata separazione importi	Fiscali / Societari	3	5	15	Controllo tecnico split multipayee	Report distribuzione importi	Medio
Refund	Gestione rimborsi	Rimborso senza nota di credito	Fiscali	3	5	15	Emissione automatica TD04; procedure refund definite	Log refund, XML, comunicazioni	Medio

---

4.3 AREA: SISTEMI INFORMATIVI E SICUREZZA

Processo	Attività sensibile	Evento di rischio	Reato	P	I	R	Presidi di controllo	Evidenze richieste	Rres
Sistemi IT	Accesso e gestione dati	Accessi non autorizzati	Informatici / Privacy	3	5	15	Sistemi autenticazione; gestione accessi	Log accessi, audit trail	Medio
Logging	Audit sistemi	Mancata tracciabilità operazioni	Informatici / Societari	3	4	12	Log operazioni admin; storico modifiche	Registro audit log	Medio
Pagamenti online	Sicurezza transazioni	Frodi o uso improprio sistemi pagamento	Informatici / Riciclaggio	3	4	12	Transazioni protette via PayPal	Log transazioni, dispute	Medio

---

4.4 AREA: CONTENUTI, UTENTI E PRIVACY

Processo	Attività sensibile	Evento di rischio	Reato	P	I	R	Presidi di controllo	Evidenze richieste	Rres
Gestione contenuti	Pubblicazione utenti	Contenuti illeciti o diffamatori	Informatica / Copyright	3	4	12	Responsabilità utente; diritto rimozione piattaforma	Log rimozioni contenuti	Medio

Processo	Attività sensibile	Evento di rischio	Reato	P	I	R	Presidi di controllo	Evidenze richieste	Rres
Trattamento dati	Dati personali	Utilizzo non conforme al GDPR	Privacy	3	5	15	Informativa privacy; raccolta consenso; sicurezza dati	Registro consensi, log trattamento	Medio
Marketing	Profilazione utenti	Utilizzo dati senza consenso	Privacy	3	4	12	Consensi separati e revocabili	Log consenso e revoche	Medio

---

4.5 AREA: GOVERNANCE E CONTROLLO

Processo	Attività sensibile	Evento di rischio	Reato	P	I	R	Presidi di controllo	Evidenze richieste	Rres
Segnalazioni	Whistleblowing	Mancata gestione segnalazioni	Societari	2	4	8	Canali interni di segnalazione	Registro segnalazioni	Basso/Medio
Relazioni esterne	Organizer	Mancata emissione documenti da parte organizer	Commerciale / Fiscale (indiretto)	3	3	9	Sistema reminder e responsabilità contrattuale	Comunicazioni e notifiche	Medio

---

5. VALUTAZIONE COMPLESSIVA

Dall’analisi svolta emergono:

- **Rischi maggiori (R ≥ 15):**
  - incassi e split pagamenti
  - fatturazione elettronica
  - gestione rimborsi
  - protezione dati
- **Rischi medi:**
  - gestione eventi
  - coerenza prezzi
  - sicurezza IT
- **Rischi residui:** prevalentemente **medi**, a condizione della corretta applicazione dei controlli.

---

6. PRINCIPALI AZIONI DI MIGLIORAMENTO

La Società prevede:

- rafforzamento dei controlli di riconciliazione contabile periodica
- implementazione audit trail completo e immodificabile
- revisione periodica dei flussi fiscali e tecnici
- monitoraggio dei sistemi IT e dei log
- formalizzazione delle procedure di controllo e verifica

---

7. CLAUSOLA DI AGGIORNAMENTO

La presente matrice:

- è soggetta a revisione periodica;

- è aggiornata in caso di modifiche normative o organizzative;
- costituisce parte integrante del Modello 231 della Società.

§

B. **ALLEGATO PR-01**

PROTOCOLLI OPERATIVI DI PREVENZIONE

ai sensi del D.Lgs. 231/2001

---

1. FINALITÀ DELL'ALLEGATO

Il presente Allegato ha lo scopo di:

- definire i **protocolli operativi** diretti a prevenire la commissione dei reati-presupposto;
- disciplinare le modalità di gestione delle attività sensibili;
- garantire **tracciabilità, trasparenza e controllabilità** dei processi aziendali;
- assicurare la coerenza tra attività operative e sistema di controllo interno.

---

2. PRINCIPI GENERALI DI CONTROLLO

Tutti i protocolli si fondano sui seguenti principi:

- **tracciabilità di ogni operazione**;
- **separazione dei ruoli** (ove applicabile);
- **documentazione e verificabilità delle attività**;
- **coerenza tra eventi economici e registrazioni contabili**;
- **utilizzo esclusivo di sistemi informatici autorizzati**;
- **rispetto delle normative fiscali, informative e privacy**.

---

3. PROTOCOLLI OPERATIVI

3.1 PROTOCOLLO PR-01/A – GESTIONE PAGAMENTI E INCASSI

3.1.1 Ambito

Il protocollo disciplina:

- incassi da clienti finali;
- gestione pagamenti tramite piattaforma;
- ripartizione importi tra Società e terzi;

- registrazione e riconciliazione dei flussi finanziari.

3.1.2 Regole operative

1. **Tracciabilità dei pagamenti**
    - Tutti i pagamenti devono avvenire mediante strumenti elettronici tracciabili.
    - È vietato gestire incassi non registrati nel sistema.
2. **Coerenza pagamento–evento**
    - Ogni pagamento deve essere associato a:
        - un evento specifico;
        - un utente identificato;
        - un importo determinato.
3. **Ripartizione importi in caso di intermediazione**
    - Il sistema deve garantire la separazione tra:
        - quota spettante alla Società;
        - quota spettante al soggetto terzo (organizzatore).
4. **Registrazione automatica**
    - Ogni transazione deve essere registrata automaticamente nei sistemi interni.

3.1.3 Controlli

- verifica periodica della corrispondenza tra:
    - incassi registrati;
    - transazioni finanziarie;
    - dati della piattaforma;
- controllo delle anomalie di importo.

3.1.4 Evidenze

- log delle transazioni
- identificativi ordine (order ID)
- dati pagamento e timestamp
- report incassi

3.2 PROTOCOLLO PR-01/B – FATTURAZIONE E ADEMPIMENTI FISCALI

3.2.1 Ambito

Regola:

- emissione fatture

- gestione note di credito
- trasmissione al Sistema di Interscambio (SdI)

3.2.2 Regole operative

1. **Emissione documenti**
    - Ogni operazione soggetta a fatturazione deve generare documento fiscale.
    - Le fatture devono essere:
        - complete
        - corrette
        - coerenti con l'operazione sottostante
2. **Numerazione**
    - Deve essere progressiva, senza salti o duplicazioni.
3. **Trasmissione**
    - I documenti devono essere trasmessi tramite canali autorizzati (SdI).
4. **Note di credito**
    - In caso di rimborso, deve essere emesso documento correttivo.

3.2.3 Controlli

- verifica periodica della corrispondenza tra:
    - incassi e fatture
- controllo esiti SdI
- verifica numerazione documenti

3.2.4 Evidenze

- file XML fatture
- ricevute SdI
- registro fatture
- storico note di credito

3.3 PROTOCOLLO PR-01/C – GESTIONE EVENTI

3.3.1 Ambito

Riguarda:

- pubblicazione eventi
- gestione ciclo di vita degli eventi
- erogazione dei servizi

3.3.2 Regole operative

1. **Creazione evento**
    - Ogni evento deve essere definito da:
        - contenuto chiaro
        - prezzo trasparente
        - condizioni esplicite
2. **Pubblicazione**
    - L'evento deve essere verificato prima della pubblicazione.
3. **Stato evento**
    - Ogni evento deve essere tracciato tramite uno stato:
        - confermato
        - cancellato
4. **Coerenza con pagamenti**
    - Lo stato dell'evento deve essere coerente con:
        - incassi
        - eventuali rimborsi

3.3.3 Controlli

- verifica eventi attivi
- controllo eventi senza corrispondenza economica
- monitoraggio cancellazioni

3.3.4 Evidenze

- registro eventi
- log modifiche evento
- storico stato evento

3.4 PROTOCOLLO PR-01/D – GESTIONE RIMBORSI

3.4.1 Ambito

Disciplina:

- rimborsi ai clienti
- rettifiche contabili

3.4.2 Regole operative

1. **Autorizzazione rimborso**
    - I rimborsi devono essere coerenti con condizioni previste.
2. **Tracciabilità**
    - Ogni rimborso deve essere registrato.
3. **Documento fiscale**
    - Deve essere emessa nota di credito.
4. **Coerenza contabile**
    - Rimborso e documento fiscale devono coincidere.

3.4.3 Controlli

- verifica rimborsi effettuati
- confronto tra rimborso e nota di credito

3.4.4 Evidenze

- log refund
- documenti TD04
- storicizzazione operazioni

3.5 PROTOCOLLO PR-01/E – SISTEMI INFORMATIVI E SICUREZZA

3.5.1 Ambito

Riguarda:

- gestione piattaforma
- accesso ai sistemi
- sicurezza informatica

3.5.2 Regole operative

1. **Accessi**
    - Solo soggetti autorizzati possono accedere ai sistemi.
2. **Protezione dati**
    - I dati devono essere:
        - protetti
        - non accessibili a terzi non autorizzati
3. **Audit trail**

- Ogni operazione rilevante deve essere tracciata.

3.5.3 Controlli

- monitoraggio accessi
- verifica integrità sistemi
- analisi attività anomale

3.5.4 Evidenze

- log accessi
- log operazioni
- report sicurezza

3.6 PROTOCOLLO PR-01/F – PROTEZIONE DATI PERSONALI (PRIVACY)

3.6.1 Ambito

Disciplina:

- raccolta dati utenti
- utilizzo dati
- conservazione

3.6.2 Regole operative

1. **Base giuridica**
   - Il trattamento deve essere:
     - giustificato
     - limitato allo scopo
2. **Consenso**
   - Deve essere raccolto ove previsto.
3. **Minimizzazione**
   - Devono essere trattati solo i dati necessari.

3.6.3 Controlli

- verifica consensi
- controllo utilizzo dati

3.6.4 Evidenze

- registro consensi
- log trattamento dati

3.7 PROTOCOLLO PR-01/G – GESTIONE CONTENUTI E UTENTI

3.7.1 Ambito

Riguarda:

- contenuti pubblicati dagli utenti
- responsabilità e rimozione contenuti

3.7.2 Regole operative

1. **Responsabilità contenuti**
    - I contenuti sono sotto responsabilità dell'utente.
2. **Controllo**
    - La Società può rimuovere contenuti illeciti.
3. **Segnalazioni**
    - Devono essere gestite tempestivamente.

3.7.3 Controlli

- gestione segnalazioni
- verifica contenuti pubblicati

3.7.4 Evidenze

- log segnalazioni
- registro rimozioni contenuti

---

4. CLAUSOLA DI AGGIORNAMENTO

I protocolli:

- sono soggetti a revisione periodica;
- devono essere aggiornati in caso di:
    - modifiche normative;
    - evoluzione della piattaforma;
    - rilevazione di criticità operative.

§

Modello ed allegato sono soggetti a revisione periodica a cura di Olistami S.R.L. .