

GIOSI 2 S.R.L.

3.5 PARTE SPECIALE

SEZIONE VI – DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (Art. 25 *octies* 1 D.lgs. n. 231/2001)

Una premessa introduttiva

Il 14 dicembre 2021, con l'entrata in vigore del D.Lgs 8 novembre 2021 n. 184, in attuazione della Direttiva UE 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, è stato introdotto l'art. 25 *octies* 1, rubricato "Delitti in materia di strumenti di pagamento diversi dai contanti".

La modifica ha comportato un rilevante arricchimento del novero dei reati presupposto, estendendo l'ambito applicativo delle sanzioni alle fattispecie di "Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti" di cui all'art. 493 ter c.p. e di "Frode informatica" di cui all'art. 640 ter c.p. come modificate dall'art. 2 del medesimo decreto.

L'art. 25 *octies* 1 annovera altresì quale ulteriore reato presupposto della responsabilità amministrativa dell'ente, il delitto di "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti" di cui all'art. 493 quater c.p., fattispecie di nuovo conio ed introdotta nel corpus del codice penale proprio con l'emanazione del D.Lgs. 184/2021.

In relazione agli artt. 493 *quater* e 640 *ter* c.p. è doveroso precisare che tali delitti vengono in rilievo ai fini della responsabilità dell'ente, solo ove commessi nell'ipotesi aggravata della realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale. La norma in parola prevede infine quali fattispecie presupposto della responsabilità dell'ente derivante da reato, una seria vasta ed indeterminata di delitti, con la previsione di una clausola di riserva avente carattere di norma di chiusura.

2. La descrizione dei reati

Si riporta di seguito una breve descrizione dei reati contemplati dall'art. 25-*octies* 1 del Decreto.

2.1. (art. 25 *octies* 1 comma 1)

Il comma 1 dell'art. 25 *octies* 1 prevede che: *" In relazione alla commissione dei delitti previsti dal codice penale in materia di strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:*

a) per il delitto di cui all'art. 493 ter, la sanzione pecuniaria da 300 a 800 quote;

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

* L'art. 493 *ter* c.p. richiamato all'art. 25 octies 1 comma 1 lett. a) dispone che *“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 è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.”*

Come anticipato nella premessa introduttiva l'art. 2 del D.Lgs n. 184/2021 ha apportato delle modifiche alla fattispecie in attuazione della Direttiva UE n. 2019/713 del Parlamento Europeo e del Consiglio del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni dei mezzi di pagamento diversi dai contanti. L'intervento dell'Unione Europea in materia è dovuto al carattere transfrontaliero di tali reati, conseguenza della loro modalità digitale di realizzazione.

Le frodi e le falsificazioni dei mezzi di pagamento diversi dai contanti rappresentano una delle forme attraverso le quali la criminalità organizzata finanzia le proprie attività criminose nonché una seria limitazione allo sviluppo del mercato unico digitale e delle tecnologie di pagamento, in quanto ledono la fiducia dei consumatori nella sicurezza degli scambi economici, tra cui gli acquisti effettuati on line.

La ratio dell'intervento normativo risiede dunque nell'esigenza di potenziare il contrasto alle summenzionate frodi e falsificazioni, operato attraverso l'ampliamento dell'ambito di applicazione dei delitti di cui all'art. 493 *ter* a tutti gli strumenti di pagamento diversi dai contanti, compresi quelli immateriali, ricompresi nella definizione fornita dall'art. 1 comma 1 lett a) del citato decreto, ovvero ogni *“dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a 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”*.

Secondo la dottrina i delitti di cui all'art. 493 *ter* si caratterizzano per la plurioffensività poiché ledono non solo il patrimonio individuale, ma anche interessi afferenti la categoria dell'ordine pubblico e della fede pubblica.

Conformemente la giurisprudenza ha individuato il bene giuridico tutelato nell'interesse pubblico a che il sistema elettronico di pagamento venga usato in maniera corretta a garanzia delle fede pubblica ed a prevenzione del riciclaggio (cfr. Cass. Sez. VI, n. 29821/2012).

Oggetto materiale dei reati di cui all'art. 493 *ter* sono le **carte di credito o di pagamento** o qualsiasi **altro documento con analoga funzione** e dunque, ogni supporto che presenta la medesima utilità economica.

Sono *carte di credito o di pagamento* le tessere munite di una banda magnetica e/o microcircuiti sui quali sono impressi i dati di identificazione del titolare, i limiti e le modalità di utilizzo, nonché gli estremi del rapporto con l'azienda o l'ente che ha rilasciato il documento abilitante alla fruizione dei servizi (bancomat, carte di credito, carte prepagate).

La giurisprudenza ha individuato i documenti con analoga funzione in strumenti di pagamento quali ad esempio:

- la tessera a banda magnetica a scalare per il pagamento del pedaggio autostradale "via card" (Cass. Sez. II n. 36295/2005);
- la tessera carburanti (Cass. S.U. n. 22902/2001);
- le tessere telefoniche prepagate;
- i vaglia postali veloci.

L'art. 493 ter c.p. è una disposizione a più norme poiché scandisce tre autonome incriminazioni di forme diverse di abuso degli strumenti di pagamento diversi dai contanti e costituisce una norma a più fattispecie in quanto sono descritte più condotte tra loro alternative e non cumulative.

Le condotte descritte nella norma sono le seguenti:

a) utilizzare indebitamente, cioè senza esserne il titolare, carte di credito o di pagamento o qualsiasi altro documento che abiliti al prelievo di denaro o all'acquisto di beni o alla prestazione di servizi, al fine di trarne profitto per sé o per altri.

Il materiale possesso dei detti strumenti di pagamento diverso dai contanti non è presupposto necessario per l'integrazione del reato, poiché è infatti sufficiente che l'agente attraverso l'immissione dei dati ricognitivi ed operativi di una valida carta di credito altrui di cui non ha la materiale disponibilità, effettui delle transazioni non autorizzate dal titolare (Cass. Sez. II n. 47725/2014)

L'utilizzo della carta è indebito quando manca il consenso del titolare o sono violate le prescrizioni e le modalità di impiego stabilite dall'emittente o dall'ente erogatore.

La Corte di Cassazione, al fine di individuare la sfera applicativa della norma, ha precisato che la titolarità della carta deve essere sostanziale, legale, attuale e non formale, ovvero derivante dall'intestazione o dal mero possesso di essa. Di conseguenza il soggetto, apparente titolare della carta di credito, commette il delitto se utilizza una carta il cui contratto è estinto o è stato sospeso per qualsiasi causa, non essendo più titolare del rapporto contrattuale con l'emittente; in tale ipotesi, ai fini della configurabilità del reato sotto il profilo soggettivo è necessario che l'agente sia consapevole del recesso e che quindi vi sia stata la comunicazione all'utente della revoca all'autorizzazione della carta.

La Cassazione, inoltre, ha affrontato anche la tematica della configurabilità o meno del reato di utilizzo indebito di una carta di credito allorquando l'utilizzatore, pur non essendone titolare, si serva del documento su autorizzazione o, comunque, senza opposizione dell'avente diritto all'uso. La giurisprudenza, a tal proposito, ha affermato che l'unica ipotesi in cui non si ravvisa l'abusività, nel caso di utilizzazione di carta da parte del non titolare, è quello di cosiddetto **uso indiretto** del documento da parte del soggetto legittimato, ovvero quando quest'ultimo si serve di un terzo come "*longa manus*" o mero strumento esecutivo di un'operazione che non necessita la sottoscrizione di alcun atto, come ad esempio, l'ipotesi di pagamento del pedaggio autostradale mediante carta di credito, per cui è sufficiente inserire il documento nell'apposito congegno automatico.

Ai fini della consumazione del reato occorre inoltre che il soggetto agente utilizzi la carta o altro strumento di pagamento al fine di trarne profitto per sé o per altri.

b) falsificare o alterare carte di credito o di pagamento o qualsiasi altro documento analogo.

La **falsificazione** consiste nella materiale creazione da parte di soggetto non legalmente autorizzato, di una nuova carta di credito artefatta (o di altro documento) solo apparentemente riconducibile all'istituto emittente, ma in realtà priva di ogni collegamento negoziale con quest'ultimo e tale da far apparire al lettore magnetico che la medesima proviene dall'emittente ed è utilizzata dal soggetto legittimato.

L'**alterazione** presuppone l'esistenza di una carta regolarmente creata dall'emittente e si concretizza nella sua artificiosa manipolazione attraverso la modificazione di alcuni dati rilevanti quali l'intestazione, la data di scadenza, il nome del titolare, la banda magnetica o dei dati in essa inseriti che permettono l'accesso ai servizi o, infine dei codici, per consentirne un uso diverso per qualità e quantità rispetto a quello previsto dall'ente emittente (limiti di spesa o di prelievo)

c) possedere, cedere o acquistare tali strumenti di pagamento diverso dai contanti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi, al fine di trarne profitto per sé o per altri.

Il concetto di possesso deve essere inteso in senso penalistico, ovvero come autonoma disponibilità della *res* accompagnata dall'*animus rem sibi habendi*, ovvero dall'animo di tenere la cosa presso di sé.

Le condotte di cessione o acquisizione ricomprendono tutte le possibili modalità di trasferimento a terzi delle carte, dei documenti e degli strumenti di pagamento diversi dai contanti, ivi comprese quelle a titolo gratuito ovvero oneroso.

La provenienza illecita, postula infine, che il possesso della carta di credito o del documento analogo o dello strumento di pagamento diverso dai contanti debba derivare da un illecito civile, amministrativo o penale di natura contravvenzionale, poiché nell'ipotesi in cui sia ricollegabile ad un delitto si configurerebbe il reato di ricettazione di cui all'art. 648 c.p.p.

* L'art. 493 *quater* c.p. richiamato dall'art. 25 octies 1 comma 1 lett. b) prevede che *"Salvo che il fatto costituisca più grave reato, 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 sé o altri apparecchiature, dispositivi o programmi informatici che per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificatamente adattati al medesimo scopo, è punito con la reclusione fino a due anni e con la multa fino a 1.000 euro."*

* L'art. 640 *ter* c.p. (art. 25 octies 1 c.1 lett. b) prevede che *"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, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032."*

La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'art. 640, ovvero se il fatto

produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore di sistema."

2.2. (art. 25 octies 1 comma 2)

Il comma 2 dell'art. 25 octies 1 stabilisce che *"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 a 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, con la sanzione da 300 a 800 quote.

3. SOGGETTI DESTINATARI DELLA PRESENTE SEZIONE

La presente Sezione si riferisce a comportamenti posti in essere dai seguenti soggetti:

- (i) i Destinatari (inclusi quindi gli Esponenti Aziendali tutti) del presente Modello in generale;
- (ii) i Destinatari, comunque, operanti nelle "attività a rischio" con particolare riferimento, ma senza limitazione, ai soggetti operanti nella Funzione amministrativa e di gestione dei pagamenti;
- (iii) i membri del Consiglio di Amministrazione, con particolare riferimento al Presidente del Consiglio di Amministrazione e all'Amministratore delegato;
- (iv) i Collaboratori Esterni, *Partner Commerciali* e Fornitori della Società, *Stageur*.

Obiettivo della presente Sezione è che tali soggetti si attengano - nella misura in cui gli stessi siano coinvolti nello svolgimento delle c.d. "attività a rischio" e in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti della Società - a regole di condotta conformi a quanto prescritto nella presente Sezione e nel Modello e nelle altre sue parti integranti, in quanto applicabili, al fine di prevenire e impedire il verificarsi dei reati inerenti gli strumenti di pagamento diversi dai contanti.

In particolare, la presente Sezione ha la funzione di:

- fornire un elenco dei principi generali e delle regole specifiche cui gli Esponenti Aziendali, i Consulenti, i Fornitori ed i *Partner* in relazione al tipo di rapporto in essere con la Società, sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV e ai responsabili delle altre funzioni aziendali, chiamati a cooperare con lo stesso, gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandate.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, i Destinatari sono tenuti a conoscere ed a rispettare tutte le regole e i principi contenuti nei seguenti documenti, che sono parte integrante e sostanziale del presente Modello e del sistema di organizzazione, controllo e gestione della Società:

- il Codice Etico;

- ogni altra documentazione relativa al sistema di controllo interno;
- le procedure, se in essere.

In quanto Destinatari della presente Sezione ai Collaboratori Esterni, *Partners Commerciali* e Fornitori deve essere resa nota l'adozione del Modello e del Codice Etico da parte della Società.

4. ATTIVITA' A RISCHIO

Con l'introduzione dell'art. 25 *octies* 1 nel D.lgs. 231/01, le attività a rischio inerenti la presente Sezione sono teoricamente tutte quelle svolte dalla Società che, in violazione della normativa vigente, potrebbero portare alla realizzazione dei delitti in materia di utilizzo di mezzi di pagamento diversi dai contanti.

Avuto riguardo all'organizzazione della GIOSI 2 SRL, si rileva che i pagamenti sia in entrata che in uscita avvengono quasi esclusivamente a mezzo bonifici bancari.

La società possiede una sola carta di credito intestata e nella disponibilità del Presidente del Consiglio di amministrazione e numero sette (7) "carte carburante" associate a singoli ed identificati mezzi di trasporto e che pertanto, il rischio di commissione dei reati previsti dalle fattispecie richiamate dall'art. 25 *octies* comma 1 lett. a) del Decreto è praticamente inesistente e assolutamente residuale.

Considerato inoltre che la società, nello svolgimento della propria attività, utilizza solo ed esclusivamente dispositivi, apparecchiature e programmi informatici regolarmente acquistati, autentici e certificati, il reato di cui all'art. 493 *quater* non è neppure astrattamente ipotizzabile.

Tenendo conto degli esiti del *risk assessment* vengono qualificate "a rischio" le seguenti attività:

- Gestione e controllo della carta di credito aziendale
- Gestione e controllo delle c.d "carte carburante"
- Gestione e controllo dei sistemi informatici o telematici

Per ciascuna di esse vengono elaborati specifici protocolli, che debbono essere necessariamente applicati.

In ogni caso, per tutte le attività a rischio devono sempre essere rispettati i principi di comportamento e di controllo indicati al § 5 della presente Sezione.

4.1. Gestione e controllo della carta di credito aziendale

Come indicato nel paragrafo che precede la società GIOSI 2 S.r.l. dispone di una sola carta di credito aziendale utilizzata esclusivamente dal Presidente del Consiglio di amministrazione per acquisti di modica entità di prodotti on line e/o su e-commerce.

L'utilizzo della carta di credito da parte di soggetti terzi (non titolari) legittimati ed espressamente autorizzati dal Presidente del Cda, oltre a rivestire ipotesi residuale, dovrà avvenire solo nei casi in cui l'operazione non necessiti la sottoscrizione di un atto.

Della detta operazione il soggetto autorizzato dovrà immediatamente dare conto al Presidente del Cda ed all'Ufficio amministrazione.

4.2. Gestione e controllo delle c.d. "carte carburante"

A far data dal settembre 2017 la società GIOSI 2 S.r.l. ha stipulato un contratto con la società Wex Europe Services srl in virtù del quale, sono state attivate sette "Esso card" anche dette schede carburante, della durata di 3 anni, di cui sei (6) abbinata ad uno specifico automezzo identificato per targa ed una (1) scheda libera non associata ad una specifica targa, poichè utilizzata per i veicoli sostitutivi.

I singoli utilizzatori possono effettuare il rifornimento presso tutti i distributori Esso presenti sul territorio nazionale ed al termine dell'operazione devono farsi rilasciare uno scontrino ove sono riportati i dati del distributore, i dati identificativi dell'operazione (MID, POS, data, ora, tipo di carburante, numero PAN) e comunque tutti i dati che consentono di associare l'operazione alla singola carta Esso utilizzata.

In forza del sopra richiamato contratto, la società Wex Europe Services con cadenza settimanale invia alla Giosi 2 S.r.l. le fatture per l'addebito degli acquisti, composte da dettagliata descrizione del consumo abbinato alla singola targa, e da parte riepilogativa per la registrazione in contabilità.

Così come già previsto dalla procedura interna, la società dovrà effettuare un controllo volto a riconciliare le singole fatture con gli scontrini ad esse riferibili nonché elaborare con cadenza mensile il Documento integrativo degli acquisti di carburante, che dovrà a sua volta riportare per ogni veicolo, il totale dei chilometri percorsi, il costo del carburante ed il costo complessivo fatturato con indicazione dell'imponibile e dell'IVA.

4.3. Gestione e controllo dei sistemi informatici o telematici

La società GIOSI 2 SRL dispone di un CED dedicato a tutti server specifici tra cui controller di dominio, posta elettronica, contabilità, produzione , documentale , file sharing e server di back up.

Ogni accesso alle applicazioni e ai dati personali deve essere condizionato da una procedura di autenticazione, attraverso la richiesta di credenziali di autenticazione composta da un nome utente, identificativo dell'incaricato e da una password rispondente ai requisiti ed alle regole fissate quanto a lunghezza e modalità di formazione.

Per quanto riguarda la gestione e monitoraggio degli accessi a sistemi informatici e telematici è prevista dalla società la seguente procedura:

- costituzione di un polo di competenza in grado di fornire il necessario supporto consulenziale e specialistico per le problematiche legate alla tutela legale del software;
- pianificazione delle attività di sicurezza informatica;
- applicazione di misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute;
- attuazione di un sistema di protezione idoneo ad identificare e autenticare univocamente gli utenti che intendono ottenere l'accesso ad un sistema elaborativo o trasmissivo;
- attuazione di un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici;
- procedura di salvataggio dati attraverso back up giornalieri.

Al fine di prevenire i reati di cui alla presente sezione è fatto divieto ai singoli operatori di:

- > alterare in qualsiasi modo il funzionamento di un sistema informatico/telematico ovvero intervenire in qualsiasi modo, e senza averne diritto, su dati, informazioni e programmi;
- > utilizzare la userid o la password di altro dipendente;
- > comunicare a terzi estranei alla Società le proprie chiavi d'accesso nonché la password;
- > accedere ad un sistema informatico e/o telematico senza autorizzazione della Società;
- > lasciare incustodite postazioni di lavoro con la console aperta ed attiva;
- > collegare ai propri computer ogni tipo di periferica proveniente dall'esterno, senza esplicita autorizzazione dell'Amministratore di sistema.

5. PRINCIPI GENERALI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO

La presente Sezione si riferisce a comportamenti posti in essere da Amministratori, Responsabili di Funzione e dipendenti (nel seguito "Esponenti Aziendali") operanti nelle aree in cui sono svolte attività a rischio nonché da Collaboratori esterni (di seguito tutti definiti i "Destinatari").

Nell'espletamento della propria attività per conto della Società, tutti i Destinatari devono rispettare il Codice Etico e le procedure aziendali, ove esistenti, nonché osservare i seguenti principi generali;

- stretta osservanza delle leggi e dei regolamenti che disciplinano le attività aziendali con particolare riferimento alle attività a rischio per i reati in materia di mezzi di pagamento diversi dai contanti e di frode informatica;
- stretta osservanza delle regole definite dal codice Etico, dal presente Modello, dalle procedure e norme di comportamento interne ed, in particolare delle norme e delle prassi operative definite dal Sistema di Gestione Integrato Qualità Ambiente Sicurezza della Società;
- redazione e conservazione della documentazione necessaria a fornire evidenza del rispetto delle prescrizioni in materia mezzi di pagamento diversi dai contanti, in modo tale da garantire un controllo efficace sui comportamenti e sulle attività della Società;
- immediata segnalazione all'ODV di qualsiasi circostanza o comportamento posto in essere da soggetti correlati a GIOSI 2 S.r.l. che destino anche il solo sospetto di attività irregolari nell'utilizzo dei mezzi di pagamento o dei sistemi informatici.

Tutti i soggetti coinvolti nelle varie attività interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nella presente Sezione.

Fatto salvo il rispetto della normativa vigente in materia, del Codice Etico della Società e delle procedure aziendali, tutti i Destinatari devono:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività interessate dalla presente sezione;
- astenersi dal porre in essere, collaborare o dar causa alla realizzazione di comportamenti tali che, considerati individualmente o collettivamente, integrino direttamente o indirettamente le fattispecie di reato rientranti tra quelle richiamate dall'art. 25 *octies* 1 del D.lgs 231/2001;
- osservare le regole contenute nelle procedure ed, in generale, nella documentazione adottata in attuazione dei principi di riferimento previsti nella presente Parte Speciale.

Tutti i Destinatari sono tenuti a segnalare all'Organismo di Vigilanza qualunque operazione che presenti indici di anomalia e, ove necessario, previa opportuna

consultazione con il proprio Responsabile, sono tenuti a sospendere/interrompere il rapporto. Le segnalazioni nonché le eventuali interruzioni dei rapporti devono essere effettuate con la massima tempestività.

5.1. Contratti

Ai Consulenti, *Partner* e Fornitori deve essere resa nota l'adozione del Modello e del Codice Etico da parte della Società e, pertanto, i contratti stipulati con i Collaboratori Esterni, i *Partner* Commerciali ed i Fornitori devono contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al Decreto nonché del Modello.

5.2. Gestione della formazione e dell'informazione

La predisposizione ed implementazione del piano di formazione ed informazione sui comportamenti da adottare, ecc. è un'attività di competenza dell'**Amministratore delegato**, che si può avvalere anche della collaborazione di strutture esterne.

La formazione deve costituire un'attività costante e continua e deve coinvolgere tutti i lavoratori, con particolare riferimento alle funzioni "sensibili" rispetto ai rischi potenziali di commissione dei reati di cui alla presente sezione di Parte speciale.

Deve essere previsto un programma di formazione, ripartito tra apici e subordinati, con la relativa frequenza.

6. I COMPITI DELL'ORGANISMO DI VIGILANZA

I compiti dell'Organismo di Vigilanza, in relazione alla prevenzione dei reati elencati nella presente Sezione sono, in aggiunta a quelli di carattere generale previsti nella Parte Generale del Modello e nel regolamento dell'OdV stesso, i seguenti:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello (Parte Generale e Speciale) in ottica di prevenzione della commissione dei reati previsti nella presente Sezione;
- verificare costantemente la completezza e l'efficacia delle disposizioni della presente Sezione;
- proporre che vengano emanate ed aggiornate le istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle "attività a rischio", come individuate nella presente Sezione;
- svolgere ogni accertamento ritenuto opportuno su singole operazioni a rischio;
- vigilare sull'effettiva applicazione della Parte Generale del Modello e della presente Sezione, rilevando eventuali violazioni e proponendo, se del caso, l'irrogazione di sanzioni disciplinari;
- valutare le eventuali segnalazioni provenienti dalle funzioni aziendali o da qualsiasi altro soggetto ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- comunicare le eventuali violazioni del Modello al Consiglio di Amministrazione;
- curare il costante aggiornamento della presente Sezione e del Modello in generale, proponendo agli organi sociali competenti l'adozione di misure ritenute opportune

o necessarie per mantenere l'effettività ed adeguatezza della Parte Speciale e del Modello in generale.

L'Organismo di Vigilanza comunica quindi i risultati della propria attività di vigilanza e controllo al Consiglio di Amministrazione e al Collegio Sindacale, secondo i termini indicati nel regolamento dell'OdV e nella Parte Generale del Modello.