PARTE SPECIALE "G"

Delitti in materia di strumenti di pagamento diversi dai contanti
(art. 25 octies. 1 del Decreto)

G.1 Delitti in materia di strumenti di pagamento diversi dai contanti

La Parte Speciale "G" è finalizzata alla prevenzione specifica dei seguenti reati:

- **Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti** (art. 493 ter);
- **Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti** (art. 493 quater);
- **Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale** (art. 640 ter c.p.).

G.2 Principi generali di comportamento applicabili I delitti in materia di strumenti di pagamento diversi dai contanti (art. 25 *bis* del Decreto).

Per quanto concerne i reati di cui all'art. 25 *octies.1* del Decreto, l'esito delle attività di *risk assessment* svolte ha portato a ritenere la concreta possibilità di commissione degli stessi applicabile; tuttavia, di minore rilevanza in virtù dell'attività svolta dalla Società. Pertanto, per essi trovano applicazione i principi generali di comportamento di seguito descritti, nonché i principi generali di controllo descritti nella Parte Generale ed i principi generali di comportamento descritti nel Codice Etico.

A tutti coloro che operano per conto della Società è fatto divieto di:

- utilizzare indebitamente carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o a all'acquisto di beni o alla prestazione di servizi. Nello specifico, per strumenti di pagamento devono intendersi (i) un dispositivo, (ii) un oggetto o (iii) un record protetto, immateriale o materiale, o una loro combinazione, diverso dalla moneta avente corso legale che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali (ad es., home banking, criptovalute, ecc.);
- falsificare o alterare gli strumenti di pagamento o i documenti summenzionati;
- possedere, cedere o acquisire gli strumenti di pagamento o documenti summenzionati di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi;

- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico, o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, al fine di ottenere un ingiusto vantaggio con altrui danno, producendo un trasferimento di denaro, di valore monetario o di valuta virtuale; commettere qualsiasi delitto contro la fede pubblica, contro il patrimonio o che comunque offenda il patrimonio, avente ad oggetto strumenti di pagamento diversi dai contanti.

G.3 Aree a rischio

Con riferimento ai reati di cui alla presente Parte Speciale, all'esito delle attività di *risk assessment*, sono state individuate le seguenti principali aree di attività a rischio:

G.3.1 Gestione amministrativa del personale, delle missioni e dei rimborsi spese;

G.3.2 gestione degli omaggi e delle spese di rappresentanza;

G.3.3 gestione della finanza e tesoreria.

Le aree a rischio sono state prese in considerazione ai fini della definizione delle procedure di controllo e, più in generale, ai fini dell'adeguamento dell'attuale sistema di controllo interno.

Con riferimento alle suddette aree vengono di seguito illustrati - in forma sintetica ed a titolo meramente esemplificativo – i principi generali di controllo, le attività sensibili, le modalità commissive ed i principi di controllo preventivo adottati dalla Società.

Principi generali di controllo:

- previsione di un sistema di deleghe e procure, nonché di un sistema organizzativo (compiti, ruoli e responsabilità formalizzati);
- esistenza di specifici protocolli aziendali che descrivono ruoli, responsabilità, attività, modalità operative e controlli;
- segregazione dei compiti tra:
  - chi richiede, chi autorizza e chi effettua i pagamenti;
  - chi esegue e chi controlla/autorizza le operazioni;
- tracciabilità e verificabilità *ex post* di ogni operazione relativa alle attività sensibili;
- archiviazione della documentazione, ivi inclusi documenti e/o scritture contabili, al fine di impedirne l'occultamento o la distruzione e di garantire la tracciabilità del processo.

G.3.1 Gestione amministrativa del personale, delle missioni e dei rimborsi spese

Principali funzioni aziendali coinvolte

1) Risorse Umane, Organizzazione

Attività sensibili

1) *Autorizzazione delle missioni e delle note spese*
2) *Gestione degli anticipi per missione*
3) *Rendicontazione e rimborso delle spese sostenute*
4) *Raccolta ed elaborazione dei dati relativi alla gestione del personale*
5) *Autorizzazione delle retribuzioni del personale*
6) *Determinazione, gestione e versamento dei trattamenti previdenziali, contributivi e assistenziali del personale*

Modalità di commissione dei reati o condotte strumentali alla commissione

- Un esponente della Società, assegnatario di una carta di credito aziendale, potrebbe cedere tale carta ad un soggetto terzo non abilitato all'utilizzo al fine di conseguire un illecito profitto per la medesima Società.

Principi di controllo

Devono intendersi qui integralmente richiamati i principi di controllo indicati nella Parte Speciale "A" (punto A.3.3).

In aggiunta a tali principi di controllo, la Società si ispira anche ai seguenti:

- Verifica di riconciliazione tra le spese sostenute tramite carta di pagamento aziendale/carta carburante (sulla base dell'estratto conto della carta) e la nota spese compilata dal personale interessato;
- Tracciabilità dell'assegnazione e revoca della carta di credito aziendale/carta carburante/ buoni pasto;
- Formale comunicazione del furto/smarrimento della carta di credito aziendale/carta carburante/buoni pasto.

G.3.2 Gestione degli omaggi e delle spese di rappresentanza

Principali funzioni aziendali coinvolte

1) Amministrazione, Finanza e Controllo

Attività sensibili

a. gestione degli omaggi;

b. gestione delle spese di rappresentanza.

Modalità di commissione dei reati o condotte strumentali alla commissione

- Un esponente della Società, assegnatario di una carta di credito aziendale, potrebbe cedere tale carta ad un soggetto terzo non abilitato all'utilizzo al fine di conseguire un illecito profitto per la medesima Società.

Principi di controllo

Devono intendersi qui integralmente richiamati i principi di controllo indicati nella Parte Speciale "A" (punto A.3.9).

In aggiunta a tali principi di controllo, la Società si ispira anche ai seguenti:

- Definizione delle tipologie di spese sostenibili con le carte di pagamento aziendali, dei relativi limiti e delle modalità di rendicontazione, nonché autorizzazione di eventuali deroghe;
- Verifica di riconciliazione tra le spese sostenute tramite carta di pagamento aziendale (sulla base dell'estratto conto della carta) e la nota spese compilata dal personale interessato.

G.3.2 Gestione della finanza e della tesoreria

Principali funzioni aziendali coinvolte

1. Amministratore Delegato
2. Amministrazione, Finanza e Controllo

Attività sensibili

1. *Gestione delle attività di apertura, variazione e chiusura dei conti correnti*
2. *Gestione degli incassi*
3. *Gestione dei pagamenti*
4. *Gestione della piccola cassa*
5. *Contabilizzazione delle movimentazioni finanziarie e riconciliazione dei conti*

Modalità di commissione dei reati o condotte strumentali alla commissione

- Un esponente della Società, assegnatario di una carta di credito aziendale, potrebbe cedere tale carta ad un soggetto terzo non abilitato all'utilizzo al fine di conseguire un illecito profitto per la medesima Società.

Principi di controllo

Devono intendersi qui integralmente richiamati i principi di controllo indicati nella Parte Speciale "A" (punto A.3.8).

In aggiunta a tali principi di controllo, la Società si ispira anche al seguente:

- formale comunicazione del furto/smarrimento delle credenziali di accesso all'applicazione "homebanking".