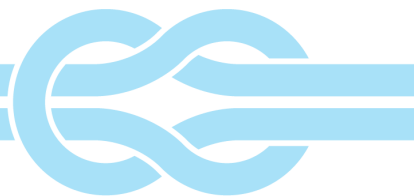


**Modello di Organizzazione,
Gestione e Controllo**
ex Decreto Legislativo n.
231/2001

*Parte Speciale “Sez. M”
Delitti in materia di strumenti
di pagamento diversi dai
contanti e trasferimento
fraudolento di valori (articolo
25-octies.1 del Decreto)*



1. Funzioni e obiettivi della Parte Speciale

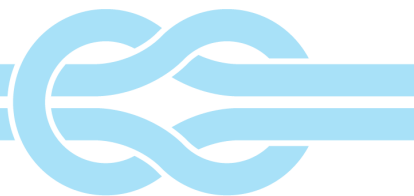
La Parte Speciale del presente Modello si propone di:

- individuare, previa descrizione delle fattispecie incriminatrici, le attività aziendali nel cui ambito potrebbero essere commessi reati rilevanti ai sensi del D.Lgs. 231/2001;
- evidenziare ai Destinatari del Modello le condotte che potrebbero comportare l'applicazione, nei confronti del Consorzio PSL, delle sanzioni previste dal D.Lgs. 231/2001;
- disciplinare i comportamenti richiesti ai Destinatari del Modello, al fine specifico di prevenire la commissione dei reati di cui alla presente Sez. M di Parte Speciale.

Obiettivo finale della Parte Speciale, pertanto, è la costruzione di un insieme strutturato di regole, oggetto di costante aggiornamento e monitoraggio, che non possa essere aggirato se non fraudolentemente, venendo così in rilievo, in tale ultima ipotesi, l'esimente da responsabilità di cui all'art. 6, comma 1, lett. c) del Decreto.

La presente Parte Speciale esamina nel dettaglio i Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori - articolo 25-octies.1 del Decreto - esemplificando le condotte che potrebbero integrarli in considerazione delle attività svolte dal Consorzio PSL.

La preventiva attività di “*Risk Assessment*” ha evidenziato un **rischio basso** per tali tipologie di reati in relazione allo svolgimento dell'attività del Consorzio.



2. Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori: le fattispecie

Premessa

L'articolo 25-octies.1 del D.Lgs. 231/2001 prevede la responsabilità amministrativa degli enti per i delitti in materia di utilizzo di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori. Le fattispecie sono disciplinate negli articoli 493-ter, 493-quater, 512 bis e 640 ter del Codice Penale.

Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.)

Punisce chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti.

Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.)

La fattispecie punisce chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

Frode informatica (art. 640 ter c.p.)

La norma punisce chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno.

Trasferimento fraudolento di valori (art. 512 bis c.p.)

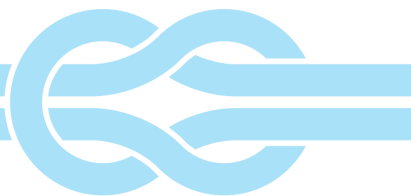
La fattispecie punisce chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648 (ricettazione), 648 bis (riciclaggio) e 648 ter (impiego di denaro, beni o utilità di provenienza illecita).

3. Attività a rischio, misure di prevenzione e divieti specifici

➤ Art. 25 octies.1 del D.Lgs. 231/2001

Attività a rischio:

1. Transazioni economiche e pagamenti:



- Ogni transazione che si perfeziona con uno strumento diverso dal denaro rappresenta un potenziale rischio di per l'integrazione delle condotte di cui alla presente Sezione M di Parte Speciale. Va considerato che l'utilizzo dei contanti è assolutamente residuale e marginale per l'attività del Consorzio PSL, ciò anche nell'ottica di favorire la tracciabilità di tutte le transazioni.

Misure di prevenzione:

- Ogni operazione o transazione deve essere documentata, verificabile e tracciabile, garantendo la possibilità di identificare l'origine e l'autorizzazione delle attività, nonché lo strumento di pagamento utilizzato e la sua titolarità.
- Formazione del personale: Sensibilizzazione sui rischi inerenti alle tipologie di reato di cui alla presente Sezione M.
- Adozione di adeguate misure di protezione dei sistemi informatici e dei terminali che impediscano l'installazione o l'utilizzo di programmi non autorizzati dal Consorzio.

Divieti specifici:

Il Consorzio vieta espressamente:

1. **L'utilizzo o installazione di programmi informatici** non autorizzati.
2. La partecipazione a **operazioni finanziarie non trasparenti** o prive di adeguata verifica sulla provenienza dei fondi.
3. Il perfezionamento di transazioni con **strumenti di pagamento diversi** da quelli in uso al Consorzio ed espressamente riconosciuti e riconoscibili.

4. Principi generali da osservare

➤ **Legalità e trasparenza**

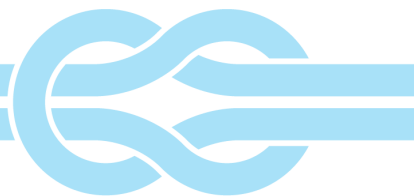
- Ogni attività aziendale deve essere svolta nel pieno rispetto delle leggi, regolamenti e delle procedure interne (ISO 9001, ISO 45001, Modello 231, Codice Etico).

➤ **Diligenza e responsabilità**

- Tutti i dipendenti, collaboratori e dirigenti devono agire con diligenza e responsabilità nello svolgimento delle loro mansioni, evitando comportamenti che possano esporre il Consorzio a rischi di violazioni normative e all'integrazione delle condotte di cui all'art. 25-octies.1 del Decreto.

➤ **Divieto di comportamenti illeciti**

- È vietata ogni condotta finalizzata alla conclusione di operazioni non trasparenti al fine ottenere indebiti vantaggi economici per il Consorzio PSL.



➤ **Controllo e tracciabilità**

- Ogni operazione o transazione deve essere documentata, verificabile e tracciabile, garantendo la possibilità di identificare l'origine e l'autorizzazione delle attività, nonché gli strumenti di pagamento utilizzati.

➤ **Riservatezza e protezione dei dati**

- I dati sensibili e riservati devono essere trattati in modo conforme alla normativa vigente (es. GDPR) e alle politiche aziendali, evitando accessi non autorizzati o divulgazioni indebite.

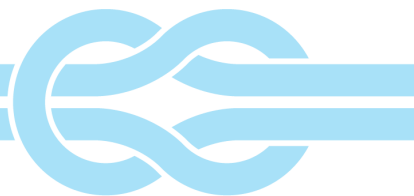
5. Aree sensibili nell'attività del Consorzio PSL

Di seguito un'analisi di rilevanza (sensibilità) delle singole Aree del Consorzio PSL rispetto ai reati presupposto di cui alla presente Sezione M.

AREA DI COMPETENZA	DENOMINAZIONE AREA NEL "SISTEMA 231"	SENSIBILITA' DELL'AREA
DIREZIONE GENERALE	A1	
RESPONSABILE DELLA SICUREZZA (RSPP) → Soggetto esterno	A2	
RESPONSABILE DEL SISTEMA DI GESTIONE INTEGRATO (Compliance)	A3	
RESPONSABILE GARE/TENDER - RESPONSABILE ACQUISTI	A4	
RESPONSABILE DIREZIONE OPERATIVA	A5	
RESPONSABILE AMMINISTRAZIONE E HR	A6	
RESPONSABILE COMMERCIALE E MARKETING → Soggetto esterno	A7	

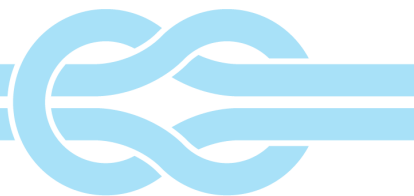
Legenda:

	Molto sensibile (Rischio elevato)
	Abbastanza sensibile (Rischio medio)
	Poco sensibile (Rischio basso)



6. Presidi e procedure specifiche per attività a rischio

ATTIVITÀ A RISCHIO	PRESIDI E PROCEDURE
Transazioni economiche (per reati ex art. 25-octies.1)	• Tracciabilità dei flussi: Implementazione di procedure interne per garantire la trasparenza e la tracciabilità di tutte le operazioni economiche e finanziarie, al fine di evitare di integrare le condotte di cui all'art. 25-octies.1 del Decreto • Formazione del personale: Sensibilizzazione costante del personale rispetto ai rischi connessi alle tipologie di reato di cui all'art. 25-octies.1 del Decreto
Selezione partner: fornitori e clienti (per i reati ex art. 25-octies.1)	• Due diligence su clienti e fornitori: Verifica dell'affidabilità dei clienti e dei fornitori attraverso controlli incrociati su blacklist, banche dati e certificazioni. Monitoraggio continuo dei rapporti con soggetti operanti in settori a rischio. • Formazione del personale: Sensibilizzazione costante del personale rispetto ai rischi connessi alle tipologie di reato di cui all'art. 25-octies.1 del Decreto.
Utilizzo apparecchiature, dispositivi e soprattutto strumenti informatici (per i reati ex art. 25-octies.1)	• Adozione di un regolamento di utilizzo degli strumenti informatici: Stabilire le modalità di utilizzo degli strumenti informatici anche con la collaborazione di appositi consulenti IT e porre in essere un costante monitoraggio circa il rispetto delle misure.



	• Formazione del personale: Sensibilizzazione costante del personale rispetto ai rischi connessi alle tipologie di reato di cui all'art. 25-octies.1 del Decreto.
--	---

7. Compiti dell'Organismo di Vigilanza

Al fine di assicurare il rispetto del Modello 231 e di prevenire il verificarsi di condotte idonee ad integrare i reati presupposto di cui alla presente Sezione M, l'Organismo di Vigilanza di TLF S.r.l. è tenuto a:

- Verificare periodicamente - con il supporto di tutte le aree dell'azienda - la corretta applicazione ed il rispetto dei Protocolli e delle Procedure aziendali con particolare riferimento ai Sistemi di Gestione ISO, e al Modello 231, anche al fine di suggerirne eventuali modifiche e/o integrazioni;
- Esaminare eventuali segnalazioni specifiche e/o obbligatorie provenienti dagli organi di controllo o da terzi o da qualsiasi Responsabile di area ed effettuare gli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute, anche ai sensi della disciplina del *Whistleblowing* di cui alla Direttiva UE 1937/2019, recepita con D.Lgs. 24/2023;
- Verificare il rispetto delle indicazioni previste nelle procedure aziendali anche in relazione ai flussi informativi nei confronti dell'OdV;
- Pianificare audit periodici con i Responsabili delle diverse aree aziendali;
- Vigilare sull'efficacia e l'adeguatezza del Modello e proporre eventuali modifiche e/o aggiornamenti;
- Predisporre un piano formativo dedicato al personale aziendale in materia di Modello 231;
- Verificare periodicamente il sistema di tracciabilità delle transazioni economiche e delle operazioni finanziarie;
- Verificare periodicamente, anche tramite il supporto di appositi consulenti IT, il corretto utilizzo degli strumenti informatici aziendali;
- Svolgere una regolare attività di reporting nei confronti del Consiglio di Amministrazione e del Revisore Legale del Consorzio.