Modello di organizzazione, gestione e controllo

ai sensi del D.Lgs. n. **231** del 8 giugno 2001

- PARTE SPECIALE -

10

DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

art. 25*octies.1* d.lgs. n. 231/2001

SOMMARIO

1.0 - Introduzione e funzione della parte speciale di delitti in materia di strumenti di pagamento diversi dai contanti e di trasferimento fraudolento di valori

La presente parte speciale (**10**) si riferisce ai delitti in materia di strumenti di pagamento diversi dai contanti e di trasferimento fraudolento di valori di cui all'art. 25*octies.1* del D.Lgs.n.231/2001 e ha come obiettivo che tutti i destinatari, ossia i componenti del Consiglio di Amministrazione, gli apicali e i dipendenti aziendali nonché consulenti e collaboratori, adottino regole di condotta conformi a quanto prescritto dal D.Lgs.n.231/2001 al fine di prevenire il verificarsi dei reati sopra richiamati

In particolare, la presente Parte Speciale ha lo scopo di:

- Fornire le regole di comportamento e le procedure che gli amministratori, i dirigenti ed i dipendenti, nonché i consulenti, liberi professionisti e partner aziendali sono tenuti ad osservare ai fini della corretta applicazione del Modello;
- Fornire all'Organismo di Vigilanza ed ai responsabili delle altre funzioni aziendali che cooperano con il medesimo, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

2.0 - Criteri per la definizione di delitti in materia di strumenti di pagamento diversi dai contanti

La fattispecie del reato è posta in relazione alla commissione di delitti in materia di strumenti di pagamento diversi dai contanti e di trasferimento fraudolento di valori previsto dal Decreto Legislativo n. 184 dell'8 novembre 2021.

Il D.Lgs. n. 184 "Attuazione della direttiva (UE) 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti" ha modificato la rubrica e i commi dell'art. 493*ter* del regio decreto n. 1398 del 19 ottobre 1930, inserendo nel codice penale l'art. 493*quater* (Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti), ampliando contestualmente i reati previsti dal D.Lgs. 231/01.

Incorre nei reati contemplati dall'**art.25*octies.1***, per la tutela del patrimonio oltre che per la corretta circolazione del credito:

- Chi utilizza carta di credito non essendone titolare avendola sottratta;
- Chi utilizza carta di credito non essendone titolare anche avendola solo trovata;
- Chi falsifica carte di credito;
- Chi cede carte di credito falsificate;
- Chi mette in circolazione carte di credito falsificate;
- Chi procura a sé o ad altri un ingiusto profitto alterando il funzionamento di un sistema informatico.

Il reato si consuma al momento dell'utilizzo delle carte o di programmi informatici indipendentemente dal fatto che ci sia stato o meno il conseguimento di un profitto.

Con l'inserimento dell'Art. 512*bis* c.p. (Trasferimento fraudolento dei valori) nel novero dell'Art 25*octies.1* si è inteso contrastare i reati di Ricettazione, Riciclaggio e Impiego di denaro, beni o utilità di provenienza illecita (artt. 648*bis* e 648*ter*).

3.0 - Le fattispecie di reato richiamate dal D.Lgs. n. 231/2001

L'attività normativa si sostanzia nell'introduzione dell'art. 25*octies.1* del D.Lgs. n. 231/01 con relative sanzioni per violazioni e l'estensione della responsabilità amministrativa degli enti ad alcuni illeciti commessi nella commissione dei **delitti in materia di strumenti di pagamento diversi dai contanti e di trasferimento fraudolento di valori**.

I reati contemplati nell'art. 25*octies.1* sono:

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (articolo 493*ter* regio decreto n.1398 del 19 ottobre 1930 modificato da D.Lgs. n. 184 del 8 novembre 2021);
- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (Articolo 493*quater* inserito da D.Lgs. n. 184 del 8 novembre 2021);
- Frode informatica (Articolo 640*ter* c.p. modificato da D.Lgs. n. 184 del 8 novembre 2021);
- Trasferimento fraudolento di valori - (art. 512*bis* c.p. introdotto da D.L.10 agosto 2023 n.105 coordinato con la Legge di conversione n.137 del 9 ottobre 2023).

3.1 - Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti

L'art. 493*ter* punisce chi al fine di trarre profitto per sé e per gli altri utilizza, cede, mette in circolazione carte di credito non collegate al proprio patrimonio personale, ma sottratte, trovate o falsificate.

Per tale delitto si applica all'ente la sanzione pecuniaria **da 300 a 800 quote.**

Salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente, in relazione alla commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:

a) se il delitto è punito con la pena della reclusione inferiore ai dieci anni, la sanzione pecuniaria sino a 500 quote;
b) se il delitto è punito con la pena non inferiore ai dieci anni di reclusione, la sanzione pecuniaria da 300 a 800 quote.

Si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2.

3.2 - Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti

L'art.493*quater* punisce chi al fine di realizzare o far realizzare il reato previsto dall'Art. 493*ter*, utilizza o fa utilizzare ad altri, tramite vendita, cessione od altro, apparecchiature, dispositivi o programmi informatici costruiti per commettere tale reato.

Per il delitto di cui all'articolo 493*quater* e per il delitto di cui all'articolo 640*ter*, nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale, la sanzione pecuniaria è **sino a 500 quote.**

Salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente, in relazione alla commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:

a) se il delitto è punito con la pena della reclusione inferiore ai dieci anni, la sanzione pecuniaria sino a 500 quote
b) se il delitto è punito con la pena non inferiore ai dieci anni di reclusione, la sanzione pecuniaria da 300 a 800 quote.

Si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2.

3.3 - Trasferimento fraudolento di valori

Il reato si configura quando con condotte fraudolenti chiunque **trasferisce fittiziamente** ad altri denaro od altri beni al fine di elidere l'applicazione della confisca (art. 240) e degli altri mezzi di prevenzione patrimoniale, ovvero al fine di agevolare la commissione dei delitti di ricettazione, riciclaggio e autoriciclaggio pur continuando dunque ad avere la disponibilità materiale degli stessi e continuando dunque a goderne.

Con l'ultima modifica apportata all'art.512*bis* c.p. la pena della reclusione da due a sei anni prevista dal primo comma si applica a chi, al fine di eludere le disposizioni in materia di documentazione antimafia, attribuisce fittiziamente ad altri la titolarità di imprese, quote societarie o azioni ovvero di cariche sociali, qualora l'imprenditore o la società partecipi a procedure di aggiudicazione o di esecuzione di appalti o di concessioni.

3.4 - Frode informatica

L'art. 640*ter* è posto a tutela del patrimonio individuale e specificatamente al regolare funzionamento dei sistemi informatici ed alla riservatezza dei dati in essi contenuti.

Questo reato si configura quando 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.

4.0 - Le attività sensibili relative ai delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori

L'art. 6, comma 2, lettera a) del D.Lgs.n.231/2001 indica come uno degli elementi essenziali dei modelli di organizzazione e di gestione previsti dal decreto, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.Lgs.n.231/2001.

Sulla base della normativa attualmente in vigore e dalle analisi svolte in relazione alle fattispecie incriminatrici richiamate dall'art. 25*octies.1* d.lgs. n. 231/2001, si rappresenta un rischio residuo di verificazione che tali reati possano essere commessi nell'interesse o a vantaggio di W.E.M.-Waste Engineering Management s.r.l. tollerabile.

Le principali **Attività Sensibili** sono le seguenti:

1. **Fatturazione**
   Pagamenti presso conti correnti, deposito titoli, deposito a risparmio, carte credito.
2. **Gestione flussi economici e finanziari**
   versamento/pagamento attraverso canali informatici, operazioni su assegni bancari o circolari, operazioni su strumenti finanziari.

Le aree a rischio "diretto" coprono tutte quelle interessate all'attività dell'azienda, in cui le singole card possono essere nominative oppure affidate ad un dipartimento e i pagamenti sono effettuati dai collaboratori.
Lo stesso dicasi laddove vengono adottati sistemi di pagamenti on line.

Per limitare i danni conseguenti ad eventuale commissione di reato l'amministrazione può decidere i massimali disponibili per ciascuno mentre nell'assegnazione di PW per pagamenti on line e per la salvaguardia del proprio sistema informatico o telematico l'amministratore può adottare tutte le misure previste per la sicurezza delle informazioni (Norma ISO 27001).

5.0 - Organi e funzioni aziendali coinvolte

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificamente a rischio risultano essere, anche in riferimento alle attività svolte da W.E.M.-Waste Engineering Management s.r.l., le seguenti:

- Gestione fatturazione;
- Gestione amministrativa;
- Gestione fornitori;
- Gestione acquisti;
- Attività di gestione del personale;

In relazione alle descritte Attività Sensibili, si ritengono particolarmente coinvolti i seguenti organi e funzioni:

1. **Il Consiglio di Amministrazione**
   I profili di rischio attengono alle funzioni di controllo sulle Aree Sensibili, nonché le attività relative alla gestione e controllo sugli acquisti effettuati, approvvigionamento di beni e servizi; gestione delle operazioni finanziarie.
2. **Acquisti, Forniture e Contratti - Gare e Appalti - Tesoreria e Affari Legali - Area Produzione**
   Sono le funzioni che coordinano il piano di sviluppo territoriale e che si occupano dell'organizzazione, verifica e predisposizione della documentazione contrattuale con fornitori e consulenti, oltre che della gestione e programmazione dei pagamenti.

6.0 - Principi e regole di comportamento

Nello svolgimento delle attività sopra descritte e, in generale, delle proprie funzioni, tutti i Destinatari del MOGC 231, devono conoscere e rispettare:

- **la normativa italiana applicabile alle attività svolte;**
- **il Codice Etico Aziendale;**

- **il presente Modello 231;**
- **la normativa Antiriciclaggio;**
- **le procedure P.1 (amministrazione), P-2 (approvvigionamento), P.4 (vendita di servizi) e le linee guida aziendali nonché tutta la documentazione attinente al sistema di organizzazione, gestione e controllo della società.**

Si individuano qui di seguito i principi che informano le specifiche procedure interne dell'azienda, relativi a qualsiasi operazione/attività che coinvolga l'ente nella famiglia dei reati previsti nella presente sezione, in aderenza alla previsione dettata dall'art. 25*octies.1* d.lgs. n. 231/2001.

In linea generale, il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli, in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

Princìpi

Tutte le operazioni/attività devono essere eseguite nel pieno rispetto delle leggi vigenti, del Codice Etico, delle regole contenute nel presente Modello, delle policy e delle procedure o ordini di servizio aziendali, dei valori e delle politiche della società e dentro i limiti delle eventuali deleghe o procure.

La struttura aziendale è articolata in modo tale da soddisfare i requisiti fondamentali di formalizzazione, chiarezza, comunicazione e separazione dei ruoli richiesti in generale nel Decreto.

Conseguentemente, l'amministratore, gli apicali, i dipendenti nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nello svolgimento delle attività a rischio hanno l'espresso obbligo di perseguire i seguenti princìpi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi di controllo specifici.

Questi sono:

- **Segregazione delle attività**

Si richiede l'applicazione del principio di separazione delle attività e dei ruoli che intervengono nelle attività chiave dei processi operativi esposti a rischio tra chi autorizza, chi esegue e chi controlla; in particolare, deve sussistere separazione dei ruoli di gestione di un processo e di controllo dello stesso.

- **Rispetto delle procedure**

L'azienda svolge la propria attività sulla base di disposizioni e procedure formalizzate idonee a fornire i principi di comportamento e le modalità operative per lo svolgimento delle attività sensibili. Le procedure devono definire formalmente le responsabilità e i ruoli all'interno del processo e le disposizioni operative e relativi controlli posti a presidio nelle attività.

- **Poteri autorizzativi e di firma**

Le attività critiche dei processi operativi esposti a rischio reati devono essere espressamente autorizzate.

Inoltre, i poteri autorizzativi e di firma devono essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese ed essere chiaramente definiti e conosciuti all'interno della società.

- **Tracciabilità**

Ogni operazione relativa alle attività sensibili deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

- **Gestione delle segnalazioni**

Raccolta, analisi e gestione delle segnalazioni di fattispecie a rischio per i reati di cui alla presente sezione rilevati da soggetti interni ed esterni all'ente.

- **Riporto all'OdV**

Riferire prontamente all'OdV eventuali situazioni di irregolarità.

7.0 - Principi e norme generali di comportamento

La presente Parte Speciale prevede l'**espresso divieto** a carico di tutti i Destinatari di:

- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- Violare i principi e le procedure esistenti in azienda e/o previste nella presente Parte Speciale.

La presente Parte Speciale prevede, conseguentemente, l'**espresso obbligo** a carico dei soggetti sopra indicati di:

- Tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività amministrativo–contabile;
- Assicurare che il processo di assunzione ed impiego del personale del settore amministrativo sia motivato da effettive necessità aziendali, che sia condotto in maniera trasparente e documentabile e che sia basato su criteri non arbitrari e quanto possibile oggettivi;
- Assicurare l'esistenza nell'impresa di un sistema sia organizzativo, sia amministrativo–contabile adeguati e che ricomprendano anche un sistema gestionale efficace.

8.0 - I controlli dell'Organismo di Vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui alla presente Parte Speciale, commessi nell'interesse o a vantaggio dell'azienda, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello

Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso

I compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i delitti in materia di strumenti di pagamento diversi dai contanti sono i seguenti:

- Proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati alla presente Parte Speciale;
- Monitorare sul rispetto delle procedure per la prevenzione della commistione di reati in materia di strumenti di pagamento diversi dai contanti;
- Esaminare eventuali segnalazioni specifiche provenienti dagli organi sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

FLUSSI INFORMATIVI VERSO ODV: nessun obbligo di flusso informativo (salvo verificazione di evento rilevante ai sensi del D.lgs. 231/2001).

VERIFICA DELL'ODV: non è prevista alcuna verifica, salvo i casi in cui venga comunicata l'insorgenza di un evento rilevante ex D.lgs. 231/2001 o altra rilevante/fondata comunicazione ovvero i casi di verifiche eccezionali dell'ODV.