MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D. LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE H

DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

(ART. 25 OCTIES.1)

APPROVATO DAL CONSIGLIO DI AMMINISTRAZIONE IL 6/12/2023

FINCANTIERI INFRASTRUCTURE OPERE MARITTIME S.P.A.

SEDE LEGALE IN TRIESTE, VIA GENOVA 1

ISCRIZIONE AL REGISTRO DELLE IMPRESE DI TRIESTE N. 01336990328

LE FATTISPECIE DI REATO

La presente Parte Speciale si riferisce ai delitti in materia di strumenti di pagamento diversi dai contanti, richiamati dall'art. 25 octies.1 del D. Lgs. 231/2001, ed in particolare riporta le singole fattispecie di reato considerate rilevanti per la responsabilità amministrativa di Fincantieri Infrastructure Opere Marittime S.p.A.. Individua inoltre le cosiddette attività "sensibili" (quelle dove è teoricamente possibile la commissione del reato e che sono state individuate nell'ambito dell'attività di *risk assessment*) specificando i principi comportamentali ed i presidi di controllo operativi per l'organizzazione, lo svolgimento e la gestione delle operazioni svolte nell'ambito delle sopracitate attività "sensibili".

In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di Fincantieri Infrastructure Opere Marittime S.p.A. i seguenti reati:

INDEBITO UTILIZZO E FALSIFICAZIONE DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (300-800 QUOTE) (ART. 493-TER C.P.)

Tale reato si realizza quando un soggetto, al fine di trarre profitto per la Società, 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. La fattispecie si applica inoltre qualora si falsifichino o alterino gli strumenti o i documenti di cui al primo periodo, ovvero si possiedano, cedano o acquisiscano tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

DETENZIONE E DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A COMMETTERE REATI RIGUARDANTI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (FINO A 500 QUOTE) (ART. 493-QUATER C.P.)

Il reato è applicabile qualora un soggetto, produca, importi, esporti, venda, trasporti, distribuisca, metta a disposizione o in qualsiasi modo procuri 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.

FRODE INFORMATICA NELL'IPOTESI AGGRAVATA DALLA REALIZZAZIONE DI UN TRASFERIMENTO DI DENARO, DI VALORE MONETARIO O DI VALUTA VIRTUALE (FINO A 500 QUOTE) (ART. 640-TER, COMMA 2 C.P.)

Tale fattispecie reato si realizza quando un soggetto, 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, procuri un ingiusto profitto con altrui danno.

IDENTIFICAZIONE DELLE ATTIVITA' A RISCHIO REATO

Le attività che la Società ha individuato come sensibili, nell'ambito dei delitti informatici, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della Segreteria di Direzione, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Tali attività sono di seguito riepilogate:

- Gestione delle carte di credito aziendali.
- Gestione dei flussi monetari e finanziari.
- Falsificazione di documenti informatici relativi, ad esempio, a rendicontazione in formato elettronico di attività e/o a attestazioni elettroniche di qualifiche o requisiti della Società.
- Accesso ai sistemi informatici aziendali o di terze parti, che contengono:
    - brevetti, disegni, attività di R&S;
    - dati di marketing;
    - informazioni riservate di enti pubblici;
    - informazioni bancarie;
    - parametri per l'attivazione di servizi;
    - dati di fatturazione o di credito;
    - dati relativi a pagamenti.
- Gestione di strumenti e dispositivi e programmi, da parte di soggetti aziendali e amministratori di sistema, mediante i quali possono:
    - essere intercettate informazioni rilevanti di terze parti o impedite comunicazioni anche alla Pubblica Amministrazione
    - danneggiare un sistema informatico o telematico, nell'ambito delle strutture di un concorrente.

PRINCIPI GENERALI DI COMPORTAMENTO

Coerentemente con i principi deontologici aziendali di cui alla Parte Generale del Modello Organizzativo ex D. Lgs. 231/2001 e del Codice di Comportamento adottati dalla Società, nello svolgimento delle attività sensibili sopra citate, tutti i Destinatari del Modello sono tenuti ad osservare i seguenti principi di comportamento e controllo.

In via generale, a tali soggetti è richiesto quanto segue:

- i flussi finanziari della Società, sia in entrata sia in uscita sono costantemente monitorati e tracciati;
- per la gestione dei flussi in entrata e in uscita, sono utilizzati esclusivamente i canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione Europea o enti creditizi/finanziari situati in uno Stato extracomunitario che imponga obblighi equivalenti a quelli previsti dalle leggi sul riciclaggio e autoriciclaggio preveda il controllo del rispetto di tali obblighi;
- le operazioni che comportano utilizzo o impiego di risorse economiche o finanziarie devono avere una causale espressa e sono documentate e registrate in conformità ai principi di correttezza e trasparenza contabile;
- la Società, ai fini dell'attuazione delle decisioni di impiego delle risorse finanziarie, si avvale soltanto di intermediari finanziari e bancari sottoposti ad una regolamentazione di trasparenza e correttezza conformi alla disciplina dell'Unione Europea;
- sono rispettati i termini e le modalità previsti dalla normativa applicabile per la predisposizione delle dichiarazioni fiscali periodiche e per i conseguenti versamenti relativi alle imposte sui redditi e sul valore aggiunto.

PROCEDURE DI CONTROLLO

Con riferimento ai delitti in materia di strumenti di pagamento diversi dai contanti, si rimanda ai principi di controllo riportati nella Parte Speciale B – Reati informatici e nella Parte Speciale A – Reati contro la Pubblica Amministrazione (con riferimento ai presidi di controllo individuati per i processi: Gestione dell'infrastruttura tecnologica, Contabilità, Bilancio e rapporti con gli Organi di Controllo e Gestione dei flussi monetari e finanziari).

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito ulteriori presidi di controllo operativi a prevenzione della commissione dei delitti in materia di strumenti di pagamento diversi dai contanti, con particolare riferimento ai processi strumentali alla commissione dei reati quali la gestione dei flussi monetari e finanziari.

- ogni movimentazione di cassa deve essere autorizzata dai soggetti dotati di idonei poteri e supportata da opportuna documentazione;
- le carte di credito attingono al conto corrente della Società, e possono essere esclusivamente utilizzate per le cd. "spese di cantiere". La Società non ammette l'uso promiscuo delle carte di credito, le quali sono provviste del nominativo del dipendente al quale esse sono assegnate;
- i pagamenti sono effettuati tramite strumenti che ne assicurano la tracciabilità (e.g. bonifici bancari, etc.) e, solo in via residuale e (ossia per gli importi massimi previsti dalle procedure vigenti in FIOM S.P.A.) previa autorizzazione, tramite l'utilizzo di contanti nel rispetto dei limiti previsti dalle leggi vigenti;
- i pagamenti devono sempre essere effettuati in favore del soggetto che ha erogato il bene e/o il servizio, con obbligo di effettuare controlli specifici sull'identità di interposte persone;
- le operazioni che comportano l'utilizzazione o impiego di risorse economiche o finanziarie devono sempre avere una causale espressa e devono essere documentate e registrate in conformità ai principi di correttezza e trasparenza contabile;
- gli incassi e i pagamenti della Società nonché i flussi di denaro devono sempre essere tracciabili e provabili documentalmente;
- sono previsti la verifica della regolarità dei pagamenti anche con riferimento alla coincidenza tra destinatario/ordinante e controparte effettivamente coinvolta nella transazione e il controllo della correttezza dei flussi finanziari aziendali con riferimento ai pagamenti verso terzi;
- per la gestione dei flussi in entrata e in uscita, sono utilizzati esclusivamente i canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione Europea o enti creditizi/finanziari situati in uno Stato extracomunitario che imponga obblighi equivalenti a quelli previsti dalle leggi sul riciclaggio e preveda il controllo del rispetto di tali obblighi;
- sono effettuati controlli formali e sostanziali e un costante monitoraggio dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi, tenendo conto della sede legale della società controparte, degli istituti di credito utilizzati, di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;
- la Società assicura il tracciamento del numero delle carte di credito assegnate ai dipendenti risalendo dal conto corrente ad essa intestata;
- è vietato utilizzare conti correnti in forma anonima o con intestazione fittizia, né in Italia né presso altri Stati esteri;
- i titolari delle firme elettroniche e/o digitali sono individuati in base ai regolamenti contrattuali con le Autorità di Certificazione emittenti delle firme;
- la custodia e l'utilizzo dei dispositivi di firma elettronica e/o digitale sono rimessi ai titolari degli stessi e devono conformarsi ai regolamenti contrattuali con le Autorità di Certificazione emittenti delle firme.