



## **PARTE SPECIALE**

Versione approvata dal Consiglio di Amministrazione del 11 luglio 2023

## 1. PREMESSE METODOLOGICHE

In conformità con quanto previsto dal Decreto, nel presente documento vengono individuate le Attività a Rischio di Reato di Generalfinance ovvero quei processi aziendali nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di Reato richiamate dal Decreto.

Al fine di individuare le aree sensibili nell'ambito delle attività aziendali di Generalfinance è stata effettuata un'analisi del contesto aziendale finalizzata a mappare tutte le aree di attività svolte dalla Società e, tra queste, individuare i processi e le attività in cui possano essere, in astratto, realizzati i Reati previsti dal Decreto.

Tra le Attività Sensibili sono state considerate anche quelle che, oltre ad avere un rilievo diretto come attività che potrebbero integrare condotte di Reato, possono anche avere un rilievo indiretto per la commissione di altri Reati, risultando strumentali alla commissione degli stessi. In particolare, si intendono strumentali quelle attività nelle quali possono realizzarsi le condizioni di fatto che rendono possibile l'eventuale commissione di reati nell'ambito delle aree direttamente preposte al compimento delle attività specificamente richiamate dalla fattispecie di Reato (ad esempio: selezione e assunzione di personale, sistema di incentivazione, consulenze e prestazioni professionali, acquisizione di beni e servizi per i reati di corruzione).

Ciascuna Parte Speciale del Modello di Generalfinance si compone di due sezioni:

- Prima Sezione: Analisi dei rischi di reato (mappa delle aree a rischio)
- Seconda Sezione: Piano di gestione del rischio

### 1.1. PRIMA SEZIONE: ANALI DEI RISCHI DI REATO

L'analisi del rischio di Reato effettuata da Generalfinance è l'attività che ha in primo luogo permesso di individuare e contestualizzare il rischio di Reato in relazione alla *governance* e all'assetto organizzativo della Società.

L'analisi del rischio è stata condotta su base documentale e completata attraverso indagini di *self assessment* che hanno permesso di evidenziare la sussistenza di un rischio di Reato.

L'indagine è stata condotta con l'ausilio del *management* a cui sono state sottoposte una serie di domande volte a rilevare le minacce di Reato attraverso la formulazione di specifici quesiti cui rispondere con "SI/NO".

Attraverso tale attività si è potuto ottenere informazioni utili a supportare le scelte del vertice esecutivo aziendale in merito alle azioni di adeguamento e miglioramento del Modello della Società rispetto alle finalità preventive indicate dal Decreto (quali i livelli di esposizione ai singoli rischi di Reato).

L'analisi del rischio di Reato è consistita, più nello specifico, nella valutazione sistematica dei seguenti fenomeni<sup>1</sup>:

---

<sup>1</sup> Deve essere sottolineato che un'indagine completa circa le componenti del rischio di reato dovrebbe considerare, altresì, gli aspetti strettamente psicologici e personali degli apicali e dei sottoposti preposti alle attività individuate quali processi a rischio (avidità, problemi finanziari personali, scarsa lealtà verso l'organizzazione, vendetta, ecc.). Indagini di tale natura, oltre a rappresentare gravi minacce ai diritti dei lavoratori, indurrebbero l'utilizzo di informazioni aleatorie e altamente variabili (in quanto soggettive e non oggettive), nonché non permetterebbero l'assunzione di decisioni in termini di politiche correttive, in quanto facilmente sconfinanti in illeciti (con riferimento al diritto del lavoro, alla privacy, ecc.). L'analisi pertanto non ha preso in considerazione tali fattori di indagine.



- l'importanza di un reato (**importanza**);
- la frequenza con cui accade un Reato (**frequenza**);
- l'accadimento di un reato (**precedenti**).

La valutazione del rischio, infatti, può essere espressa nella seguente formula:

$$\text{Rischio di Reato} = F (\text{Probabilità della Minaccia} * \text{Vulnerabilità} * \text{Impatto})$$

In tale ottica, si riporta qui di seguito la definizione di alcuni termini fondamentali utili per comprendere la metodologia utilizzata da Generalfinance:

- Probabilità della Minaccia:** è la frequenza di accadimento di una Minaccia, ovvero di un'azione, un'attività, un processo o un potenziale evento che, in funzione della fattispecie di Reato, rappresenta una possibile modalità attuativa del Reato stesso.
- Livello di Vulnerabilità:** il livello di debolezza aziendale di natura etica od organizzativa; le vulnerabilità possono essere sfruttate per commettere Reati e consistono nella mancanza di misure preventive o in un clima etico aziendale negativo, che rendono possibile l'accadimento di una minaccia e la conseguente realizzazione del Reato;
- Impatto:** è il danno conseguente alla realizzazione di un reato in termini di sanzioni, conseguenze economiche, danni di immagine, così come determinati dal legislatore o raffigurabili;
- Rischio di Reato:** è la probabilità che l'ente subisca un danno determinato dalla commissione di un Reato attraverso le modalità attuative che sfruttano le vulnerabilità rappresentate dalla mancanza delle misure preventive o dal clima etico e organizzativo negativo.

Per analizzare il rischio di Reato si è proceduto in base alle seguenti fasi operative:

- identificazione della fattispecie di Reato e conseguente individuazione delle Minacce che permettono la realizzazione dei fatti di Reato (in termini di condotte o attività operative)<sup>2</sup>;
- contestualizzazione delle Minacce che permettono la realizzazione dei fatti di Reato rispetto alla Società tramite tecniche di *self assessment*;
- assegnazione a ciascuna Minaccia di un valore probabilistico circa il verificarsi, in base ai seguenti parametri:
  - storia o statistica aziendale o di contesto;
  - contesto economico e/o geografico;
  - valutazione del livello di vulnerabilità rispetto a ciascuna Minaccia, tramite l'identificazione delle misure preventive attuate;
  - valutazione dell'impatto in caso di realizzazione del rischio di Reato in termini di sanzioni pecuniarie e/o interdittive.

Per l'aggiornamento del Modello (resasi necessari a seguito delle recenti modifiche al D.Lgs. n. 231/2001, della revisione dell'organigramma e dell'ordinamento organizzativo di Generalfinance nonché della

---

<sup>2</sup> Tale fase ha avuto l'obiettivo di predefinire le cosiddette "componenti strutturali" del rischio di reato. L'individuazione delle componenti strutturali si è basata su una preliminare attività di interpretazione del dettato normativo (ovvero del testo della norma che prevede la sanzione penale e dei precedenti giurisprudenziali utili e necessari per una corretta interpretazione). L'attività interpretativa è stata condotta con la consulenza di primari studi legali che hanno fornito gli elementi chiave della cosiddetta fattispecie oggettiva del reato (ovvero della condotta, sia essa azione od omissione, o dell'evento previsti come punibili). Tali elementi chiave sono stati utilizzati per definire un set di domande finalizzate ad individuare le aree e le attività a rischio di reato dell'azienda costituente l'ente (tramite tecniche di *self assessment*). L'individuazione è resa possibile attraverso la correlazione degli elementi chiave con i dati attinenti alla realtà aziendale (organizzazione, processi, sistemi e poteri).



quotazione delle azioni della Società sul mercato Euronext Milan, segmento STAR) Generalfinance ha attuato la medesima metodologia di *risk assessment* utilizzata in occasione delle ultime revisioni del Modello. Da un punto di vista operativo, sono stati intervistati taluni referenti aziendali interessati (*process owner*) per comprendere gli attuali mutati assetti societari connessi con l'operatività aziendale e con l'implementazione del sistema dei controlli interni al fine di: (i) identificare i processi e le aree esposti al rischio di compimento di uno dei nuovi reati-presupposto, (ii) valutare l'impatto delle novelle legislative sui reati-presupposto già contemplati dal Modello, (iii) valutarne il livello di rischio residuo e (iv) individuare le azioni di prevenzione e mitigazione dei profili di rischio identificati, anche in un'ottica di *gap analysis*.

### **1.2. SECONDA SEZIONE: PIANO DI GESTIONE DEL RISCHIO**

Rispetto alle aree individuate come a rischio di Reato, ed in particolare rispetto ai gruppi di Reato a rischio medio e alto, Generalfinance ha definito una serie di Protocolli preventivi. In questa sezione si definiscono per ciascuna Attività sensibile:

- ✓ i singoli reati a rischio;
- ✓ le specifiche attività di Generalfinance a Rischio di commissione di Reato e le relative modalità attuative;
- ✓ i Protocolli per mitigare il Rischio di Reato suddivisi in:
  - Protocolli Generici, ovvero i protocolli previsti dal Modello per governare genericamente i profili di rischio di realizzazione di tutti i Reati di cui al Decreto (a titolo esemplificativo, il Codice Etico, le attività di *risk assessment*, le attività della società di revisione, ecc.);
  - Protocolli Specifici, ovvero le misure organizzative, fisiche e/o logiche previste dal Modello per governare uno specifico profilo di rischio di realizzazione di un Reato o di una classe specifica di Reati di cui al Decreto (a titolo esemplificativo, le procedure operative, le policy specifiche, ecc.)
- ✓ i controlli effettuati da Generalfinance ed i flussi informativi che ciascuna delle funzioni coinvolte nell'applicazione dei Protocolli Generici/Specifici è chiamata ad inviare periodicamente all'Organismo di Vigilanza.

### **1.3. ANALISI DEI RISCHI DI REATO: ESCLUSIONE DI REATI**

Generalfinance ha implementato i Protocolli specifici per i Reati a cui è esposta tenendo conto degli esiti del *risk assessment*.

Precisiamo che la Società ha ritenuto di non implementare Protocolli Specifici per le seguenti classi di reato, sul presupposto che, per i reati sottoelencati:

- 1) l'interesse o vantaggio per la Società è di difficile configurazione o non sussiste ovvero,
- 2) la probabilità di accadimento del rischio in questione è bassa in considerazione della tipologia di *business*;
- 3) il livello di vulnerabilità del sistema organizzativo e gestionale della Società rispetto al rischio in oggetto è basso.

**Art. 24-ter del D.lgs. 231/2001 – Delitti di criminalità organizzata (Reati associativi, mafiosi e in materia di armi).** La Società, vista la tipologia di attività e di business, non è attiva in settori a rischio di commissione di

tali reati, pertanto, la probabilità di accadimento del rischio in questione è nulla. Inoltre, il livello di vulnerabilità del sistema organizzativo e gestionale della Società rispetto al rischio in oggetto è basso avendo la stessa implementato i Protocolli Generici.

**Art. 25-bis1 del D.lgs. 231/01 – Delitti contro l'industria e il commercio.** La Società non è attiva in settori a rischio di commissione di tali reati poiché non commercializza beni o prodotti alimentari. La probabilità di accadimento del rischio in questione è pertanto nulla in considerazione della tipologia di business di Generalfinance. Inoltre, il livello di vulnerabilità del sistema organizzativo e gestionale della Società rispetto al rischio in oggetto è basso avendo la stessa implementato i Protocolli Generici.

**Art. 25 quater del D.lgs. 231/01 - Reati in materia di terrorismo ed eversione dell'ordine democratico.** La Società non è attiva in settori a rischio di commissione di tali reati, pertanto, la probabilità di accadimento del rischio in questione è nulla, in considerazione della tipologia di business di Generalfinance. Inoltre, il livello di vulnerabilità del sistema organizzativo e gestionale della Società rispetto al rischio in oggetto è basso avendo la stessa implementato i Protocolli Generici.

**Art. 25-quater1 del D.Lgs. 231/01 - Pratiche di mutilazione degli organi genitali femminili.** La Società non è attiva in settori a rischio di commissione di tali reati, pertanto, la probabilità di accadimento del rischio in questione è nulla, in considerazione della tipologia di business di Generalfinance. Inoltre, il livello di vulnerabilità del sistema organizzativo e gestionale della Società rispetto al rischio in oggetto è basso avendo la stessa implementato i Protocolli Generici.

**Art. 25-novies del D.Lgs. 231/01 – Delitti in materia di violazione del diritto d'autore.** La Società non è attiva in settori a rischio di commissione di tali reati (non produce né commercializza opere protette dal diritto d'autore) pertanto la probabilità di accadimento del rischio in questione è molto bassa, in considerazione della tipologia di business di Generalfinance. Inoltre, il livello di vulnerabilità del sistema organizzativo e gestionale della Società rispetto al rischio in oggetto è basso avendo la stessa implementato i Protocolli Generici.

**Art. 25-undecies del D.Lgs. 231/2001 – Reati ambientali.** La Società, vista la tipologia di attività e di business, non è attiva in settori a rischio di commissione di tali reati, pertanto, la probabilità di accadimento del rischio in questione è nulla. Inoltre, il livello di vulnerabilità del sistema organizzativo e gestionale della Società rispetto al rischio in oggetto è basso.

**Art. 25 -quaterdecies del D.Lgs. 231/2001 - Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati.** La probabilità di accadimento delle fattispecie ivi descritte è bassa in considerazione della tipologia di attività in concreto svolta dalla Società. Il livello di vulnerabilità del sistema organizzativo e gestionale della Società rispetto al rischio di reato in oggetto è stato, inoltre, ritenuto basso avendo la stessa implementato idonei Protocolli generici.

**Art. 25-sexiesdecies del D.Lgs. 231/2001 – Contrabbando.** La Società, vista la tipologia di attività e di business, non è attiva in settori a rischio di commissione di tali reati, pertanto la probabilità di accadimento del rischio in questione è nulla.

**Artt. 25-septiesdecies e 25-duodevicies del D.Lgs. 231/2001 – Delitti contro il patrimonio culturale e Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici.** La probabilità di accadimento di tali reati-presupposto si rivela remota e inconfidente rispetto alle peculiarità statutarie, alla tipologia di *business* della Società e ai suoi *asset* patrimoniali, dal momento che essa non intermedia,



acquista, vende o espone beni culturali e non si occupa della gestione, in conto proprio o terzi, di immobili di pregio culturale o paesaggistico sottoposti a vincolo (diretto o indiretto) ai sensi e per gli effetti del Codice dei beni culturali e del passaggio (D.Lgs. 22 gennaio 2004, n. 42).



## **PARTE SPECIALE I**

*Indebita percezione di erogazioni, truffa in danno dello stato, di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24)*

*Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione, abuso d'ufficio e traffico di influenze illecite (art. 25)*

*Corruzione privata e istigazione alla corruzione tra privati (art. 25-ter)*

*Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies)*

## 1.1 I REATI RICHIAMATI DEL DECRETO E LA RELATIVA MODALITÀ DI COMMISSIONE

### A) I reati inerenti finanziamenti pubblici (art. 24 del D.Lgs. 231/01)<sup>1</sup>

- **Malversazione di erogazioni pubbliche (Art. 316-bis codice penale)**

Tale fattispecie di reato si realizza quando, dopo avere ricevuto contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate dallo Stato (da qualsiasi ente dello Stato, anche territoriale, quale la Regione o il Comune) o dall'Unione Europea, destinati a favorire la realizzazione di una o più finalità, non si proceda all'utilizzo (anche solo parzialmente) delle somme ricevute per gli scopi per i quali sono state erogate, e ciò anche nell'ipotesi in cui l'attività programmata si sia comunque svolta.

Si pensi alla richiesta e ottenimento di un finanziamento pubblico erogato in vista dell'assunzione, presso la Società, di personale appartenente a categorie protette, ovvero alla ristrutturazione di immobili danneggiati in occasione di calamità naturali che, una volta conseguito, non venga destinato a dette finalità.

- **Indebita percezione di erogazioni pubbliche (Art. 316-ter codice penale)**

Tale fattispecie di reato si realizza quando si ottengono, senza averne diritto, contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni di questo tipo dallo Stato, altri enti pubblici, o dall'Unione Europea, attraverso l'utilizzo o la presentazione di dichiarazioni o documenti falsi ovvero attraverso l'omissione delle informazioni dovute. A differenza dell'ipotesi delittuosa di cui al punto precedente (art. 316 bis c.p.) in questo caso non assume alcun rilievo la destinazione dei finanziamenti pubblici erogati, poiché il reato si consuma al momento del loro indebito ottenimento.

Va evidenziato, altresì, che tale reato ha natura residuale o sussidiaria rispetto alla più grave fattispecie della truffa aggravata ai danni dello Stato (art. 640, comma 2, n. 1 c.p.) per la cui sussistenza è necessaria l'induzione in errore mediante artifici o raggiri, per cui si configura solo qualora la condotta non integri gli estremi richiamati del più grave reato di truffa aggravata.

A titolo esemplificativo si citano, in particolare, le ipotesi di indebito ottenimento di un finanziamento pubblico finalizzato al sostegno delle attività imprenditoriali in determinati settori, mediante la presentazione di false fatture attestanti prestazioni inesistenti; ovvero mediante la produzione di documentazione attestante falsamente la sussistenza dei requisiti necessari per l'ottenimento del finanziamento.

- **Frode nelle pubbliche forniture (Art. 356 codice penale)**

Tale fattispecie di reato si configura nelle ipotesi di fraudolento inadempimento dei contratti di fornitura, ovvero sia ogniqualvolta si rinvenivano casi di "*malafede contrattuale*" da intendersi quali espedienti maliziosi o ingannevoli tali da far apparire l'esecuzione del contratto come conforme agli obblighi assunti.

---

<sup>1</sup> Articolo novellato dall'art. 5, comma 1, lett. a) del D.lgs. n. 75/2020 che ha introdotto nel catalogo dei reati-presupposto anche il delitto di frode nelle pubbliche forniture di cui all'art. 356 c.p. Più nel dettaglio, il Decreto citato (avente ad oggetto l'attuazione della direttiva (UE) 2017/1371, relativa "*alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale*" – cd. Direttiva PIF), all'art. 5, comma 1, lett. a), ha (i) esteso il catalogo dei reati presupposto includendovi i delitti di frode nelle pubbliche forniture (art. 356 c.p.) e di appropriazione indebita o distrazione di fondi comunitari, commesso da chi "*mediante l'esposizione di dati o notizie false, consegue indebitamente per sé o altri, aiuti, premi, indennità, restituzioni, contributi o altre erogazioni a carico totale o parziale del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale*" (cd.. frode in agricoltura, art. 2 L. 898/1986); (ii) ed ha previsto la configurabilità della responsabilità amministrativa dell'ente anche laddove dalla commissione delle fattispecie di reato già previste al comma 1 dell'art. 24 consegua una lesione agli interessi finanziari dell'Unione europea.

A titolo esemplificativo, si pensi alle ipotesi in cui vengano consapevolmente consegnate cose, in tutto o in parte, difformi (per origine, provenienza, qualità o quantità) dalle caratteristiche disposte (per legge o atto amministrativo), ovvero ancora alle ipotesi di ritardata consegna.

- **Truffa ai danni dello Stato, di altro ente pubblico o dell'Unione Europea (Art. 640, comma 2, n. 1, codice penale)**

Tale fattispecie di reato si realizza quando, per procurare un ingiusto profitto, sono posti in essere artifici o raggiri tali da indurre in errore l'ente pubblico o l'Unione Europea e tali da arrecare un danno ai medesimi.

E' questa l'ipotesi, ad esempio, della presentazione di documenti, dati o dichiarazioni false nella partecipazione ad una gara di appalto, al fine di ottenere l'aggiudicazione dell'appalto medesimo, o, ancora, della trasmissione all'amministrazione finanziaria di documentazione contenente false informazioni al fine di ottenere un rimborso fiscale non dovuto; ovvero, più in generale, dell'invio ad enti previdenziali, amministrazioni locali o ripartizioni di queste, di comunicazioni contenenti dati falsi in vista dell'ottenimento di un qualsiasi vantaggio o agevolazione per la Società.

- **Truffa aggravata per il conseguimento di erogazioni pubbliche (Art. 640-bis codice penale)**

La struttura del delitto è del tutto analoga a quella segnalata per l'ipotesi precedente, ma qualificata ed aggravata dall'oggetto materiale della frode ovvero sia l'indebita percezione di erogazioni pubbliche o provenienti dall'Unione Europea, quali sovvenzioni, finanziamenti, contributi o agevolazioni finanziarie.

Si precisa che: i contributi e le sovvenzioni sono attribuzioni pecuniarie a fondo perduto che possono avere carattere periodico o una *tantum*, una misura fissa o determinata in base a parametri variabili, natura vincolata relativamente all'*an* o al *quantum* o di pura discrezionalità; i finanziamenti sono atti negoziali caratterizzati dall'obbligo di destinazione delle somme o di restituzione o da ulteriori e diversi oneri; i mutui agevolati sono erogazioni di somme di denaro con obbligo di restituzione per il medesimo importo, ma con interessi in misura minore a quelli praticati sul mercato.

Tale fattispecie, a titolo esemplificativo, può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, attraverso la comunicazione di dati non veri o attraverso la predisposizione di documentazione falsa, per ottenere finanziamenti pubblici finalizzati, ad esempio, al finanziamento di corsi di formazione del personale o all'ottenimento di licenze, autorizzazioni, concessioni essenziali per accedere ad una gara pubblica.

- **Frode informatica (Art. 640-ter codice penale)**

Tale fattispecie di reato si realizza nell'ipotesi in cui, alterando il funzionamento di un sistema informatico o telematico, o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando un danno.

L'interferenza può realizzarsi in varie forme: in fase di raccolta ed inserimento dei dati, in fase di elaborazione, in fase di emissione. In tutti questi casi l'intervento avviene sulla memoria di un elaboratore sul cui corretto funzionamento l'autore materiale del reato interferisce in modo da ricavarne un indebito arricchimento in danno dello Stato o di altro ente pubblico.

Ad esempio, integra il reato, la modificazione delle informazioni relative alla situazione contabile di un rapporto contrattuale in essere con un ente pubblico, ovvero l'alterazione dei dati fiscali e/o previdenziali contenuti in una banca dati facente capo alla pubblica amministrazione.

## **B) I reati corruttivi (Art. 25, 25-ter, lett. s-bis e 25-decies del D. Lgs. 231/01)**

## Premessa

Negli ultimi anni il Legislatore al fine di dare compiuta attuazione agli obblighi internazionali derivanti dalla ratifica della Convenzione penale sulla corruzione del Consiglio d'Europa del 1999 e così adeguarsi alle indicazioni del *Group d'Etats contre la corruption* ("GRECO")<sup>2</sup>, è più volte intervenuto sul microsystema dei reati corruttivi previsti dal codice penale con conseguenti importanti ricadute sulla materia della responsabilità amministrativa degli enti ex D.Lgs. 231/2001 essendo tali fattispecie incluse nel novero dei reati presupposto di cui al citato Decreto.

Dapprima, la Legge n. 190 del 6 novembre del 2012 ("Legge Severino"), ritenuta tra le più importanti riforme in materia di contrasto alla corruzione, ha novellato (cambiandone la struttura) i reati di cui agli artt. 317 e ss. c.p. e ha introdotto per la prima volta nel sistema penale innovative fattispecie delittuose come il traffico di influenze illecite di cui all'art. 346 *bis* c.p.

Successivamente, il Legislatore con il D.Lgs. n. 38 del 15 Marzo 2017, al fine di rendere la normativa interna pienamente conforme alle previsioni della decisione quadro 2003/568/GAI relativa alla lotta contro la corruzione nel settore privato, ha riformulato il testo dell'art. 2635 c.c. in materia di corruzione tra privati; ha introdotto la nuova fattispecie di istigazione alla corruzione tra privati (art. 2635-bis c.c.) contestualmente inserendola nel catalogo dei reati presupposto di cui al D.Lgs. 231/2001; ed ha inasprito le sanzioni ivi previste per ambedue le fattispecie modificando la lettera s-bis dell'art. 25-ter, comma 1.<sup>3</sup>

Recentemente, poi, il Legislatore è nuovamente intervenuto sulla materia con la Legge n. 3 del 9 gennaio 2019 (meglio nota come Legge "Spazzacorrotti"). Tale Legge ha inciso sia sul codice penale (abrogando la fattispecie del millantato credito di cui all'art. 346 c.p., assorbita oggi nel vigente traffico di influenze illecite di cui all'art. 346 *bis* c.p.), sia sulla disciplina della responsabilità amministrativa degli enti dove ha apportato alcune significative modifiche. Tra le modifiche di maggior rilievo si segnalano in particolare:

- 1) l'estensione del catalogo dei reati presupposto che possono dar luogo alla responsabilità dell'ente attraverso l'introduzione del delitto di traffico di influenze illecite (si veda dopo *sub* art. 346-*bis* c.p.);
- 2) l'inasprimento delle sanzioni interdittive previste dall'articolo 9, comma 2 del Decreto per alcuni dei reati contro la PA (concussione; induzione indebita a dare o promettere utilità; corruzione; istigazione alla corruzione) con l'applicazione di una differente forbice edittale a seconda della qualifica del soggetto colpevole. In particolare, è prevista l'applicazione di sanzioni interdittive da quattro a sette anni quando il reato è commesso da un soggetto apicale e da due a quattro anni se il reato è commesso da un sottoposto;
- 3) l'introduzione del beneficio della riduzione delle sanzioni interdittive per i reati di cui sopra (per un termine compreso tra 3 mesi e 2 anni) nel caso in cui l'ente, prima della sentenza di primo grado, si sia efficacemente adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per individuarne i responsabili ovvero per il sequestro delle somme o altre utilità trasferite, e abbia eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della

<sup>2</sup> Organo di monitoraggio previsto dalla Convenzione penale sulla corruzione del Consiglio d'Europa del 1999.

<sup>3</sup> L'art. 25-ter, lett. s-bis così dispone "per il delitto di corruzione tra privati, nei casi previsti dal terzo comma dell'art. 2635 del codice civile, la sanzione pecuniaria da quattrocento a seicento quote e, nei casi di istigazione di cui al primo comma dell'art. 2635 bis del codice civile, la sanzione pecuniaria da duecento a quattrocento quote. Si applicano altresì le sanzioni interdittive previste dall'art. 9, comma 2."

specie di quello verificatosi;

- 4) la previsione della procedibilità d'ufficio per i reati di corruzione tra privati e di istigazione alla corruzione tra privati.

Infine, merita di segnalarsi come il Legislatore sia nuovamente intervenuto sulla materia con il D.lgs. n. 75/2020 (avente ad oggetto l'attuazione della direttiva (UE) 2017/1371 relativa "alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale" – cd. direttiva PIF) annoverando, nell'ambito dei reati presupposto di cui all'art. 25 del D.lgs. 231/2001, anche i delitti di peculato (artt. 314, comma 1, e 316 c.p.) e di abuso d'ufficio (art. 323 c.p.) laddove dalla relativa commissione consegue una lesione agli interessi finanziari dell'Unione Europea.

- **Concussione (Art. 317 codice penale)**

Tale ipotesi di reato si configura nel caso in cui un Pubblico Ufficiale o un Incaricato di Pubblico Servizio, abusando della sua qualità o dei suoi poteri, costringa taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro o altra utilità.

A titolo meramente esemplificativo, il reato di concussione potrebbe rilevare nell'ambito di applicazione del Decreto nell'ipotesi in cui un esponente, un dipendente aziendale o un collaboratore esterno della Società concorra nel reato del Pubblico Ufficiale, il quale, approfittando della propria qualità, richieda a terzi prestazioni non dovute; ovvero nell'ipotesi in cui l'esponente aziendale svolga concretamente pubblici uffici e, in tale veste, favorisca la Società abusando del suo ufficio (sempre che, da tale comportamento, derivi in qualche modo un vantaggio per la Società).

- **Corruzione per l'esercizio della funzione (Art. 318 codice penale)**

Commette il reato di cui alla fattispecie in esame, il Pubblico Ufficiale che, in relazione all'esercizio delle sue funzioni o dei suoi poteri, riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa.

L'attività delittuosa del Pubblico Ufficiale potrà venire in essere sia nel compimento di un atto dovuto (i.e. velocizzare una pratica la cui evasione è di propria competenza), sia nel compimento di un atto contrario ai suoi doveri (i.e. il Pubblico Ufficiale che accetta denaro per garantire l'aggiudicazione di una gara).

Le ipotesi di corruzione potrebbero rilevare ai sensi del Decreto sotto un duplice profilo:

- 1) nel caso della corruzione attiva, allorché un dipendente della Società corrompa un Pubblico Ufficiale o Incaricato di Pubblico Servizio per l'ottenimento di qualche vantaggio a favore della Società medesima (affinché, ad esempio, nel corso di una ispezione da parte di Banca di Italia o di Consob non siano rilevate eventuali irregolarità emerse );
- 2) nel caso della corruzione passiva, allorché un dipendente della Società che rivesta, a titolo esemplificativo, la qualità di Pubblico Ufficiale o Incaricato di Pubblico Servizio, riceva denaro o la promessa di denaro o altra utilità quale controprestazione per il compimento di atti contrari ai doveri del proprio ufficio. In quest'ultima ipotesi, è però nel concreto difficilmente individuabile l'interesse o il vantaggio tratto dalla Società in ragione del fatto che è più probabile che il dipendente si faccia corrompere non tanto nell'interesse della Società ma, quanto nel proprio. In ogni caso, in considerazione delle peculiarità giuridico-soggettive, statutarie, operative e di linea di *business* di Generalfinance, tale fattispecie risulta di remota applicabilità.

La corruzione si distingue dalla concussione in quanto presuppone, quali elementi di tipicità, la posizione paritetica del corrotto e del corruttore e la presenza tra i medesimi di un vero e proprio accordo corruttivo

finalizzato al raggiungimento di un reciproco vantaggio. Diversamente la concussione presuppone lo sfruttamento da parte del Pubblico Ufficiale o dell'Incaricato di Pubblico Servizio della propria posizione di superiorità che si contrappone a quella di soggezione del privato.

Tale fattispecie delittuosa, ad esempio, potrebbe realizzarsi mediante l'assunzione di personale segnalato dal Pubblico Ufficiale o dall'Incaricato di Pubblico Servizio, mediante il riconoscimento al Pubblico Ufficiale o all'Incaricato di Pubblico Servizio o a terzi a questi ricollegabili di compensi non in linea con la prestazione/fornitura erogata, mediante l'emissione di fatture a fronte di prestazioni/operazioni inesistenti, mediante la corresponsione di rimborsi spese fittizi presentati anche attraverso consulenti oppure attraverso l'assegnazione di beni fittiziamente a titolo di omaggio o liberalità.

- **Corruzione per un atto contrario ai doveri d'ufficio e circostanze aggravanti (Artt. 319 e 319 bis codice penale)**

Commette il reato di cui alla fattispecie in esame, il Pubblico Ufficiale che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa.

Il Decreto contempla tra i reati presupposto anche l'ipotesi aggravata, ovverossia l'ipotesi in cui il fatto corruttivo di cui all'art. 319 c.p. abbia ad oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene nonché il pagamento o il rimborso di tributi.

A titolo esemplificativo, è il caso del funzionario pubblico che, a fronte della corresponsione di una somma di denaro da parte di consulenti della Società interessata, si renda disponibile a rilasciare un proprio parere favorevole rispetto ad una proposta transattiva in realtà lesiva degli interessi dell'Erario.

- **Corruzione in atti giudiziari (Art. 319-ter codice penale)**

Il reato si configura allorché i fatti di corruzione, indicati negli artt. 318 e 319 c.p., siano commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo. La pena è aumentata se dal fatto deriva l'ingiusta condanna di taluno.

- **Induzione indebita a dare o promettere utilità (Art. 319-quater codice penale)**

Con tale fattispecie è punito il Pubblico Ufficiale o l'Incaricato di Pubblico Servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere indebitamente, a lui o a un terzo, denaro od altra utilità. E' altresì punito chi dà o promette denaro o altra utilità (comma 2). Nell'ipotesi in cui il fatto offenda gli interessi finanziari dell'Unione europea e il danno o il profitto siano superiori a Euro 100.000 l'art. 1, comma 1, lett. c), D.lgs. n. 75/2000, ha previsto un inasprimento sanzionatorio.

Il reato rappresenta una novità tanto nel sistema della responsabilità penale delle persone fisiche, quanto in quello della responsabilità da reato degli enti e, per vero, le due innovazioni risultano tra loro strettamente correlate. Di fatti, l'introduzione dell'art. 319 quater c.p. da parte della Legge Severino consegue alla scomposizione dell'originaria ed unitaria condotta di concussione in due fattispecie distinte sul piano della condotta, dei soggetti attivi e della risposta sanzionatoria.

Da un lato, con riferimento al soggetto attivo, si differenzia dalla concussione, ricomprendendo sia il Pubblico Ufficiale che l'Incaricato di Pubblico Servizio; dall'altro, se ne differenzia con riferimento alla modalità di perseguimento del risultato, postulando la sola induzione e non anche la condotta costringitiva.

- **Corruzione di persona incaricata di un pubblico servizio (Art. 320 codice penale)**

Le disposizioni di cui agli artt. 318 e 319 c.p. si applicano anche all'Incaricato di Pubblico Servizio.

- **Pene per il corruttore (Art. 321 codice penale)**

La disposizione prevede che le pene stabilite nel primo comma dell'art. 318 c.p., nell'art. 319 c.p., nell'art. 319-*bis* c.p., nell'art. 319-*ter* c.p., e nell'art. 320 c.p. in relazione alle ipotesi di reato di cui agli artt. 318 e 319 c.p., si applicano anche a chi dà o promette al Pubblico Ufficiale o all'Incaricato di Pubblico Servizio il danaro o altra pubblica utilità.

- **Istigazione alla corruzione (Art. 322 codice penale)**

Tale ipotesi di reato si configura nel caso in cui venga offerto o promesso denaro o altra utilità ad un Pubblico Ufficiale o Incaricato di Pubblico Servizio per indurlo a compiere, omettere, ritardare ovvero a fare un atto contrario ai doveri del suo ufficio e tale offerta o promessa non venga accettata.

- **Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione, abuso d'ufficio di membri delle Corti Internazionali o degli Organi delle Comunità Europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità Europee e di Stati Esteri (Art. 322 *bis* codice penale)<sup>4</sup>**

La famiglia dei reati corruttivi in esame assume rilevanza anche quando i medesimi fatti di reato siano compiuti nei confronti dei Pubblici Ufficiali o degli Incaricati di Pubblico Servizio dell'Unione Europea o di singoli Stati membri o di organizzazioni internazionali al fine di procurare a sé o altri un indebito vantaggio nell'ambito di operazioni economiche internazionali. Altresì, le medesime previsioni si applicano a quanti nell'ambito di Stati non appartenenti all'Unione esercitano funzioni o attività corrispondenti a quelle dei Pubblici Ufficiali e degli Incaricati di Pubblico Servizio qualora però il fatto risulti offensivo degli interessi finanziari dell'Unione.

Più nel dettaglio, le disposizioni di cui agli articoli 321 (i.e. pene per il corruttore) e 322 (i.e. istigazione alla corruzione), primo e secondo comma del codice penale, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:

- ai membri della Commissione delle Comunità europee, del Parlamento Europeo, della Corte di Giustizia e della Corte dei Conti delle Comunità Europee;
- ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità Europee o del regime applicabile agli agenti delle Comunità Europee;
- alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità Europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità Europee;
- alle persone che esercitano funzioni o attività corrispondenti a quelle dei Pubblici Ufficiali e degli Incaricati di un Pubblico Servizio nell'ambito di altri Stati membri o delle organizzazioni pubbliche internazionali;
- ai membri delle assemblee parlamentari internazionali o di un'organizzazione internazionale o sovranazionale e ai giudici e funzionari delle corti internazionali;

---

<sup>4</sup> Si segnala che l'art. 322 *bis* c.p. ha di recente subito interventi riformatori. In primo luogo, con la Legge n. 3/2019 ("Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici") che ne ha modificato la rubrica e aggiunto i numeri 5-*ter* e 5-*quater* al primo comma e novellato il comma 2. Da ultimo, con il D.lgs. n. 75/2020 (avente ad oggetto l'attuazione della direttiva (UE) 2017/1371, relativa alla "lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale – c.d. direttiva PIF) che ha aggiunto il numero 5-*quinqüies* al primo comma, prevedendo l'estensione della punibilità a titolo di corruzione dei Pubblici Ufficiali e degli Incaricati di Pubblico Servizio di Stati non appartenenti all'Unione Europea, ove tali fatti siano tali da ledere gli interessi finanziari dell'Unione stessa.

- alle persone che esercitano funzioni o attività corrispondenti a quelle dei Pubblici Ufficiali o Incaricati di Pubblico Servizio nell'ambito di Stati non appartenenti all'Unione, quando il fatto offende gli interessi finanziari dell'Unione europea.

Inoltre, la norma statuisce che le disposizioni degli artt. 319-*quater*, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:

- alle persone indicate nel primo comma dell'art. 322-*bis*;
- alle persone che esercitano funzioni o attività corrispondenti a quelle dei Pubblici Ufficiali e degli Incaricati di un Pubblico Servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali.

Infine, la norma disciplina i casi di assimilazione ai Pubblici Ufficiali e agli Incaricati di Pubblico Servizio prevedendo che saranno considerati alla stregua dei pubblici ufficiali tutti quei soggetti che esercitano funzioni a questi corrispondenti mentre, in tutti gli altri casi, l'assimilazione avverrà con la figura dell'incaricato di pubblico servizio.

- **Traffico di influenze illecite (Art. 346-bis codice penale)<sup>5</sup>**

La fattispecie delittuosa del traffico di influenze illecite è stata inserita nel codice penale per effetto della Legge n. 190/2012 ("Legge Severino") recante "*disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione*", con la quale il Legislatore nazionale ha dato seguito agli impegni internazionali<sup>6</sup> precedentemente assunti, ed è stata recentemente annoverata tra i reati presupposto della responsabilità dell'ente (art. 25 del Decreto) dalla L. n. 3/2019.

La Legge n. 3/2019 non solo ha introdotto la fattispecie in commento nel catalogo dei reati presupposto, ma ha anche novellato la medesima fattispecie apportandone significative modifiche:

- in primo luogo, attraverso l'abrogazione dell'art. 346 c.p., i fatti qualificati originariamente come "*millantato credito*" vengono ad essere ricompresi sotto il nuovo art. 346 *bis* c.p. La condotta punita non consiste più solo nello sfruttamento di relazioni esistenti, ma anche nella vanteria di asserite relazioni con un Pubblico Ufficiale, con un Incaricato di Pubblico Servizio o, ancora, con uno dei soggetti elencati all'art. 322 *bis* c.p.;
- in secondo luogo, rispetto alla sua originaria formulazione, il momento consumativo del delitto di traffico di influenze illecite si rinviene al momento della dazione o della promessa di denaro o altra utilità laddove il denaro o l'altra utilità rappresentano, nel reato base, il prezzo della mediazione illecita verso il Pubblico Ufficiale, l'Incaricato di Pubblico Servizio o di uno dei soggetti di cui all'art. 322 *bis* c.p., ovvero la remunerazione per l'esercizio, da parte di uno di questi, delle sue funzioni o dei suoi poteri;
- ancora, nella struttura della fattispecie non è più essenziale la finalizzazione dell'accordo, rientrando tale ipotesi nella aggravante di cui al 4 comma dell'art. 346 *bis* c.p.;
- ed infine, al comma 2 dell'art. 346 *bis* c.p., viene prevista un'estensione della punibilità, oltre che al mediatore, anche al soggetto che promette o dà il denaro o altra utilità, che viene ad essere punito indipendentemente dal fatto che la relazione tra il mediatore e il Pubblico Ufficiale esista o meno.

<sup>5</sup> Articolo inserito dalla Legge 3/2019 ("*Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici*").

<sup>6</sup> Ci si riferisce a quelli assunti a seguito della ratifica della "*Convenzione penale sulla corruzione*" (con L. 110/2012) e della "*Convenzione contro la corruzione*", Convenzione di Merida (con L. 116/2009).

Tali condotte potrebbero concretizzarsi, ad esempio, nell'ambito di rapporti intrattenuti da mediatori, agenti, procuratori, consulenti o collaboratori, anche esterni che, a vario titolo, per l'espletamento della propria attività concludono in nome e per conto della società attività finalizzate al rilascio di licenze, autorizzazioni, permessi o finanziamenti da parte di soggetti pubblici.

Si pensi ai casi in cui un soggetto, sfruttando le proprie conoscenze e/o rapporti con funzionari pubblici, riesca illecitamente a intercedere per la società al fine di farle ottenere un vantaggio quale l'aggiudicazione di una gara o l'erogazione di un finanziamento come corrispettivo della propria mediazione (illicita).

- **Corruzione tra privati (Art. 2635 codice civile)<sup>7</sup>**

Il D.Lgs. n. 38 del 15 Marzo 2017 (*"Attuazione della decisione quadro 2003/568/GAI del Consiglio, del 22 luglio 2003 relativa alla lotta contro la corruzione nel settore privato"*) in vigore dal 14 Aprile 2017 ha modificato il testo dell'art. 2635 c.c. in materia di *"corruzione tra privati"*, prevedendo:

- in primo luogo, l'ampliamento dell'ambito di relativa applicazione attraverso l'estensione del novero dei soggetti attivi, includendovi, oltre coloro che effettivamente rivestono posizioni apicali di amministrazione o di controllo, anche coloro che di fatto svolgono l'esercizio di funzioni direttive differenti da quelle contemplate al primo comma;
- in secondo luogo, l'estensione del novero dei soggetti collettivi interessati dalla disposizione, non più limitato alle sole società, ma ampliato a qualsiasi ente privato;
- in terzo luogo, l'ampliamento delle modalità con le quali può essere realizzata la corruzione tra privati, sia attivamente che passivamente, con l'introduzione della possibilità di commettere il reato anche per interposta persona;
- in quarto luogo, è stato disposto l'ampliamento delle condotte punibili attraverso cui può pervenirsi all'accordo corruttivo, includendovi anche la sollecitazione alla dazione di denaro o altre utilità, da parte dell'*intraneus* nei confronti dell'*extraneus*;
- l'eliminazione, dal testo della norma, del riferimento alla necessità che la condotta realizzata dall'*intraneus* cagioni nocumento alla società, con il conseguente mutamento della fattispecie da reato di danno a reato di pericolo e l'ampliamento, quindi, delle ipotesi in cui il del reato *de quo* può essere contestato.

Si badi che il reato-presupposto ai sensi del D.Lgs. 231/01 è la sola fattispecie di cui al comma 3 dell'articolo 2635 del codice civile, ossia il delitto commesso dal soggetto corruttore per avvantaggiare la propria società di appartenenza (corruzione attiva).

- **Istigazione alla corruzione tra privati (Art. 2635 - bis codice civile)**

Il presente articolo è stato introdotto dal D.Lgs. 15.3.2017, n. 38, in vigore il 14.4.2017, con il quale è stata data attuazione alla delega prevista dall'art. 19, L. 12.8.2016, n. 170 (*"Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - legge di delegazione europea 2015"*), così recependo la decisione quadro 2003/568/GAI del Consiglio dell'Unione Europea relativa alla lotta contro la corruzione nel settore privato che danneggia l'economia ed altera la concorrenza.

La norma punisce la condotta di: *"chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia o ometta un atto in violazione degli obblighi inerenti al proprio ufficio"*

---

<sup>7</sup> La legge n.3/2019 ha previsto la procedibilità d'ufficio per la fattispecie in commento.

*o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo (istigazione alla corruzione passiva). La pena di cui al primo comma si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per sé o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata (istigazione alla corruzione attiva)".*

Dal lato attivo, è punito chiunque offra o prometta denaro o altre utilità non dovuti ad un soggetto *intraeus* al fine del compimento od omissione di atti in violazione degli obblighi inerenti il proprio ufficio o degli obblighi di fedeltà, qualora l'offerta o la promessa non sia accettata.

Dal lato passivo, è prevista la punibilità dell'*intraeus* che solleciti una promessa o dazione di denaro o altra utilità, al fine del compimento o dell'omissione di atti in violazione dei medesimi obblighi, qualora tale proposta non sia accettata.

Le pene previste per entrambe le fattispecie (istigazione attiva e passiva) sono quelle contemplate per la corruzione privata, ma ridotte di un terzo<sup>8</sup>.

Quanto alla rilevanza del reato in esame rispetto al Decreto, il D.lgs. n. 38/2017 ha modificato l'art. 25-ter allargando il catalogo dei reati presupposto al delitto di istigazione alla corruzione limitatamente però al solo caso della istigazione alla corruzione passiva di cui al comma 1 dell'art. 2635 bis<sup>9</sup>, per il quale viene comminata la sanzione pecuniaria da duecento a quattrocento quote e l'applicazione di sanzioni interdittive rispetto ai casi di reiterazione del reato.

- **Pene accessorie (Articolo 2635 ter codice civile)<sup>10</sup>**

La condanna per il reato di cui all'articolo 2635, primo comma, importa in ogni caso l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese di cui all'articolo 32-bis del codice penale nei confronti di chi sia già stato condannato per il medesimo reato o per quello di cui all'articolo 2635-bis, secondo comma.

- **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (Art. 377 bis codice penale)**

L'articolo 377 bis c.p. punisce *"chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere"*.

L'ente in relazione alla commissione del reato *de quo* rischia l'irrogazione di una sanzione pecuniaria fino a cinquecento (500) quote.

---

<sup>8</sup> Si ricorda che nel tentativo (art.56 c.p.) si prevede in via generale la diminuzione della pena stabilita per il delitto da un terzo a due terzi se l'azione non si compie o l'evento non si verifica.

<sup>9</sup> Nel comma 2 dell'art. 2635 c.c., l'*intraeus* infedele contravviene, infatti, ai propri obblighi nei confronti dell'ente di appartenenza, sicchè non potrà dirsi che agisce nell'interesse o a vantaggio dell'ente stesso.

Rispetto alla realizzazione della fattispecie in esame, l'art. 25 *decies* del Decreto sancisce la responsabilità dell'ente nel caso in cui dalla relativa commissione sia conseguito un interesse o vantaggio in capo all'ente stesso.

- **Peculato e abuso d'ufficio (Artt. 314, comma 1, 316, 322 codice penale)**

Con il D.lgs. n. 75/2020 (di attuazione della direttiva (UE) n. 2017/1371 relativa "alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale" – direttiva PIF) è stato novellato l'art. 25 del Decreto, prevedendo al comma primo l'estensione del novero dei reati contro la PA che possono determinare la responsabilità amministrativa dell'ente, includendovi i delitti di peculato e quello di abuso d'ufficio esclusivamente nell'ipotesi in cui dalle condotte delittuose derivi un danno agli interessi finanziari dell'Unione.<sup>11</sup>

I delitti di peculato di cui agli artt. 314 e 316 c.p. sono preposti alla tutela del buon andamento ed imparzialità della PA (art. 97 Cost.) ed assicurano che l'azione amministrativa vada scevra da ogni forma di abuso appropriativo da parte del soggetto titolare della qualifica pubblicistica, indipendentemente dalle conseguenze che una simile appropriazione possa avere sull'efficienza amministrativa. La fattispecie delittuosa dell'abuso d'ufficio di cui all'art. 323 c.p. incrimina il duplice comportamento del Pubblico Ufficiale o dell'Incaricato di Pubblico Servizio che, intenzionalmente, procura a sé o ad altri un ingiusto vantaggio patrimoniale oppure procura ad altri un danno ingiusto. Anche in tal caso, perché la condotta possa ritenersi tipizzata, è richiesto che la stessa sia compiuta nello svolgimento delle funzioni o del servizio e che sia posto in essere in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità.

A titolo meramente esemplificativo e non esaustivo, i nuovi delitti potrebbero assumere rilevanza nell'ambito del Decreto rispetto alle ipotesi del concorso nel reato (cd. proprio) del pubblico funzionario, ovvero sia quando l'esponente aziendale (*extraneus*) per favorire la sua azienda istighi o aiuti concretamente il pubblico funzionario ad appropriarsi di utilità che non gli spettino o ad abusare del suo ufficio pur senza alcuna dazione o promessa di utilità (in tal caso, infatti, si rientrerebbe nei fatti corruttivi in precedenza esaminati).

## 1.2 ATTIVITÀ SENSIBILI

L'analisi dei processi aziendali di Generalfinance ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dagli artt. 24, 25, 25-ter e 25-*decies* del Decreto. Qui di seguito sono elencati i processi sensibili:

- 1) richiesta e gestione di contributi e finanziamenti. Le attività a rischio per Generalfinance potrebbero essere identificate:
  - nella richiesta di finanziamenti o contributi pubblici per le attività di formazione;
  - nell'ottenimento e nell'utilizzo del finanziamento o del contributo pubblico ottenuto;
  - nella rendicontazione all'ente erogatore delle attività svolte.
- 2) gestione dei rapporti di "profilo istituzionale" con autorità pubbliche e soggetti appartenenti alla Pubblica Amministrazione (funzionari pubblici nell'ambito delle gare d'appalto) per l'ottenimento di certificazioni, autorizzazioni, licenze, concessioni e altri provvedimenti amministrativi per

---

<sup>11</sup> Art. 25, comma 1 "in relazione alla commissione dei delitti di cui agli artt. 318, 321, 322 commi primo e terzo, e 346 bis del codice penale, si applica la sanzione pecuniaria fino a 200 quote. La medesima sanzione si applica, quando il fatto lede gli interessi finanziari dell'unione europea, in relazione alla commissione dei delitti di cui agli artt. 314, primo comma, 316 e 323 c.p."

- l'esercizio delle attività aziendali;
- 3) gestione dei rapporti con la Pubblica Amministrazione (INAIL, INPS, Ispettorato del Lavoro) per gli adempimenti in materia finanziaria, fiscale, previdenziale, contributiva di dichiarazioni fiscali e previdenziali e pagamento dei relativi oneri;
  - 4) gestione dei rapporti e delle informative dirette alle Autorità di Vigilanza (in particolare, Consob e Banca di Italia) anche in occasione di verifiche, ispezioni ed accertamenti;
  - 5) gestione dei rapporti con i soggetti pubblici per gli aspetti che riguardano la sicurezza e l'igiene sul lavoro (D.Lgs. 81/2008 e successive modifiche/integrazioni);
  - 6) gestione dei rapporti con autorità di Pubblica Sicurezza (Carabinieri, Polizia di Stato, Polizia Municipale, Guardia di Finanza);
  - 7) gestione dei rapporti con l'amministrazione finanziaria;
  - 8) gestione del contenzioso giudiziale e stragiudiziale;
  - 9) gestione dei rapporti commerciali, contrattuali e finanziari con la clientela e soggetti terzi privati;
  - 10) gestione delle liberalità di carattere benefico e culturale nonché delle sponsorizzazioni e degli omaggi.

Sono altresì state individuate altre Attività Sensibili relative ai processi strumentali c.d. "di provvista", ossia quei processi che possono costituire supporto e presupposto (finanziario ed operativo) per la creazione delle utilità di scambio ai fini della commissione del reato corruttivo.

Di seguito sono indicate le fattispecie di attività sensibili relative ai processi di provvista individuate nell'ambito d'attività di Generalfinance:

- 1) gestione del ciclo passivo (selezione e gestione dei fornitori);
- 2) gestione e affidamento di incarichi professionali;
- 3) gestione dei beni mobili aziendali;
- 4) selezione, assunzione e gestione del personale;
- 5) gestione delle risorse finanziarie.

### 1.3 I PROTOCOLLI PER MITIGARE IL RISCHIO

- **Protocolli Generici**

In linea con quanto sopra riportato, la Società ha adottato ed ha debitamente formalizzato e divulgato al proprio interno i seguenti Protocolli Generici, soggetti a periodico aggiornamento:

- Sistema di deleghe e procure con relativi limiti di spesa;
- Principi di comportamento descritti nel Codice Etico;
- Organigramma aziendale e ordinamento organizzativo;
- Sistema sanzionatorio e disciplinare;
- Procedura *Whistleblowing*.

Inoltre, per la medesima finalità, rilevano i seguenti presidi:

- Formazione del Personale;
- Controllo svolto dal Collegio Sindacale;
- Controllo svolto dalla Società di Revisione.
- Controllo svolto dalla Funzione *Compliance*;
- Controllo svolto dalla Funzione *Internal Audit*;
- Supporto del Comitato Controllo, Rischi e Sostenibilità al Consiglio di Amministrazione

nelle valutazioni e decisioni relative al sistema di controllo interno e di gestione dei rischi e all'approvazione delle relazioni periodiche di carattere finanziario e non finanziario, nonché nella promozione della continua integrazione delle *best practice* nazionali e internazionali nella *governance* della Società e dei fattori ambientali, sociali e di governance societaria nelle strategie aziendali volte al perseguimento del successo sostenibile.

- **Protocolli Specifici**

I Protocolli Specifici di Generalfinance si basano sui seguenti principi generali di controllo:

- 1) Separazione dei compiti: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- 2) Esistenza di procedure formalizzate: devono esistere disposizioni aziendali e/o procedure formalizzate, idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- 3) Esistenza di un sistema di deleghe e procure coerente con le responsabilità organizzative assegnate: nell'ambito delle disposizioni aziendali e/o procedure formalizzate, i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere definiti e conosciuti all'interno della società;
- 4) Tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informatici: ogni operazione relativa all'area a rischio 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.

Di seguito, i Protocolli specifici per la riduzione e mitigazione del rischio di commissione di realizzazione dei reati nei confronti della Pubblica Amministrazione ai sensi del Decreto:

- **Protocollo Anticorruzione**: sul presupposto che la Società si pone in una posizione di assoluta intransigenza nei confronti di qualsiasi forma di abuso d'ufficio e corruzione, anche nei confronti di personale di imprese private, il protocollo ha quale obiettivo principale la definizione di regole di condotta e di governo che indichino i comportamenti che i Destinatari devono e non devono tenere nei confronti di soggetti terzi, affinché siano prevenuti comportamenti idonei a realizzare Reati di cui al Decreto (ad es. regole su omaggi, regalie, erogazioni di denaro, sponsorizzazioni e, in generale, gestione rapporti con la PA).
- **Procedura di gestione dei rapporti con la Pubblica Amministrazione**: sul presupposto che la Società si pone in una posizione di assoluta intransigenza nei confronti di qualsiasi forma di abuso d'ufficio e corruzione, la procedura definisce ruoli, responsabilità, modalità operative, controlli e principi comportamentali cui i Destinatari devono attenersi nell'ambito del processo di gestione dei rapporti con la Pubblica Amministrazione affinché siano prevenuti comportamenti idonei a realizzare Reati di cui al Decreto.
- **Protocollo gestione delle liberalità, donazioni, sponsorizzazioni e omaggi**: obiettivo della procedura è la definizione di regole di condotta e operative che indichino i comportamenti cui i Destinatari devono attenersi nell'ambito del processo di gestione delle liberalità (intendendosi con esse le

donazioni, le sponsorizzazioni e gli omaggi) affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.

- **Procedura di approvvigionamento di beni, servizi, consulenze ed incarichi professionali:** obiettivo della procedura è la definizione di regole di condotta e procedurali che indichino i comportamenti cui i Destinatari devono attenersi nella gestione del processo di approvvigionamento affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.
- **Procedura di selezione, assunzione e gestione del personale:** obiettivo della procedura è la definizione di regole di condotta e procedurali che indichino i comportamenti cui i Destinatari devono attenersi nello svolgimento delle attività, nonché dei processi ad esse connessi, di selezione, assunzione e gestione delle risorse umane affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.
- **Vademecum per i rimborsi spese (gestione trasferte e note spese):** obiettivo della procedura è la definizione di regole di condotta e procedurali che indichino i comportamenti che i Destinatari devono e non devono tenere nell'attività di gestione dei rimborsi spese a dipendenti e spese di rappresentanza, affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.
- **Procedura per la gestione dei flussi finanziari (Regolamento tracciabilità flussi finanziari):** la procedura ha lo scopo di definire le regole per la gestione e l'autorizzazione dei flussi finanziari in entrata ed in uscita dalla Società. In particolare, formalizza e definisce le scelte operative e i processi interni preordinati al rispetto delle norme in materia di tracciabilità dei flussi finanziari, con riferimento al pagamento di crediti che abbiano formato oggetto di cessione a favore di Generalfinance.
- **Clausole Contrattuali 231:** il Protocollo ha l'obiettivo di disciplinare le attività di redazione dei contratti con le terze parti, allo scopo di evitare che, nella prestazione dei servizi contrattualizzati, possano essere commessi i Reati di cui al Decreto.

Con particolare riguardo alla corretta gestione dei rapporti con l'Autorità per la vigilanza dei mercati finanziari e con Banca d'Italia, si rende doverosa l'osservanza da parte dei Destinatari del Modello dei seguenti e ulteriori Protocolli specifici:

- **Codice per il trattamento delle Informazioni Privilegiate:** obiettivo del Codice è quello di disciplinare l'individuazione, la gestione e il trattamento delle Informazioni Privilegiate riguardanti la Società, indicando le procedure da osservare nella comunicazione di dette informazioni, affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto. In tale contesto, rivestono un ruolo-chiave:
  - (i) l'obbligo per la Società di informare per iscritto la Consob nell'ipotesi in cui la Società si sia avvalsa della facoltà di ritardare la comunicazione dell'Informazione Privilegiata, (immediatamente dopo la pubblicazione di quella informazione), avendo, altresì, cura di trasmettere all'Autorità la documentazione comprovante la spiegazione delle modalità con cui sono state soddisfatte le condizioni per il ritardo nella comunicazione;
  - (ii) la comunicazione alla Consob dell'elenco delle persone aventi accesso alle Informazioni Privilegiate da parte della Funzione Gestione Informazioni Privilegiate, a seguito di espressa richiesta dell'Autorità.
- **Codice di Comportamento in materia di *internal dealing*:** il Codice ha lo scopo di dare attuazione alle disposizioni comunitarie e nazionali, applicabili, in materia di obblighi di comunicazione, *inter alios*, alla Consob – entro termini e modalità stabilite dal codice – di operazioni concernenti strumenti finanziari o strumenti finanziari collegati – con caratteristiche ben specifiche – realizzate nell'ambito

societario da parte di determinati soggetti collegati all'organizzazione/compagine societaria.

- **Regolamento del voto maggiorato che delinea la disciplina di dettaglio sul voto maggiorato** che, nel codificare la disciplina di dettaglio del voto maggiorato – definendo, più in particolare, le modalità di iscrizione, tenuta e aggiornamento dell'elenco in cui sono iscritti i titolari del diritto reale legittimante che hanno chiesto la maggiorazione del voto, nel rispetto della normativa applicabile – prevede, *inter alia*, la comunicazione alla Consob dell'ammontare complessivo dei diritti di voto, con indicazione del numero di azioni che compongono il capitale sociale, entro il quinto giorno di mercato aperto dalla fine di ciascun mese di calendario durante il quale la Società ha accertato un aumento o una diminuzione di tale ammontare, nonché entro il giorno successivo alla c.d. *record date*.
- **Regolamento in materia di Pianificazione e di Controllo di Gestione** nella parte in cui, disciplinando il controllo e le quadrature per la produzione del *fast closing* e della chiusura trimestrale, regola e impone la comunicazione a Banca d'Italia degli estratti del saldo dei "Crediti verso clientela" derivanti da impieghi per *factoring pro-soluto* e *pro-solvendo*, unitamente alle segnalazioni di vigilanza.
- **Policy di governance del processo ICAAP**, laddove prevede la trasmissione annuale a Banca d'Italia della rendicontazione ICAAP riferita al 31 dicembre dell'anno precedente che documenta il processo di controllo prudenziale attraverso il quale Generalfinance compie una valutazione autonoma della propria adeguatezza patrimoniale.

#### 1.4 CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza esegue verifiche periodiche con riguardo alle specifiche attività sensibili di cui alla presente Parte Speciale secondo le seguenti modalità: (i) attenendosi alla programmazione da esso prevista nel piano di attività elaborato per ciascun anno di riferimento ovvero (ii) a campione, qualora la verifica non sia ricompresa all'interno del piano annuale di attività, ma l'OdV la ritenga comunque necessaria.

#### 1.5 FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

La funzione aziendale nella cui competenza ricade la gestione dell'Attività Sensibile dà apposita evidenza documentale di ogni attività a rischio, secondo quanto previsto dalla specifica procedura operativa applicabile. A seconda dell'attività, la funzione competente dovrà effettuare i controlli definiti nella procedura e, in caso di anomalia, inviare all'Organismo di Vigilanza le opportune segnalazioni e i flussi informativi richiesti.

In ogni caso, la funzione aziendale nella cui competenza ricade la gestione dell'Attività Sensibile, invierà periodicamente all'Organismo di Vigilanza flussi informativi circa:

- le decisioni prese in qualsiasi ambito all'interno della struttura organizzativa che non abbiano seguito il normale *iter* autorizzativo previsto dalle procedure interne;
- la gestione delle operazioni aventi ad oggetto denaro, beni o utilità che possano in generale essere utilizzate come utilità di scambio o provenire da reato o finalizzate alla creazione di "fondi neri";
- le richieste di assistenza, consulenza, fornitura, con corrispettivi superiori ad euro 100.000,00 (centomila/00);
- circostanze significative (quali, ad esempio, procedimenti ispettivi o richieste di chiarimenti) da cui siano scaturiti/e rilievi/richieste da parte delle Autorità, indicando specificamente tutte le informazioni rilevanti (quali, a titolo esemplificativo, Autorità richiedente, i documenti richiesti e/o consegnati, una



sintesi delle informazioni verbali richieste dall’Autorità e/o fornite alla medesima, criticità evidenziate, sanzioni irrogate o altri atti emanati, ecc.);

- gli omaggi, le liberalità e le sponsorizzazioni effettuati per importi superiori a quelli previsti dalla delega/procura conferita al soggetto che ha posto in essere l’atto;
- gli omaggi e le liberalità di cui siano stati destinatari soggetti appartenenti alla Pubblica Amministrazione o Pubblici Ufficiali o Incaricati di Pubblico Servizio.



## **PARTE SPECIALE II**

*Reati societari (art. 25-ter)*

## 1.1 I REATI RICHIAMATI DAL DECRETO E LA RELATIVA MODALITÀ DI COMMISSIONE

- **False comunicazioni sociali delle società quotate (Art. 2622 codice civile)**

A seguito dell'ammissione delle azioni di Generalfinance alla negoziazione sul mercato regolamentato Euronext Milan, gestito da Borsa Italiana S.p.A., acquista prevalente rilievo nell'ambito della presente analisi la norma incriminatrice di cui all'art. 2622 c.c., rubricata "*False comunicazioni sociali delle società quotate*", destinata a prevalere, per specialità, sull'applicazione dell'art. 2621 c.c., che incrimina le ipotesi di c.d. falso in bilancio in relazione alle società non quotate<sup>1</sup>.

In particolare, la condotta illecita di false comunicazioni sociali delle società quotate si realizza mediante condotte che, con riguardo alla situazione economica, patrimoniale o finanziaria della Società (o del gruppo), consistono (alternativamente) nella consapevole:

- esposizione – nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico – di fatti materiali non rispondenti al vero;
- omissione di fatti materiali rilevanti, la cui comunicazione è imposta dalla legge, inerenti alla situazione economica, patrimoniale o finanziaria della Società (o del gruppo al quale la stessa appartiene).

"La condotta in parola è sanzionata penalmente quando risulta rivolta a conseguire, per se o per altri, un ingiusto profitto e idonea a indurre altri in errore.

La disposizione trova applicazione anche qualora le falsità o le omissioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Possono compiere il delitto in questione gli amministratori, i direttori generali, i dirigenti preposti alla redazione delle scritture contabili, i sindaci e i liquidatori di Società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione Europea e la pena prevista per tale reato è costituita dalla reclusione da tre a otto anni.

Quanto alle concrete modalità di condotta del reato di false comunicazioni sociali delle società quotate, l'esposizione di fatti non rispondenti al vero o l'occultamento di informazioni la cui comunicazione è imposta dalla legge può essere realizzata non soltanto attraverso la materiale alterazione di dati contabili (come, ad esempio, nel caso di iscrizione in bilancio di prestazioni mai effettuate o effettuate ad un valore inferiore a quello reale), ma anche attraverso una valutazione estimativa artificiosa di beni o valori inseriti in dette comunicazioni: si pensi, ad esempio, alla valutazione estimativa di immobilizzazioni materiali o finanziarie che fanno parte del patrimonio della società, compiuta in difformità dai criteri indicati nella relazione o da quelli previsti dalla legge o sulla base di parametri comunque irragionevoli e tale, comunque, da ingannare soci o creditori.

Il reato potrà essere commesso nell'interesse della società nel caso, ad esempio, di creazione di riserve occulte illiquide, ottenute attraverso la sottovalutazione di poste attive o la sopravvalutazione di quelle passive per favorire l'autofinanziamento dell'impresa ovvero coprire eventuali perdite intervenute nell'esercizio sociale.

---

<sup>1</sup> Giova evidenziare i tratti differenziali tra l'art. 2621 c.c. e la figura delittuosa disciplinata dall'art. 2622 c.c.: quando il fatto riguarda società diverse da quelle quotate o da quelle ad esse equiparate, l'esposizione di fatti materiali falsi integra il reato di falso in bilancio, previsto e punito dall'art. 2621 c.c., solo se contenuta in comunicazioni sociali previste dalla legge e i dati sono rilevanti. Nel caso di particolare tenuità si applicano le pene attenuate e la causa di esclusione della punibilità.

Praticamente infiniti sono, ancora, gli strumenti economico-finanziari utilizzabili per il trasferimento del denaro da una società all'altra: sovrapprestazioni o false fatturazioni (ad esempio per consulenze fittizie o prestazioni di beni o servizi fittizi), finanziamenti attivi, ecc.

- **Impedito controllo (Art. 2625 codice civile)<sup>2</sup>**

I tipi di condotta sanzionati dalla norma sono di due tipologie: l'occultamento di documenti e l'utilizzo di altri idonei artifici per impedire o ostacolare lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali. L'impedito controllo è un reato proprio, pertanto può essere commesso esclusivamente dagli amministratori.

La sanzione penale è prevista solo nel caso in cui dalla condotta posta in essere derivi un danno ai soci, degradando gli altri casi ad illecito amministrativo.

Il reato *de quo* si perfeziona mediante le seguenti condotte tipiche:

- diniego o accesso alla sede o alle scritture contabili;
- alterazione o sottrazione delle scritture contabili;
- occultamento dei libri sociali;
- rifiuto a fornire chiarimenti o notizie su determinate operazioni;
- omessa convocazione dell'assemblea pur in presenza di richiesta di soci come previsto dalla legge, quando tale assemblea sia richiesta per finalità di controllo.

Si tratta, più precisamente, delle attività che influiscono sulle:

- iniziative di controllo dei soci previste dal codice civile e dagli altri atti normativi, quali ad esempio l'art. 2422 c.c. che prevede il diritto dei soci di ispezionare i libri sociali;
- attività di controllo del Collegio Sindacale, previste dal codice civile e dagli altri provvedimenti normativi, quali ad esempio gli artt. 2403 e 2403-bis che prevedono il potere dei membri del Collegio Sindacale di procedere ad atti di ispezione e di controllo e di richiedere agli amministratori notizie sull'andamento delle operazioni sociali o di determinati affari;
- attività della Società di revisione, previste dalle leggi in materia, quali ad esempio quelle disciplinate dagli artt. 2049 da *bis* a *septies* c.c.

La norma prevede dunque una tutela del:

- controllo interno operato dal collegio sindacale;
- controllo interno operato dal collegio sindacale (nelle società di capitali, a norma dell'art. 2403 c.c.) o dai soci (nei casi previsti, ad esempio, dal codice civile).

- **Indebita restituzione dei conferimenti (Art. 2626 codice civile)**

Il reato si configura quando gli amministratori, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci, ovvero li liberano dall'obbligo di eseguirli.

---

<sup>2</sup> Articolo modificato dall'art. 37.35, lett. a) e b) del d. lg 27 gennaio 2010, n. 39, che ha eliminato il riferimento alle società di revisione come enti deputati al controllo dei documenti societari.

La restituzione dei conferimenti può avvenire sia in forma palese, ancorché indiretta (ad esempio, tramite la compensazione di un debito del socio nei confronti della società), che simulata (ad esempio attraverso il riconoscimento ad un socio di un credito in realtà inesistente, la stipulazione di un mutuo fittizio, la concessione di un prestito senza serie prospettive di restituzione, corresponsione di onorari per prestazioni professionali inesistenti o comunque inadeguate), sia, infine, attraverso una distribuzione di acconti-dividendo o di utili fittizi effettuata con somme prelevate dal capitale sociale.

La seconda ipotesi di condotta consiste nell'esonero dei soci dall'obbligo di eseguire conferimenti rimasti in tutto o in parte inadempiti.

Soggetti attivi del reato possono essere solo gli amministratori (reato proprio): la legge, cioè, non ha inteso punire anche i soci beneficiari della restituzione o della liberazione, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione nei confronti degli amministratori.

- **Illegale ripartizione degli utili e delle riserve (Art. 2627 codice civile)**

Il reato si configura in capo agli amministratori che ripartiscono utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite. E' opportuno, tuttavia, precisare che la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estinguono il reato.

La condotta criminosa di tale reato consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.

Quanto all'individuazione della nozione di "utili", si ritiene che il termine vada inteso nella sua accezione più ampia, quale "utile di bilancio", ossia qualsiasi incremento del patrimonio netto rispetto al valore nominale del capitale, anche se indipendente (diversamente dall'utile d'esercizio) dall'esercizio dell'attività economica.

Ai fini della sussistenza del reato deve trattarsi di utili non effettivamente conseguiti (e dunque fittizi), ovvero non distribuibili, perché destinati per legge a riserva: rilevano, dunque, le sole riserve legali, quali, ad esempio, quelle imposte alla società dagli artt. 2423, co. 4, 2426, n. 4 c.c.

Assume rilievo penale anche la distribuzione di riserve, ancorché non costituite con utili indisponibili per legge: la relazione, al riguardo, fa espressamente riferimento al caso, oggi controverso, delle riserve da sovrapprezzo, nonché di quelle da rivalutazione.

Quanto all'illegale ripartizione di acconti sui dividendi, ossia la distribuzione di acconti su un futuro dividendo in corso di esercizio, il legislatore si limita a sanzionare la ripartizione di acconti sugli utili solo nel caso in cui essi non siano effettivamente conseguiti o siano destinati a riserva legale.

Soggetti attivi del reato sono gli amministratori (reato proprio).

- **Illecite operazioni sulle azioni o quote sociali o della società controllante (Art. 2628 codice civile)**

Commettono il reato in esame gli amministratori che, fuori dei casi consentiti dalla legge (cfr., in particolare, gli artt. 2357, 2359 bis, co. 1, 2360, 2483 e 2529 c.c.), acquistano o sottoscrivono azioni o quote sociali, anche della società controllante (cfr. art. 2359 c.c.) cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

Si precisa che il reato si estingue se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio afferente all'esercizio in relazione al quale è stata posta in essere la condotta.

Le operazioni sulle azioni proprie appartengono alla fisiologia della gestione delle società e possono assolvere a varie funzioni sotto il profilo economico-aziendalístico, molte delle quali perseguite nell'interesse o a vantaggio della società, e dunque idonee, ove sussistano gli estremi del reato di cui all'art. 2628 c.c., a dar luogo a una concorrente responsabilità della Società. Si pensi, ad esempio, ad operazioni di investimento di fondi sociali compiute a fini di speculazione finanziaria ovvero al rastrellamento delle azioni al fine di fronteggiare la prospettiva di scalate ostili mediante offerte pubbliche di acquisto ovvero, ancora, per le società quotate in borsa, ad operazioni volte a regolarizzare i propri corsi azionari, evitando le oscillazioni del titolo in caso di assenza di domanda delle azioni della Società. Più problematica la configurabilità di una concorrente responsabilità dell'ente nell'ipotesi in cui l'operazione di *buy back* sia indirizzata più specificamente a fini interni alla compagine sociale, non direttamente riconducibili ad un interesse generale della Società: così, ad esempio, nel caso di acquisto di azioni realizzato al fine di rafforzare il potere di una maggioranza rispetto alle minoranze, oppure di modificare degli assetti di potere esistenti.

Un'ultima considerazione riguarda le operazioni finanziarie di c.d. *leveraged buy out*, finalizzate all'acquisto di attività di un'azienda, o di partecipazioni di società (azioni o quote), finanziate da un consistente ammontare di debiti e da un limitato o nullo ammontare di mezzi propri, consentiti dall'utilizzo delle attività oggetto dell'acquisizione e dal flusso di cassa che l'investimento genererà in futuro. La rilevanza penale di tali operazioni – che era stata oggetto di dibattito in passato – è oggi espressamente esclusa dal legislatore: come si legge, infatti, nella relazione, *“le operazioni di leveraged buy out sono espressamente considerate a parte dalla legge delega, che conferisce ad esse il crisma della legittimità (art. 7, lett. d)”*. L'art. 2501-bis c.c. – introdotto dalla riforma del diritto societario (D.Lgs. n. 6/2003) entrata in vigore il 1° gennaio 2004 – prevede espressamente la possibilità di procedere alla *“fusione tra società, una delle quali abbia contratto debiti per acquisire il controllo dell'altra, quando per effetto della fusione il patrimonio di quest'ultima viene a costituire garanzia generica o fonte di rimborso di detti debiti”*.

- **Operazioni in pregiudizio dei creditori (Art. 2629 codice civile)**

Il reato in esame si configura quando gli amministratori, violando le disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori.

Si precisa che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Il bene tutelato è l'integrità del capitale sociale quale generale garanzia dei creditori.

Soggetti attivi del reato sono, anche in questo caso, gli amministratori. Tuttavia, i soci che votino la delibera di riduzione del capitale sociale, consapevoli di indurre gli amministratori al fatto, possono eventualmente concorrere nel reato ex art. 110 c.p.

- **Omessa comunicazione del conflitto d'interessi (Art. 2629-bis codice civile)**

La fattispecie è stata introdotta dall'art. 31 della L. n. 262 del 2005 che ha altresì previsto l'introduzione dell'art. 2629-bis c.c. tra i reati che, a norma dell'art. 25-ter del Decreto, possono comportare, ove commessi nell'interesse o a vantaggio dell'ente, la sua responsabilità amministrativa.

La condotta esecutiva del reato è imperniata sulla violazione del precetto civilistico previsto dall'art. 2391 c.c. nell'ipotesi in cui ne derivi un danno alla società o a terzi.

Tale norma – al fine dichiarato di assicurare il valore della trasparenza nella gestione – impone oggi ai componenti del consiglio di amministrazione di dare notizia agli altri amministratori e al collegio sindacale di ogni interesse che, per conto proprio o di terzi, abbiano in una determinata operazione e, ove si tratti di amministratore delegato, astenersi dal compiere l'operazione.

La norma si applica esclusivamente a:

- “società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea”;
  - “società con titoli [...] diffusi tra il pubblico in misura rilevante ai sensi dell'art. 116 del Testo Unico di cui al decreto legislativo 24 febbraio 1998, n. 58”;
  - “soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo 1° settembre 1993, n. 385”, ossia banche, gruppi bancari e intermediari finanziari;
  - “soggetto sottoposto a vigilanza ai sensi del Testo unico di cui al decreto legislativo n. 58 del 1998”, ossia le imprese di investimento (SIM e imprese di investimento comunitarie ed extracomunitarie), le società di gestione del risparmio (SGR), le società di gestione armonizzate, le società di investimento a capitale variabile (SICAV), gli intermediari finanziari iscritti nell'elenco previsto dall'art. 107 del T.U. bancario e le banche autorizzate all'esercizio dei servizi di investimento;
  - “soggetto sottoposto a vigilanza ai sensi del d. lg. 7 settembre 2005, n. 209<sup>3</sup>”;
  - “soggetto sottoposto a vigilanza ai sensi del decreto legislativo 21 aprile 1993, n. 124<sup>4</sup>”.
- **Formazione fittizia del capitale (Art. 2632 codice civile)**

Tale ipotesi di reato mira a tutelare l'integrità del capitale sociale, punendo gli amministratori ed i soci conferenti che:

- 1) formano o aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale. Trattasi di condotta che impedisce la integrale copertura del capitale nominale;
- 2) effettuano una sottoscrizione reciproca di azioni o quote. Il carattere della reciprocità non richiede necessariamente la contestualità temporale delle operazioni, né la loro connessione. La sottoscrizione reciproca può, infatti, concernere sia operazioni omogenee (relative, ad esempio, all'aumento del capitale) sia operazioni tra loro eterogenee (concernenti, ad esempio, la costituzione della società e l'aumento del capitale). Ciò che rileva è la previa sussistenza di uno specifico accordo (anche tacito), non casuale incentrato su di un'intesa *ad hoc*, avente appunto ad oggetto lo scambio di azioni o quote. Si tratta di un reato necessariamente plurisoggettivo;
- 3) effettuano una sopravvalutazione rilevante dei conferimenti di beni in natura e dei crediti ovvero del patrimonio sociale nel caso di trasformazione. La terza condotta incriminata dalla norma in esame può essere realizzata sia in fase genetica di costituzione della società che in quella successiva di aumento di capitale sociale. Oggetto della sopravvalutazione sono, alternativamente, i beni, i crediti ed il patrimonio.

<sup>3</sup> Le parole del “d. lg. 7 settembre 2005, n. 209” sono state sostituite alle precedenti “della legge 12 agosto 1982, n. 576” dall'art. 6, d. lg. 29 dicembre 2006, n. 303.

<sup>4</sup> Il decreto legislativo 21 aprile 1993, n. 124 è stato abrogato dall'art. 21.8 d. lg. 5 dicembre 2005, n. 252.

Soggetti attivi del reato sono gli amministratori e i soci conferenti.

Soggetto attivo può essere anche l'esperto nominato dal Tribunale che redige la relazione giurata di stima da allegare all'atto costitutivo o di aumento del capitale sociale.

- **Indebita ripartizione dei beni sociali da parte dei liquidatori (Art. 2633 codice civile)**

Tale ipotesi di reato si configura nei casi in cui il liquidatore cagioni un danno ai creditori sociali per aver ripartito i beni della società tra i soci prima ancora di aver soddisfatto i creditori sociali stessi ovvero di aver accantonato le somme necessarie per soddisfarli.

Il reato si estingue se prima del giudizio ai creditori venga rifiuto il danno dagli stessi patito a seguito della suddetta condotta illecita.

Soggetti attivi del reato sono esclusivamente i liquidatori.

- **Illecita influenza sull'assemblea (Art. 2636 codice civile)**

Tale ipotesi di reato si configura nel caso in cui chiunque (gli amministratori, i direttori generali, il dirigente preposto, i sindaci, i liquidatori e/o i responsabili della revisione), con atti simulati o fraudolenti, determini la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto.

Si precisa che la norma si applica anche alle società con socio unico o, comunque, quasi totalitario, in quanto anche in tali casi è evidentemente possibile l'alterazione della volontà del socio espressa in assemblea.

La norma mira ad evitare che, attraverso condotte fraudolente (come, ad esempio, la cessione fittizia delle quote a persona di fiducia al fine di ottenerne il voto in assemblea oppure la fittizia sottoscrizione di un prestito con pegno delle quote, in modo da consentire al creditore pignoratizio l'esercizio del diritto di voto in assemblea) si influisca illegittimamente sulla formazione della maggioranza assembleare.

Ai fini della norma in esame vengono in considerazione le condotte volte alla convocazione dell'assemblea, all'ammissione alla partecipazione all'assemblea e al computo dei voti per la deliberazione, nonché le relative attività di supporto.

È opportuno ricordare che la responsabilità della Società è configurabile solo quando la condotta prevista dall'articolo in esame sia realizzata nell'interesse di Generalfinance. Ciò rende difficilmente ipotizzabile il reato in questione che, di norma, viene realizzato per favorire interessi di parte e non della Società.

- **Aggiotaggio (Art. 2637 codice civile)**

La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato<sup>5</sup> ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

Anche questo reato è un reato comune, che può essere commesso da chiunque.

- **Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (Art. 2638 codice civile)**

Si tratta di una fattispecie generale, a fini di coordinamento e di uniformità sanzionatoria, si sostituisce alle diverse figure di falsità nelle comunicazioni, di omissione di comunicazioni e di ostacolo nello svolgimento

---

<sup>5</sup> Le parole "strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato" sono state così sostituite alle precedenti "strumenti finanziari quotati o non quotati" dall'art. 9.4, l.18 aprile 2005 n. 62.

delle funzioni delle Autorità di Vigilanza previste fuori dal codice civile (ad esempio, Consob, Banca d'Italia, U.I.F., Ivass).

La norma individua due distinte ipotesi di reato:

- la prima si realizza attraverso l'esposizione nelle comunicazioni alle Autorità di Vigilanza previste dalla legge, al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazione, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza, ovvero con l'occultamento con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima;
- la seconda, che configura un reato di evento a forma libera, si realizza con il semplice ostacolo all'esercizio delle funzioni di vigilanza, attuato consapevolmente, in qualsiasi forma, anche omettendo le comunicazioni dovute alle autorità di vigilanza.

La fattispecie *de qua* individua un'ipotesi di reato proprio, per cui soggetti attivi sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione di documenti contabili societari, i sindaci, i liquidatori di società ed enti e gli altri soggetti per legge alle Autorità pubbliche di vigilanza, o tenuti a obblighi nei loro confronti.

## 1.2 ATTIVITÀ SENSIBILI

Riguardo alle fattispecie di reati sopra descritte, i Processi Sensibili individuati nell'ambito delle attività della Società sono:

1. gestione e monitoraggio della tenuta della contabilità generale;
2. predisposizione e stesura del *budget* e del bilancio d'esercizio, nonché pianificazione strategica e finanziaria;
3. elaborazione/formazione e gestione delle comunicazioni sociali previste dalla legge e, più in generale, dell'informativa societaria, ivi inclusa la predisposizione di note e prospetti informativi rivolti al pubblico (ad esempio, resoconto intermedio di gestione, relazione finanziaria annuale, semestrale e trimestrale);
4. gestione della tesoreria e dei flussi finanziari in entrata ed in uscita;
5. gestione delle consulenze e degli incarichi professionali nonché dei relativi pagamenti;
6. gestione delle liberalità, sponsorizzazioni e omaggi;
7. gestione dei rimborsi spese;
8. gestione dei rapporti con i soci/azionisti, gli investitori, potenziali o effettivi, e la comunità finanziaria, nonché con gli organi di controllo e con la Società di revisione;
9. gestione del patrimonio aziendale, delle operazioni sul capitale sociale/straordinarie e relativi adempimenti;
10. regolamentazione e gestione dell'esercizio dei diritti sociali connessi con la proprietà delle azioni della Società e relativi adempimenti, con particolare riguardo alla maggioranza del diritto di voto e ai patti parasociali;
11. gestione delle operazioni con parti correlate;
12. gestione dei rapporti e delle informative/delle segnalazioni dirette alle Autorità di Vigilanza (in particolare, Consob e Banca di Italia) anche in occasione di verifiche, ispezioni ed accertamenti.

## 1.3 I PROTOCOLLI PER MITIGARE IL RISCHIO



Tutte le attività a rischio sono svolte conformandosi alle leggi e alla regolamentazione secondaria vigenti e seguendo i principi, le procedure e i protocolli aziendali, generici e specifici, di cui al presente Modello.

- **Protocolli Generici**

In linea con quanto sopra riportato, la Società ha adottato ed ha debitamente formalizzato e divulgato al proprio interno i seguenti Protocolli Generici, soggetti a periodico aggiornamento:

- o Sistema di deleghe e procure con relativi limiti di spesa;
- o Principi di comportamento descritti nel Codice Etico;
- o Organigramma aziendale e ordinamento organizzativo;
- o Sistema sanzionatorio e disciplinare;
- o Formazione del Personale;
- o Procedura *Whistleblowing*.

Inoltre, per la medesima finalità, rilevano i seguenti presidi:

- o Controllo svolto dal Collegio Sindacale;
- o Controllo svolto dalla Società di Revisione;
- o Controllo svolto dalla Funzione *Compliance*;
- o Controllo svolto dalla Funzione *Internal Audit*;
- o Controllo svolto dalla Funzione *Risk Management*;
- o Supporto del Comitato Controllo, Rischi e Sostenibilità al Consiglio di Amministrazione nelle valutazioni e decisioni relative al sistema di controllo interno e di gestione dei rischi e all'approvazione delle relazioni periodiche di carattere finanziario e non finanziario, nonché nella promozione della continua integrazione delle *best practice* nazionali e internazionali nella *corporate governance* della Società e dei fattori ambientali, sociali e di *governance* nelle strategie aziendali volte al perseguimento del successo sostenibile. Ad esso sono state attribuite anche le funzioni di comitato per le operazioni con parti correlate, fatta eccezione per le decisioni relative ad operazioni aventi a oggetto le remunerazioni degli amministratori e dei dirigenti con responsabilità strategiche;
- o Supporto del Comitato Nomine e Remunerazione al Consiglio di Amministrazione nell'elaborazione della politica di remunerazione, nel monitorare la concreta applicazione di tale politica e nel verificare l'effettivo raggiungimento degli obiettivi di *performance*, nonché nell'autovalutazione del Consiglio stesso e dei suoi comitati, nella definizione della loro composizione ottimale e nell'individuazione di una lista per l'elezione dell'organo amministrativo, secondo modalità che ne assicurino una formazione e una presentazione trasparente.

Con particolare riguardo alla tutela della trasparenza dell'informazione societaria, si segnala che Generalfinance ha nominato, ai sensi dell'art. 154-*bis* del T.U.F., il **Dirigente preposto alla redazione dei documenti contabili societari**, a cui spetta la responsabilità del sistema di controllo interno in materia di informativa finanziaria. Tra le sue principali funzioni si annoverano: (i) la predisposizione di adeguate procedure amministrative per la formazione del bilancio di esercizio, nonché di ogni altra comunicazione di carattere finanziario della Società; (ii) il supporto al *management* nell'identificazione e nella valutazione dei rischi di informativa finanziaria, oltre che l'individuazione dei relativi controlli da porre a presidio; (iii) la

predisposizione di una relazione annuale e di una semestrale sulla valutazione del sistema di controllo sull'informativa finanziaria a supporto del rilascio delle attestazioni; (iv) l'attestazione con apposita relazione sul bilancio d'esercizio, unitamente all'Amministratore Delegato; (v) l'attestazione della corrispondenza degli atti e delle comunicazioni di Generalfinance diffusi al mercato, concernenti l'informativa contabile (anche infra-annuale) della Società, alle risultanze documentali, ai libri e alle scritture contabili della stessa.

- **Protocolli Specifici**

I Protocolli Specifici di Generalfinance si basano sui seguenti principi generali di controllo:

- 1) Separazione dei compiti: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- 2) Esistenza di procedure formalizzate: devono esistere disposizioni aziendali e/o procedure formalizzate, idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- 3) Esistenza di un sistema di deleghe e procure coerente con le responsabilità organizzative assegnate: nell'ambito delle disposizioni aziendali e/o procedure formalizzate, i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere definiti e conosciuti all'interno della società;
- 4) Tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informatici: ogni operazione relativa all'area a rischio 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.

Oltre ai protocolli di carattere generale, la Società ha sviluppato e implementato i seguenti protocolli specifici per la riduzione del rischio di realizzazione dei reati societari ovvero di condotte strumentali:

- **Protocollo per la gestione delle liberalità, donazioni, sponsorizzazioni e omaggi**: obiettivo della procedura è la definizione di regole di condotta e procedurali che indichino i comportamenti cui i Destinatari devono attenersi nell'ambito del processo di gestione delle liberalità (intendendosi con esse le donazioni, le sponsorizzazioni e gli omaggi) affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.
- **Procedura gestione dei rapporti con i soci e con gli organi di controllo**: obiettivo della procedura è la definizione di regole di condotta e operative che indichino i comportamenti cui i Destinatari devono attenersi nelle attività connesse con la gestione dei rapporti con i soci e gli organi di controllo societario affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.
- **Politica per la gestione del dialogo con gli azionisti e gli altri soggetti interessati** che regola le modalità di svolgimento del rapporto dialettico e istituzionale tra i soggetti interessati all'operatività/andamento aziendale (ad esempio, gli azionisti, i titolari o portatori di altri strumenti finanziari emessi, gli investitori istituzionali attuali e potenziali, ecc.) e la Società su materie/tematiche di competenza del Consiglio di Amministrazione al di fuori dell'informativa resa e delle interlocuzioni instaurate con gli azionisti in relazione e/o in occasione delle Assemblee.
- **Procedura approvvigionamento di beni, servizi, consulenze ed incarichi professionali**: obiettivo della procedura è la definizione di regole di condotta e procedurali che indichino i comportamenti

cui i Destinatari devono attenersi nella gestione del processo di approvvigionamento affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.

- **Procedura gestione della tesoreria:** obiettivo della procedura è la definizione di regole di condotta e procedurali che indichino i comportamenti cui i Destinatari devono attenersi nell'ambito dei processi connessi all'amministrazione della tesoreria aziendale e, in particolare, degli investimenti e disinvestimenti, degli affidamenti bancari e approvvigionamenti, della gestione della liquidità, nonché della gestione amministrativa di incassi e pagamenti, affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.
- **Procedura gestione della contabilità e redazione del bilancio fiscale (Policy redazione bilancio di esercizio):** il cui obiettivo è definire le regole di condotta e operative che indicano i comportamenti cui i Destinatari devono attenersi nella gestione dei processi legati alla tenuta della contabilità, alla redazione del bilancio, nonché di tutte quelle attività connesse alla pianificazione strategica, alla predisposizione del budget e al controllo di gestione, affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.
- **Policy per la determinazione degli accantonamenti,** che stabilisce i criteri di contabilizzazione che la Società segue in merito agli accantonamenti da rilevare a fronte di rischi ed oneri.
- **Procedura per la gestione dei flussi finanziari (Regolamento tracciabilità flussi finanziari):** l'obiettivo è formalizzare e definire le scelte operative e i processi interni preordinati al rispetto delle norme in materia di tracciabilità dei flussi finanziari con particolare riferimento al pagamento dei crediti che hanno formato oggetto di cessione a favore di Generalfinance, in considerazione del *core business* societario.
- **Regolamento in materia di Pianificazione e di Controllo di Gestione** che descrive e detta le regole del processo di pianificazione e controllo di gestione di cui la Società si è dotata per supportare adeguatamente le decisioni operative e strategiche attraverso strumenti di misurazione dell'efficacia e dell'efficienza, e in particolare: piani, documenti di programmazione, indicatori di *performance*, contabilità analitica, sistema di *reporting* interno, bilancio consolidato e bilancio sociale.
- **Policy di Governance del Processo ICAAP:** obiettivo della Policy è quello di documentare e formalizzare il processo di controllo prudenziale (ovverosia: il processo ICAAP) mediante il quale la Società compie una valutazione, sia attuale che prospettica, della propria adeguatezza patrimoniale tenendo in considerazione: i) i rischi assunti nello svolgimento della propria attività; ii) gli obiettivi strategici; iii) la struttura di governo e controllo; iv) il sistema di gestione dei rischi; v) le variabili di contesto. In essa sono, altresì, definiti ruoli e responsabilità degli organi e delle funzioni aziendali coinvolti nella gestione dei rischi e le metodologie di valutazione dell'esposizione. La Società trasmette annualmente alla Banca d'Italia, entro il 30 aprile, la rendicontazione ICAAP riferita al 31 dicembre dell'anno precedente.
- **Policy in materia di classificazione e valutazione delle esposizioni creditizie:** scopo della *Policy* è quello di formalizzare e definire le scelte operative e i processi preordinati ad una corretta classificazione e valutazione delle esposizioni creditizie della Società, conformemente a quanto stabilito sia dalla normativa di Vigilanza sia dal principio contabile IFRS 9, il quale fissa le regole relative alla classificazione ed alla misurazione degli strumenti finanziari.
- **Manuale Metodologico (Governance 262/05) – Regolamento del Dirigente Preposto** che è volto a descrivere e definire le linee guida e la prassi operativa che la struttura organizzativa aziendale deve seguire per presidiare e neutralizzare il rischio di errata informativa finanziaria, prevedendo controlli interni a livello societario, controlli dei processi amministrativo-finanziari e controlli sul governo dei sistemi e degli strumenti informatici implementati.
- **Regolamento in materia di redazione dell'Informativa al pubblico di "Terzo Pilastro":** scopo del

Regolamento aziendale è quello di definire e di formalizzare le modalità che la Società deve adottare per la predisposizione dell'Informativa di Terzo Pilastro – la quale ha ad oggetto l'adeguatezza patrimoniale della Società, la sua esposizione ai rischi e le caratteristiche generali dei sistemi interni di gestione e controllo ed è prevista dal Regolamento (UE) 575/2013 (CRR) –, nonché di individuare le responsabilità delle funzioni preposte alla predisposizione della stessa.

- **Codice di Comportamento in materia di *internal dealing*:** il Codice ha lo scopo di dare attuazione alle disposizioni comunitarie e nazionali applicabili in materia di obblighi di comunicazione al pubblico, a Consob e alla Società di operazioni concernenti strumenti finanziari o strumenti finanziari collegati realizzate nell'ambito societario da parte di determinati soggetti (segnatamente: i gli azionisti che detengono una partecipazione pari almeno al 10% del capitale sociale componenti del Consiglio di Amministrazione e del Collegio Sindacale, il *top management*, nonché le persone fisiche e giuridiche ad essi strettamente legate). Oltre a fissare (i) gli obblighi di comunicazione dei soggetti rilevanti, degli azionisti rilevanti e delle persone strettamente legate in merito alla realizzazione delle predette operazione, (ii) le modalità e le tempistiche di notifica, nonché (iii) la funzione aziendale preposta a garantire l'osservanza delle regole ivi previste, il Codice fissa i divieti al compimento delle operazione in questione (con particolare riguardo ai c.d. *black out period*) e la possibilità di porre ulteriori divieti/limitazioni ad opera del Consiglio di Amministrazione.
- **Regolamento del voto maggiorato** che delinea la disciplina di dettaglio sul voto maggiorato, prevedendo, in particolare, le modalità di iscrizione, tenuta e aggiornamento dell'elenco in cui sono iscritti i titolari del diritto reale legittimante che hanno chiesto la maggiorazione del voto, nel rispetto della normativa applicabile, in modo da assicurare il tempestivo scambio di informazioni tra gli azionisti della Società, la Società stessa e gli intermediari abilitati alla tenuta dei conti sui quali sono registrate le azioni. Inoltre, il Regolamento fissa gli obblighi di comunicazione verso il pubblico e la Consob a cui la Società deve periodicamente adempiere, avendo riguardo ai dati identificativi degli azionisti che richiedono l'iscrizione nell'Elenco Speciale e l'ammontare complessivo dei diritti di voto.
- **Procedura per le operazioni con parti correlate:** la procedura disciplina le condizioni e le modalità di realizzazione di operazioni con parti correlate da parte della Società, ai sensi dell'art. 2391-*bis* c.c. e in conformità alla normativa primaria (europea e nazionale) e a quella regolamentare emanata dalla Consob della normativa regolamentare emanata da Consob, distinguendo tra operazioni di minore rilevanza e quelle di maggiore rilevanza e prevedendo altresì (i) l'istituzione di un registro nel quale vengono iscritte le parti correlate e, soprattutto, (ii) gli obblighi di comunicazione al pubblico e alla Consob che devono essere assolti dalla Società; unitamente al **Regolamento del Comitato Controllo, Rischi e Sostenibilità** laddove prevede che il Comitato è chiamato, tra le altre cose, ad esprimere pareri preventivi in occasione dell'approvazione da parte dell'organo competente di determinate operazioni poste in essere dalla Società, anche per il tramite di società da essa controllate, con parti correlate.
- **Politica di remunerazione** che stabilisce i principi e le linee guida sulla base dei quali sono determinati i compensi fissi e variabili (componenti di breve e lungo termine) dei membri del Consiglio di Amministrazione, dell'organo di controllo e dei Dirigenti con Responsabilità Strategiche, oltre che i benefici non monetari e i piani di incentivazione basati su strumenti finanziari diversi dalle *stock option*; unitamente al **Regolamento del Comitato Nomine e Remunerazione** che svolge funzioni istruttorie, propositive e consultive nei confronti del Consiglio di Amministrazione in materia di remunerazione degli amministratori, dei sindaci e del *top management*, nonché in merito alla composizione e dimensione del Consiglio stesso, mediante la formulazione di pareri,

raccomandazioni e proposte.

- **Clausole Contrattuali 231:** il Protocollo ha l'obiettivo di disciplinare le attività di redazione dei contratti con le terze parti, allo scopo di evitare che, nella prestazione dei servizi contrattualizzati, possano essere commessi i Reati di cui al Decreto.

**Per quanto attiene alla gestione dei rapporti con le Autorità di Vigilanza trovano applicazione gli ulteriori Protocolli Specifici contemplati nella Parte Speciale I – “Reati Corruttivi”. Con riguardo all'utilizzo dei sistemi e degli strumenti informatici e telematici nell'ambito delle attività sensibili si osservano, altresì, i Protocolli Specifici richiamati nella Parte Speciale IV – “Reati Informatici”.**

#### 1.4 CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza esegue verifiche periodiche con riguardo alle specifiche attività sensibili di cui alla presente Parte Speciale secondo le seguenti modalità: (i) attenendosi alla programmazione da esso prevista nel piano di attività elaborato per ciascun anno di riferimento ovvero (ii) a campione, qualora la verifica non sia ricompresa all'interno del piano annuale di attività, ma l'OdV la ritenga comunque necessaria.

#### 1.5 FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

La funzione aziendale nella cui competenza ricade la gestione dell'Attività Sensibile dà apposita evidenza documentale di ogni attività a rischio, secondo quanto previsto dalla specifica procedura operativa applicabile. A seconda dell'attività, la funzione competente dovrà effettuare i controlli definiti nella procedura e, in caso di anomalia, inviare all'Organismo di Vigilanza le opportune segnalazioni e i flussi informativi richiesti.

Più concretamente, le funzioni aziendali coinvolte provvedono a comunicare periodicamente all'Organismo di Vigilanza:

- le decisioni prese in qualsiasi ambito all'interno della struttura organizzativa che non abbiano seguito il normale *iter* autorizzativo previsto dalle procedure interne;
- le risultanze di eventuali perizie effettuate;
- le eventuali comunicazioni della Società di Revisione riguardanti aspetti che possono indicare una carenza nei controlli interni;
- il bilancio annuale, corredato della nota integrativa, nonché la situazione patrimoniale semestrale e ogni altra informativa diretta al pubblico relativa alla situazione economica, finanziaria e patrimoniale della Società;
- le comunicazioni, da parte del Collegio Sindacale e della Società di Revisione, relative ad ogni criticità emersa, anche se risolta.

Con riferimento al bilancio e alle altre comunicazioni sociali, i controlli dell'Organismo di Vigilanza riguardano: (i) la verifica di eventuali specifiche situazioni o circostanze segnalate dagli organi di controllo interno ed esterno o da qualsiasi dipendente e (ii) l'esecuzione degli accertamenti ritenuti necessari in conseguenza delle segnalazioni ricevute.

Le funzioni coinvolte nel processo a rischio reati societari provvedono, inoltre, a comunicare tempestivamente all'Organismo di Vigilanza ogni violazione o sospetto di violazione di propria conoscenza rispetto alle modalità esecutive disciplinate dai Protocolli della Società e dal Codice Etico.





### **PARTE SPECIALE III**

*Reati di Ricettazione, Riciclaggio e Impiego di denaro, beni o utilità di provenienza illecita nonché di auto-riciclaggio (Art. 25-Octies)*

## 1.1 I REATI RICHIAMATI DAL DECRETO E LA RELATIVA MODALITÀ DI COMMISSIONE

Con il D. Lgs. n. 231 del 21 novembre 2007 (di seguito, il “D. Lgs. 231/2007”), il Legislatore ha dato attuazione alla direttiva 2005/60/CE del Parlamento e del Consiglio, del 26 ottobre 2005, concernente la prevenzione dell’utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (c.d. III direttiva antiriciclaggio) e alla direttiva 2006/70/CE della Commissione che ne reca le misure di esecuzione. L’intervento normativo ha comportato un riordino della complessa normativa antiriciclaggio.

Il panorama normativo è stato poi recentemente innovato: i) con la Direttiva (UE) 2015/849 relativa alla prevenzione dell’uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (c.d. IV Direttiva Antiriciclaggio)<sup>1</sup> che ha abrogato la III Direttiva) con la Direttiva (UE) 2018/843 (c.d. V Direttiva Antiriciclaggio) recentemente recepita all’interno del nostro ordinamento con Decreto Legislativo n. 125 del 4 ottobre 2019 e, da ultimo, iii) con la Direttiva (UE) 2018/1673 “*sulla lotta al riciclaggio mediante diritto penale*”, che è stata recepita dall’Italia con il Decreto Legislativo n. 195 dell’8 novembre 2021.

Al riguardo, merita segnalare che quest’ultima novella legislativa ha significativamente ampliato l’area di precettività delle norme incriminatrici della ricettazione (art. 648 c.p.), del riciclaggio (art. 648-bis c.p.), dell’impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.) e dell’autoriciclaggio (art. 648-ter.1 c.p.), prevedendo principalmente:

- l’estensione del novero dei reati presupposto (c.d. *predicate crime*) di tutte le predette fattispecie criminose, nelle cui maglie ricadono ora sia i delitti colposi, che le contravvenzioni punite con la pena detentiva dell’arresto superiore nel massimo a un anno ovvero nel minimo a sei mesi;
- la diversificazione della risposta sanzionatoria a seconda che il reato presupposto configuri un delitto ovvero una contravvenzione.

L’art. 25-octies<sup>2</sup> D.Lgs. n. 231/2001 estende la responsabilità amministrativa degli enti ai reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, auto-riciclaggio previsti dagli artt. 648, 648-bis, 648-ter e 648-ter.1 c.p., nei casi in cui il reato sia commesso nell’interesse o a vantaggio dell’ente medesimo.

- **Ricettazione (Art. 648 codice penale)**

Il reato in esame si configura in capo a chiunque, al di fuori dei casi di concorso nel reato, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto (anche colposo) ovvero da contravvenzione punita con l’arresto superiore nel massimo a un anno o nel minimo a sei mesi, o comunque si intromette nel farle acquistare, ricevere od occultare (c.d. intermediazione).

Lo scopo dell’incriminazione della ricettazione è quello di impedire il perpetrarsi della lesione di interessi patrimoniali iniziata con la consumazione del reato principale. Ulteriore obiettivo della incriminazione consiste nell’evitare la commissione dei reati principali, come conseguenza dei limiti posti alla circolazione dei beni provenienti dai reati medesimi.

---

<sup>1</sup> La IV Direttiva antiriciclaggio, recepita nel nostro ordinamento dal D. Lgs. 19 giugno 2017, n. 90, pur apportando significative novità in materia di antiriciclaggio, non ha inciso sulla responsabilità amministrativa degli enti.

<sup>2</sup> Cfr. art. 25-octies “*Si applica all’ente la sanzione pecuniaria da 200 a 800 quote. Nel caso in cui il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni si applica la sanzione pecuniaria da 400 a 1000 quote*”.

La ricettazione è un reato contro il patrimonio, la cui oggettività giuridica si sostanzia nell'interesse di garantire il diritto del privato contro l'intervento di attività estranee al delitto anteriore, capaci di portare alle estreme conseguenze il pregiudizio già provocato e di rendere più difficoltoso il recupero del prodotto stesso.

Con riferimento agli elementi costitutivi del reato, si precisa che:

- la condotta che assume preminente rilievo nel reato di specie è quella avente ad oggetto l'acquisto (*lato sensu*) del possesso di cose di provenienza criminosa, riferibile sia ai delitti (dolosi o colposi) che alle contravvenzioni punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi, allo scopo di trarre da queste un profitto. Per la configurabilità dell'"acquisto" non è necessario che sussista un vincolo di proprietà sul denaro o sulle altre cose provenienti dal reato (delitto o contravvenzione), considerato che, da un lato, è sufficiente il loro mero possesso e, dall'altro, ben può rientrare in tale concetto qualsiasi attività negoziale, a titolo sia oneroso che gratuito, idonea a realizzare il trasferimento della cosa nella sfera giuridico-patrimoniale dell'acquirente; per "ricezione" deve intendersi, invece, qualsiasi forma di acquisizione delle cose che implichi il materiale mutamento della detenzione della *res*, a titolo definitivo o temporaneo, gratuito od oneroso, essendo sufficiente il conseguimento di qualsiasi utilità, anche non patrimoniale; infine, l'"occultamento" sottende il nascondimento anche temporaneo del denaro o della cosa, dopo che l'agente ne sia entrato in possesso;
- l'altra condotta incriminata riguarda la c.d. intermediazione nella ricettazione da parte di altra persona: per la sua configurabilità non è necessario che venga posta in essere un'attività di mediazione in senso civilistico, bensì costituisce condizione necessaria e indefettibile che il soggetto mediatore funga, in concreto, da tramite tra le due (o più) parti per far acquistare da una di esse la cosa di provenienza illecita, con modalità idonee e univoche rispetto al predetto scopo;
- quanto all'elemento soggettivo del reato, per la configurabilità della ricettazione è necessaria la consapevolezza della provenienza illecita del bene ricevuto, senza che sia indispensabile che tale consapevolezza si estenda alla completa e precisa conoscenza delle circostanze di tempo, di modo e di luogo del reato presupposto, potendo anche essere desunta da prove indirette, purché gravi, univoche e tali da generare in qualsiasi persona di media levatura intellettuale, secondo la comune esperienza, la certezza della provenienza illecita di quanto ricevuto; ed infatti, per l'affermazione della responsabilità non è necessario l'accertamento giudiziale della commissione del delitto presupposto, né dei suoi autori, né dell'esatta tipologia del reato;
- la ricettazione di particolare tenuità di cui all'art. 648, comma 4, c.p., non costituisce un'autonoma ipotesi incriminatrice, ma una circostanza attenuante speciale che per essere rilevante deve comportare che la cosa ricettata sia di valore economico particolarmente tenue;
- qualora le condotte alternative di acquisto, ricezione od occultamento abbiano ad oggetto denaro o cose provenienti da una contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi, il trattamento sanzionatorio subisce una mitigazione, così come previsto dall'inedito comma 2;
- per converso, la pena è aumentata nel caso in cui i) il fatto riguardi denaro o cose provenienti dai delitti di rapina aggravata ex art. 628, comma 3, c.p., di estorsione aggravata (art. 629, comma 2, c.p.) o di furto aggravato commesso su componenti sottratte ad infrastrutture destinate all'erogazione di energia, di servizi di trasporto, telecomunicazioni o di altri servizi di pubblico rilievo (art. 625, comma 1, n. 7-bis c.p.), ovvero ii) il fatto sia stato commesso nell'esercizio di un'attività professionale;

- la ricettazione è perseguibile anche se l'autore del reato presupposto da cui il denaro o le cose provengono non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale reato.

A mero titolo esemplificativo, il reato potrebbe configurarsi qualora la Società, nell'ambito della propria attività *core*, una volta acquisita la pratica, riceva e registri gli incassi, sapendo (o potendo sapere) che gli stessi derivino da una provvista di matrice criminosa e si astenga da qualsiasi segnalazione. Il delitto potrebbe, inoltre, essere integrato dall'acquisto, dall'emissione di un ordine ovvero dalla sottoscrizione di un contratto di acquisto di beni da un fornitore, appositamente selezionato, che offra cose di provenienza illecita a prezzi sensibilmente inferiori rispetto a quelli di mercato, con conseguente utilizzo degli stessi nell'ambito delle attività operative della Società. Ancora, il delitto *de quo* si potrebbe realizzare nell'ipotesi in cui un esponente di Generalfinance, nell'implementare un investimento in strumenti finanziari, proceda all'investimento o ad un'operazione, al fine di far conseguire un profitto alla Società, sebbene abbia la consapevolezza o si sia rappresentato la concreta possibilità che lo strumento finanziario oggetto d'investimento sia stato acquisito con fondi di provenienza illecita; e ciò in quanto abbia ommesso o condotto in modo erroneo la verifica dell'attendibilità commerciale e professionale della controparte, pur in presenza degli indici di anomalia previsti dall'art. 6, comma 4, lett. e) D.Lgs. n. 231/2007 e individuati con successivi provvedimenti attuativi.

- **Riciclaggio (Art. 648-bis codice penale)**

Il reato in esame si configura in capo a chiunque, al di fuori dei casi di concorso nel reato, sostituisce (e.g. "ripulendo" il bene mediante il conseguimento di un valore equivalente), trasferisce (e.g. mutando il rapporto di titolarità) denaro, beni o altre utilità provenienti da delitto (doloso o colposo che sia) o da contravvenzione, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Lo scopo dell'incriminazione del reato di riciclaggio è quello di impedire che gli autori dei reati possano fruttare i capitali illegalmente acquisiti, rimettendoli in circolazione come capitali ormai "depurati" e perciò investibili anche in attività economiche produttive lecite. In tal modo, la norma incriminatrice persegue anche un ulteriore obiettivo-finale, vale a dire scoraggiare la stessa commissione dei reati principali, mediante le barriere frapposte alla possibilità di sfruttarne i proventi.

Con riferimento agli elementi costitutivi del reato, si precisa che:

- la fattispecie in oggetto, pur configurando un reato a forma libera, richiede che la condotta del riciclaggio sia caratterizzata da un tipico effetto dissimulatorio, risultando diretta in ogni caso ad ostacolare l'accertamento sull'origine illecita di denaro, beni od altre utilità. In particolare, integra il reato di riciclaggio il compimento di operazioni volte non solo ad impedire in modo definitivo ma anche a rendere difficile l'accertamento circa la provenienza del denaro, dei beni o altre utilità, attraverso un qualsiasi espediente che consista nell'aggirare la libera e normale esecuzione dell'attività posta in essere;
- quanto all'elemento soggettivo, questo è integrato dal dolo generico che ricomprende sia la volontà di compiere le attività relative ad impedire l'identificazione della provenienza diletta di beni, sia la consapevolezza di tale provenienza senza alcun riferimento a scopi di profitto o di lucro;
- qualora le condotte incriminate abbiano ad oggetto denaro o cose provenienti da una contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi, il trattamento sanzionatorio subisce una mitigazione, così come previsto dall'inedito comma 2;

- del pari, è prevista un'attenuazione della pena nel caso in cui il denaro, i beni o le altre utilità provengano da un delitto punito con la reclusione inferiore nel massimo a cinque anni;
- di contro, la pena è aumentata se il fatto è commesso nell'esercizio di un'attività professionale;
- da ultimo, si badi che il riciclaggio è perseguibile anche se l'autore del reato presupposto da cui il denaro o le cose provengono non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale reato.

A mero titolo esemplificativo, il reato potrebbe configurarsi qualora la Società, nell'ambito della propria attività *core*, conceda al cliente l'affidamento richiesto, pur essendo consapevole che il debito ceduto sia frutto di un delitto o di una contravvenzione ovvero pur potendosi rappresentare tale provenienza illecita, in ragione della presenza di anomalie associate alla posizione del cliente (potenziale o effettivo) ovvero al debitore ceduto (e.g. la controparte utilizza documenti identificativi che appaiano contraffatti, fornisce informazioni manifestamente inesatte, incomplete ovvero mendaci, è residente o ha sede in aree geografiche ad alto rischio, palesa una struttura operativo-organizzativa qualificabile come veicolo di interposizione patrimoniale, si tratta di cliente in difficoltà economica che effettua operazioni di rilevante ammontare senza fornire valide giustificazioni sull'origine dei fondi). Lo stesso disvalore potrebbe, altresì, acquisire la condotta di un esponente di Generalfinance che emetta ordini, sottoscriva contratti di acquisto ovvero attesti l'avvenuta ricezione di approvvigionamenti di beni, servizi o prestazioni professionali, in tutto o in parte, fittizi ovvero che prevedano condizioni economiche non allineate a quelle di mercato, al fine di trasferire, sostituire o occultare denaro di provenienza illecita, così da dissimularne l'origine. Parimenti la figura delittuosa in commento potrebbe ricorrere qualora la Società eroghi rimborsi a fronte di note spese prive di riscontro fattuale o inesistenti, sempre allo scopo di trasferire, sostituire o occultare denaro di provenienza illecita. Nell'ambito della gestione dei flussi finanziari e della cassa/tesoreria, il delitto potrebbe, invece, concretizzarsi in una delle seguenti condotte (meramente esemplificative): i) trasferimento di disponibilità finanziarie di provenienza illecita, affluite su conti transitori, in modo tale da ostacolare l'identificazione di tale provenienza delittuosa; ii) gestione anomala della cassa (e.g. attraverso l'infedele registrazione di pagamenti o di incassi ovvero la registrazione degli stessi in difetto di documentazione giustificatrice) o dei conti correnti societari (e.g. mercè l'apertura e l'immediata chiusura degli stessi in un arco temporale circoscritto), finalizzata a ostacolare l'identificazione della provenienza illecita delle disponibilità finanziarie destinate alla Società.

- **Impiego di denaro, beni o utilità di provenienza illecita (Art. 648-ter codice penale)**

Il reato in esame si configura in capo a chiunque, al di fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis del c.p., impegna in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto (sia doloso che colposo) ovvero da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi. La fattispecie in oggetto, pur configurando un reato a forma libera al pari del reato di riciclaggio, richiede che la condotta del reimpiego sia caratterizzata da un tipico effetto dissimulatorio risultando diretta in ogni caso ad ostacolare l'accertamento sull'origine delittuosa di denaro, beni od altre utilità. Qualora le condotte incriminate abbiano ad oggetto denaro o cose provenienti da una contravvenzione, il trattamento sanzionatorio subisce una mitigazione, così come previsto dal comma 2 (di recente conio). Del pari, costituisce una circostanza attenuante l'ipotesi di particolare tenuità contemplata dall'art. 648, comma 4, c.p. Di contro, la pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale, mentre subisce una diminuzione nell'ipotesi prevista dall'art. 648, comma 4, c.p. (ipotesi di particolare tenuità).

Il delitto in commento è perseguibile anche se l'autore del reato presupposto da cui il denaro o le cose provengono non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale reato

Premesso che presupposto comune a tutte e tre le fattispecie previste dagli articoli 648, 648–bis e 648–ter del c.p. è quello costituito dalla provenienza da delitto o contravvenzione del denaro e dell'altra utilità di cui l'agente è venuto a disporre, le suddette fattispecie si distinguono, sotto il profilo soggettivo, per il fatto che la prima di esse richiede, oltre alla consapevolezza della suindicata provenienza, necessaria anche per le altre, solo una generica finalità di profitto, mentre la seconda e la terza richiedono la specifica finalità di far perdere le tracce dell'origine illecita, con l'ulteriore peculiarità, quanto alla terza, che detta finalità deve essere perseguita mediante l'impiego delle risorse in attività economiche finanziarie. Pertanto, l'art. 648–ter c.p. è quindi in rapporto di specialità con l'art. 648–bis c.p. il quale a sua volta, lo è con l'art. 648 c.p.

A titolo meramente esemplificativo, si segnala che uno dei Destinatari del Modello potrebbe impiegare disponibilità finanziarie provenienti da delitto (doloso o colposo) ovvero da contravvenzione effettuando operazioni fittizie di acquisto con il medesimo fornitore, reiterate in un ristretto arco temporale e anche per modico importo, con l'effetto di eludere la identificazione della provenienza illecita dei fondi. Ancora, il reato potrebbe ritenersi integrato laddove l'esponente della Società, pur essendo consapevole o essendosi rappresentato la concreta possibilità, accettandone il rischio, di aver ricevuto denaro, beni o utilità provenienti da delitto, li impieghi per compravendere strumenti finanziari nell'interesse dell'ente.

- **Auto-riciclaggio (Art. 648–ter1 codice penale)**

Il 3° comma dell'art. 3, Legge n. 186 del 15 dicembre 2014 ha introdotto nell'ordinamento penale italiano il delitto di auto-riciclaggio. Soggetto attivo del reato sono l'autore del delitto presupposto e i concorrenti del medesimo. Si tratta, pertanto, di un reato proprio. La condotta tipica consiste nell'impiegare, sostituire, trasferire, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione del reato presupposto: delitto (sia dolo che colposo) o contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi; nel caso in cui il c.d. *predicate crime* sia costituito da un reato contravvenzionale, il trattamento sanzionatorio risulta mitigato, così come previsto dall'inedito comma 2.

Due elementi contribuiscono alla delimitazione dell'area di rilevanza penale del fatto:

- 1) le condotte devono essere idonee ad ostacolare concretamente l'identificazione della provenienza criminosa del loro oggetto;
- 2) i beni devono essere tassativamente destinati ad attività economiche, finanziarie, imprenditoriali o speculative. Al riguardo, merita segnalare che nella nozione di "altra utilità" ben vi può rientrare il mero risparmio d'imposta discendente da un illecito tributario (cfr. Cass. Pen., Sez. II, 21/03/2017, n. 18308).

Ai sensi del 5° comma dell'art. 648–ter1 non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale. L'oggetto materiale del reato è costituito da denaro, beni o altre utilità provenienti da delitto(doloso o colposo) ovvero da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi.

Le pene previste per il delitto di auto-riciclaggio variano in ragione della gravità del delitto presupposto.



Costituisce una circostanza aggravante a effetto comune l'aver commesso il fatto nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale (6° comma); integra invece una circostanza attenuante ad effetto speciale (diminuzione della pena fino alla metà) l'essersi efficacemente adoperato per evitare che le condotte fossero portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto (7° comma).

L'autoriciclaggio è perseguibile anche laddove il reato presupposto da cui il denaro o le cose provengono non sia punibile ovvero difetti una condizione di procedibilità riferita al predetto reato.

A mero titolo esemplificativo il reato potrebbe inverarsi nell'ipotesi in cui un esponente della Società, dopo aver realizzato un illecito fiscale (e.g. l'indicazione di elementi passivi fittizi nella dichiarazione dei redditi o I.V.A. previa registrazione in contabilità di fattura per operazione, in tutto o in parte, inesistenti) ovvero dopo aver colposamente omesso di adottare le necessarie cautele contro gli infortuni sul lavoro (e.g. dispositivi di protezione individuale), impieghi il denaro così "risparmiato" per effettuare acquisti di beni/servizi o investimenti nell'interesse della Società ovvero lo trasferisca ad un soggetto terzo nella prospettiva di un mutuo vantaggio. Ancora, potrebbe rilevare in tale contesto il compimento di operazioni straordinarie in modo tale da ostacolare la ricostruzione dell'operazione sottostante simulata, con l'obiettivo di reinvestire proventi propri derivanti da reato.

## 1.2 ATTIVITÀ SENSIBILI

In relazione alle fattispecie di reati sopra descritte, i Processi Sensibili individuati nell'ambito delle attività di Generalfinance sono i seguenti:

1. gestione dei flussi finanziari in entrata ed in uscita;
2. attività commerciali e di procacciamento della clientela;
3. attività di istruttoria relativa al cliente per affidamento;
4. programmazione, decisione ed esecuzione di investimenti (anche in canali diversi dal ciclo attivo) e reinvestimenti (e.g. investimento e reinvestimento temporaneo delle liquidità in valori mobiliari, partecipazioni e altri strumenti finanziari), di disinvestimenti, operazioni sul capitale sociale e/o straordinarie, avuto riguardo anche ai rapporti *intercompany*;
5. gestione della cassa, della tesoreria e dei conti correnti societari, nonché esercizio dei poteri di firma per le disposizioni di pagamento (versamento, assegni, etc);
6. contratti di acquisto e/o di vendita dei prodotti da ufficio;
7. gestione delle fasi e sottofasi del ciclo passivo e degli acquisiti, ivi inclusi, a titolo esemplificativo, la gestione del processo di selezione dei fornitori, la valutazione degli acquisti di beni e servizi e l'autorizzazione dei pagamenti;
8. gestione e fruizione dei rimborsi spese tramite sistema informatico;
9. utilizzo delle carte di credito aziendali, nonché delle carte carburante per l'utilizzo dell'autovettura;
10. gestione delle liberalità, sponsorizzazioni e omaggi;

- 11.gestione e monitoraggio della tenuta della contabilità generale, nonché predisposizione e formazione del bilancio;
- 12.predisposizione e stesura del budget;
- 13.gestione delle consulenze e del conferimento degli incarichi professionali, disposizione ed esecuzione dei relativi pagamenti;
- 14.gestione della fiscalità aziendale e degli adempimenti fiscali.

### 1.3    **PROTOCOLLI PER MITIGARE IL RISCHIO**

Tutte le attività a rischio sono svolte conformandosi alle leggi vigenti e seguendo i principi, le procedure ed i protocolli aziendali - generici e specifici - di cui al presente Modello.

- **Protocolli Generici**

In linea con quanto sopra riportato, Generalfinance ha adottato, debitamente formalizzato e divulgato al proprio interno i seguenti Protocolli Generici, soggetti a periodico aggiornamento:

- Sistema di deleghe e procure con relativi limiti di spesa;
- Principi di comportamento descritti nel Codice Etico, con particolare riguardo a quelli dettati dall'art. 10, laddove prescrive l'obbligo per i Destinatari di impegnarsi a contrastare, nell'ambito dei diversi rapporti instaurati con la Società, vicende connesse al riciclaggio di denaro proveniente da attività criminali o alla ricettazione di beni o altre utilità di provenienza illecita;
- Organigramma aziendale e ordinamento organizzativo;
- Sistema sanzionatorio e disciplinare;
- Formazione del personale;
- Procedura *Whistleblowing*.

Inoltre, per la medesima finalità, rilevano i seguenti presidi:

- Controllo svolto dal Collegio Sindacale;
- Controllo svolto dalla Società di Revisione;
- Controllo della Funzione di *Compliance*;
- Controllo della Funzione di *Internal Audit*;
- Controllo della Funzione di *Risk Management*;
- Controllo della Funzione Antiriciclaggio;
- Supporto del Comitato Controllo, Rischi e Sostenibilità al Consiglio di Amministrazione nelle valutazioni e decisioni relative al sistema di controlli interni e di gestione dei rischi e all'approvazione delle relazioni periodiche di carattere finanziario e non finanziario, nonché nella promozione della continua integrazione delle *best practice* nazionali e internazionali nella *corporate governance* della Società e dei fattori ambientali, sociali e di *governance* nelle strategie aziendali volte al perseguimento del successo sostenibile.

- **Protocolli Specifici**

I Protocolli Specifici si basano sui seguenti principi generali di controllo:

- 1)    Separazione dei compiti: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;

- 2) Esistenza di procedure formalizzate: devono esistere disposizioni aziendali e/o procedure formalizzate, idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- 3) Esistenza di un sistema di deleghe e procure coerente con le responsabilità organizzative assegnate: nell'ambito delle disposizioni aziendali e/o procedure formalizzate, i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere definiti e conosciuti all'interno della Società;
- 4) Tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informatici: ogni operazione relativa all'area a rischio 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.

Oltre ai Protocolli Generici, la Società ha sviluppato e implementato i seguenti Protocolli Specifici per la riduzione del rischio di realizzazione dei Reati sopra citati:

- **Policy e Manuale Antiriciclaggio e Contrasto al finanziamento del terrorismo**: obiettivo di questi due documenti è descrivere e definire i presidi adottati dalla Società in termini di organizzazione, procedure e controlli per il contrasto al riciclaggio e al finanziamento del terrorismo nonché gli assetti organizzativi posti in essere in materia di governo, organizzazione e controllo dei medesimi. Essi, quindi, definiscono e formalizzano i ruoli e le responsabilità dei soggetti coinvolti in tali Processi Sensibili definendo, a titolo esemplificativo e non esaustivo:
  - a. le modalità di esecuzione degli obblighi di adeguata verifica della clientela;
  - b. la procedura di valutazione per ciascun cliente del rischio di riciclaggio e i criteri per la relativa assegnazione del profilo di rischio;
  - c. l'attività di controllo costante nel corso del rapporto e le verifiche da porre in essere nei riguardi della clientela;
  - d. le attività di registrazione e conservazione dei dati e delle informazioni acquisiti nel corso dell'assolvimento degli obblighi di adeguata verifica;
  - e. la procedura di segnalazione delle operazioni sospette;
  - f. la formazione del personale.

Generalfinance ha, inoltre, provveduto all'adozione di un sistema organizzativo idoneo ad assicurare l'efficace prevenzione e gestione del rischio di riciclaggio.

### **La Funzione Antiriciclaggio**

In adempimento di quanto previsto nel provvedimento della Banca d'Italia *"Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo"*, emanato in data 26 marzo 2019 e in ossequio al principio di proporzionalità, il Consiglio di Amministrazione, in data 2 agosto 2011, ha deliberato l'istituzione della Funzione Antiriciclaggio, la cui responsabilità è ora attribuita al Responsabile dell'ufficio denominato *"AML e Compliance"*. Al medesimo soggetto è stata attribuita la delega per le segnalazioni di operazioni sospette.



La Società si è dotata di un sistema organizzativo e di controllo nonché di strategie, regole, risorse, procedure e funzioni chiaramente individuate e adeguatamente specializzate idonee ad assicurare l'efficace prevenzione del rischio di riciclaggio.

In particolare, la Funzione Antiriciclaggio si occupa di verificare nel continuo che le procedure aziendali siano coerenti con l'obiettivo di prevenire e contrastare la violazione di norme antiriciclaggio e, a tal fine, provvede a:

- identificare le norme applicabili e valutare il loro impatto sui processi e le procedure interne;
- collaborare alla definizione del sistema dei controlli interni e delle procedure finalizzati alla prevenzione e al contrasto dei rischi in rilievo;
- verificare nel continuo l'adeguatezza del processo di gestione dei rischi di riciclaggio, l'idoneità del sistema dei controlli interni e delle procedure adottati e proporre le modifiche organizzative e procedurali necessarie o opportune al fine di assicurare un adeguato presidio dei rischi;
- condurre verifiche sulla funzionalità del processo di segnalazione e sulla congruità delle valutazioni effettuate dal primo livello sull'operatività della clientela, nonché verificare l'affidabilità del sistema informativo di alimentazione dell'Archivio Unico informatico aziendale;
- collaborare alla definizione delle politiche di governo del rischio di riciclaggio e delle varie fasi in cui si articola il processo di gestione di tale rischio;
- condurre, in raccordo con le altre funzioni aziendali interessate, l'esercizio annuale di autovalutazione dei rischi di riciclaggio cui è esposta la Società;
- prestare supporto e assistenza agli organi aziendali e all'alta direzione;
- valutare in via preventiva il rischio riciclaggio connesso all'offerta di prodotti e servizi nuovi;
- verificare l'affidabilità dei sistemi e delle procedure interne adottate dalla Società in materia di obblighi di adeguata verifica della clientela e di registrazione, conservazione dei dati, nonché dei sistemi di individuazione, valutazione e segnalazione delle operazioni sospette, ponendo particolare attenzione, altresì, all'efficace rilevazione delle altre situazioni oggetto di obbligo di comunicazione, nonché all'appropriata archiviazione della documentazione e delle evidenze richieste dalla normativa. Nella valutazione dell'adeguatezza di tali procedure, la funzione può effettuare controlli su base campionaria per verificarne l'efficacia e la funzionalità ed individuare, ove necessario, aree di criticità insieme con i piani di rimedio;
- trasmettere mensilmente alla UIF i dati aggregati concernenti le registrazioni nell'Archivio Unico Informatico;
- ;
- curare, in raccordo con le altre funzioni aziendali competenti in materia di formazione, la predisposizione di un adeguato piano di formazione, finalizzato a conseguire un aggiornamento su base continuativa del personale dipendente e dei collaboratori;
- predisporre e trasmettere all'organo con funzione di gestione e a quello con funzione di supervisione strategica un documento (il Manuale Antiriciclaggio) che definisce responsabilità, compiti e modalità operative nella gestione del rischio di riciclaggio, e si assicura che sia reso disponibile e facilmente accessibile da tutto il personale;

- presentare, almeno una volta l'anno, agli organi di supervisione strategica, gestione e controllo una relazione sulle iniziative intraprese, sulle disfunzioni accertate e sulle relative azioni correttive attuate e/o da intraprendere nonché sull'attività formativa del personale;
  - informare tempestivamente gli organi aziendali di violazioni o carenze rilevanti riscontrate nell'esercizio dei relativi compiti;
  - predisporre flussi informativi diretti agli organi aziendali e all'alta direzione;
  - in qualità di presidio aziendale specialistico antiriciclaggio, collaborare con le Autorità di cui al Titolo I, Capo II del D.Lgs. n. 231/2007;
  - svolgere le attività di rafforzata verifica della clientela nei casi in cui, per circostanze oggettive, ambientali e/o soggettive, appaia particolarmente elevato il rischio di riciclaggio e verificare l'adeguatezza del processo di rafforzata verifica condotto dalle strutture di linea;
  - in considerazione della delega conferita ai sensi dell'art. 42, comma 4, del D.Lgs. n. 231/2007, valutare le segnalazioni di operazioni sospette pervenute e trasmettere tempestivamente alla UIF quelle ritenute fondate.
- 
- **Disposizioni operative circa il rinnovo dell'adeguata verifica nei confronti di clienti il cui fido è posto in stato "revocato"** che forniscono le regole che gli addetti agli adempimenti attinenti all'obbligo di adeguata verifica della clientela devono seguire nel caso in cui il fido accordato ad un cedente (nell'ambito di un rapporto continuativo di *factoring*) venga revocato.
  - **Protocollo gestione delle liberalità, donazioni, sponsorizzazioni e omaggi:** il cui obiettivo è la definizione di regole di condotta e procedurali che indichino i comportamenti cui i Destinatari devono attenersi nell'ambito del processo di gestione delle liberalità (intendendosi con esse le donazioni, le sponsorizzazioni e gli omaggi) affinché siano prevenuti comportamenti idonei a realizzare i Reati Presupposto.
  - **Procedura di approvvigionamento di beni, servizi, consulenze ed incarichi professionali:** volta a definire le regole di condotta e operative che indicano i comportamenti cui i Destinatari devono attenersi nella gestione del processo di approvvigionamento affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.
  - **Procedura rimborsi spese (gestione trasferte e note spese):** finalizzata a definire le regole di condotta e operative che i dipendenti/collaboratori della Società devono porre in essere per poter richiedere (e ottenere) un rimborso spese, affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.
  - **Procedura per la gestione dei flussi finanziari (Regolamento tracciabilità flussi finanziari):** il cui scopo è formalizzare e definire le scelte operative e i processi interni preordinati al rispetto delle norme in materia di tracciabilità dei flussi finanziari, con riferimento al pagamento di crediti che abbiano formato oggetto di cessione a favore di Generalfinance.
  - **Procedura gestione della contabilità redazione del bilancio fiscale (Policy redazione bilancio di esercizio) e Regolamento in materia di pianificazione e controllo di gestione:** obiettivo della procedura e del regolamento è la definizione di regole di condotta e procedurali che indichino i comportamenti cui i Destinatari devono attenersi nella gestione dei processi legati alla tenuta della contabilità, alla redazione del bilancio nonché di tutte quelle attività connesse alla pianificazione strategica, alla predisposizione del budget e al controllo di gestione affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.

- **Procedura gestione della tesoreria:** obiettivo della procedura è la definizione di regole di condotta e procedurali che indichino i comportamenti cui i Destinatari devono attenersi nell'ambito dei processi connessi all'amministrazione della tesoreria aziendale e, in particolare, degli investimenti e disinvestimenti; degli affidamenti bancari e approvvigionamenti; della gestione della liquidità nonché della gestione amministrativa di incassi e pagamenti affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.
- **Clausole Contrattuali 231:** il Protocollo ha l'obiettivo di disciplinare le attività di redazione dei contratti con le terze parti, allo scopo di evitare che, nella prestazione dei servizi contrattualizzati, possano essere commessi i Reati di cui al Decreto.

#### **1.4 CONTROLLI DELL'ORGANISMO DI VIGILANZA**

L'Organismo di Vigilanza esegue verifiche periodiche con riguardo alle specifiche attività sensibili di cui alla presente Parte Speciale secondo le seguenti modalità: (i) attenendosi alla programmazione da esso prevista nel piano di attività elaborato per ciascun anno di riferimento ovvero (ii) a campione, qualora la verifica non sia ricompresa all'interno del piano annuale di attività, ma l'OdV la ritenga comunque necessaria.

#### **1.5 FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA**

La funzione aziendale nella cui competenza ricade la gestione dell'Attività Sensibile dà apposita evidenza documentale di ogni attività a rischio, secondo quanto previsto dalla specifica procedura operativa applicabile, ovvero di eventuali criticità insorte (e.g. accertamenti e/o richieste da parte della Guardia di Finanza, dell'Agenzia delle Entrate, dell'Autorità Giudiziaria o dell'Autorità di Vigilanza). A seconda dell'attività, la funzione competente dovrà effettuare i controlli definiti nella procedura e, in caso di anomalia, inviare all'Organismo di Vigilanza le opportune segnalazioni e i flussi informativi richiesti.



## **PARTE SPECIALE IV**

*Delitti contro la personalità individuale (art. 25-quinquies)*

## 1.1 I REATI RICHIAMATI DAL DECRETO E LE RELATIVE MODALITÀ DI COMMISSIONE

- **Reati contro la personalità individuale**

Gli illeciti penali ricompresi nella categoria dei reati contro la personalità individuale si possono raggruppare in due distinte tipologie, di seguito indicate:

- 1) reati a tutela della libertà individuale (artt. 600, 601 e 602 e 603-*bis* c.p.);
- 2) reati a tutela della sfera sessuale dei minori (artt. 600-*bis*, 600-*ter*, 600-*quater*, 600-*quinquies* c.p.).

I reati in esame sono puniti anche se commessi all'estero da un cittadino italiano, ovvero in danno di un cittadino italiano ovvero da un cittadino italiano in concorso con un cittadino straniero.

- **Reati a tutela della libertà individuale**

I reati previsti dagli artt. 600, 601 e 602 c.p. sanzionano le c.d. nuove forme di schiavitù, consistenti in comportamenti che realizzano:

- la riduzione o mantenimento in schiavitù, in servitù o in stato di soggezione continuativa<sup>1</sup> di taluno, in modo da costringerlo a prestazioni lavorative, sessuali, all'accattonaggio o, comunque, a prestazioni che ne comportino lo sfruttamento (art. 600 c.p.);
- la tratta di persone che si trovino nelle condizioni di schiavitù, servitù o in stato di soggezione o l'induzione di taluno a fare ingresso, soggiornare o uscire dal territorio dello Stato mediante violenza o minaccia, abuso di autorità o approfittamento di una situazione di inferiorità psichica o fisica o dello stato di necessità in cui il soggetto versa ovvero a seguito dell'offerta di vantaggi su chi abbia su di esso autorità (art. 601 c.p.).

Con riferimento a tale categoria di Reati si è evidenziata la difficoltà di individuare il rischio della loro commissione nell'interesse o a vantaggio della Società.

Pertanto, nell'ipotesi specifica di Generalfinance, le predette fattispecie potrebbero essere integrate, a titolo di concorso nel reato, con il consapevole affidamento di contratti di servizi o forniture a soggetti o imprese che utilizzino manodopera con modalità tali da integrare i reati riduzione o mantenimento in schiavitù, tratta di persone o acquisto e alienazione di schiavi. In tal caso l'interesse della Società potrebbe essere ravvisato nelle più vantaggiose condizioni economiche praticate da tali imprese rispetto alle imprese concorrenti.

- **Reati a tutela della sfera sessuale dei minori**

I reati previsti dagli artt. 600 *bis* - 600 *quinquies* c.p. sanzionano le forme di abuso sessuale poste in essere in danno di minori ovvero, comunque, tramite lo sfruttamento dei minori a scopo sessuale.

In particolare, si punisce:

- la prostituzione minorile, ossia l'induzione, il favoreggiamento o lo sfruttamento della prostituzione di una persona di età inferiore ai 18 anni nonché il compimento di atti sessuali con un minore di età

---

<sup>1</sup> La riduzione o il mantenimento nello stato di soggezione ha luogo quando la condotta è attuata mediante, violenza, minaccia, inganno abuso di autorità o approfittamento di una situazione fisica o psichica o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha l'autorità sulla persona.

- compresa tra i 14 e i 18 anni, in cambio di denaro o altra utilità economica (art. 600 *bis* c.p.);
- la pornografia minorile, ossia lo sfruttamento di minori di anni 18 per realizzare esibizioni pornografiche o produrre materiale pornografico, fare commercio di materiale pornografico, nonché la cessione, anche a titolo gratuito, di tale materiale. Si punisce altresì chi, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga o pubblicizza materiale pornografico relativo a minori ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori di anni 18 (art. 600-*ter* c.p.);
  - la detenzione di materiale pornografico ossia il procurarsi o semplicemente il disporre (consapevole) dell'indicato materiale pornografico (art. 600-*quater* c.p.);
  - la pornografia virtuale. Le disposizioni di cui agli artt. 600-*ter* c.p. e 600-*quater* c.p. si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni 18 o parti di esse, ma la pena è diminuita di un terzo (art. 600-*quater*1 c.p.);
  - le iniziative turistiche volte allo sfruttamento della prostituzione minorile, attinenti, in particolare, alla organizzazione o propaganda di viaggi finalizzati alla fruizione di attività di prostituzione a danno di minori (art. 600-*quinquies*).

Più in generale, si potrebbe ravvisare per tutte le imprese, indipendentemente dall'attività esercitata, un interesse delle stesse ad organizzare viaggi aziendali in località estere note per il fenomeno del c.d. "turismo sessuale" al fine di motivare/gratificare i dipendenti e trarne così, indirettamente, un vantaggio, ovvero una commissione del reato a titolo di concorso mediante l'utilizzo per l'approvvigionamento interno di agenzie di viaggi di cui è nota l'attività di organizzazione di viaggi in località estere note per il fenomeno del c.d. "turismo sessuale", in quanto operino prezzi inferiori ai concorrenti.

- **Reato di Caporalato**

La Legge 29 ottobre 2016, n. 199, che reca disposizioni in materia di contrasto ai fenomeni del lavoro nero, dello sfruttamento del lavoro in agricoltura e di riallineamento retributivo nel settore agricolo, ha previsto, fra l'altro:

- a) la modifica dell'articolo 603-*bis* c.p. in materia di intermediazione illecita e sfruttamento del lavoro (cd. caporalato) e
- b) l'introduzione del reato di caporalato nel novero dei reati presupposto del Decreto attraverso la modifica dell'articolo 25-*quinquies* comma 1, lettera a).

La legge n. 199 del 2016 ha riformulato la disposizione tentando di semplificare la struttura del reato ed ampliando il novero dei soggetti attivi del reato non solo a chi svolge l'attività di illecita intermediazione (il caporale), ma anche a chi (in particolare, il datore di lavoro) si avvalga di manodopera sottoponendola a condizioni di sfruttamento ed approfittando del suo stato di bisogno.

Il vigente primo comma dell'articolo 603-*bis* c.p. individua due distinte fattispecie: 1) il reclutamento di manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento e 2) l'utilizzo, l'assunzione o l'impiego di manodopera, con sottoposizione dei lavoratori a condizioni di sfruttamento.

In entrambi i casi, la condotta deve essere realizzata approfittando dello stato di bisogno del lavoratore. Non è, invece, più richiesta la sussistenza di un'attività organizzata, con conseguente rilevanza penale anche di condotte poste in essere da un singolo o comunque da soggetti privi di stabile organizzazione di mezzi e di persone, ed è stato altresì eliminato il riferimento alla violenza, alla minaccia o

all'intimidazione, quali necessarie modalità di realizzazione dello sfruttamento del lavoratore. La violenza e la minaccia sono ora considerate nella circostanza aggravante prevista al 2° comma.

Il 3° comma della norma individua quattro situazioni che, per espressa valutazione legislativa, costituiscono indice di sfruttamento del lavoratore. Esse concernono:

- a) il rapporto tra la qualità e quantità del lavoro prestato e la retribuzione (*“la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato”*);
- b) le condizioni contrattuali (*“la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie”*);
- c) la sicurezza nei luoghi di lavoro (*“la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro”*);
- d) le condizioni di lavoro e di vita del lavoratore (*“la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti”*).

## 1.2 ATTIVITÀ SENSIBILI

È importante sottolineare, ai fini della corretta individuazione dei profili di rischio connessi ai Reati in esame, che solo in ipotesi estreme e assolutamente peculiari l'Ente può essere considerato esso stesso una vera e propria associazione finalizzata alla commissione di una pluralità di delitti, ipotesi cui consegue - a norma dell'art. 14, co. 4 - l'interdizione definitiva dall'attività. Al riguardo, la Relazione al Decreto e l'art. 10, co. 4, della L. 146/2006 forniscono importanti elementi interpretativi: tale identificazione, infatti, è possibile soltanto nell'ipotesi in cui *“l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati”*.

Per tale ragione, si ritiene che, al di là di tale ipotesi estrema, maggiori profili di rischio connessi all'operatività societaria insistono nello svolgimento di attività che comportino contatti con soggetti esterni che facciano parte di associazioni a delinquere già esistenti, cui gli esponenti aziendali potrebbero fornire consapevole supporto, in vista del perseguimento anche di presunti interessi sociali.

Si richiama l'attenzione degli esponenti aziendali sui casi in cui la Società opera in associazione con *partner*; ovvero si avvale dell'assistenza di consulenti o rappresentanti esterni.

In ragione di ciò, i Processi Sensibili sono individuati come segue:

1. selezione, assunzione e gestione del personale;
2. gestione e affidamento di incarichi professionali;
3. gestione dei rapporti commerciali e contrattuali con la clientela di Generalfinance e con soggetti terzi privati;
4. gestione del ciclo passivo (selezione e gestione dei fornitori).

## 1.3 PROTOCOLLI PER MITIGARE IL RISCHIO

Tutte le attività a rischio sono svolte conformandosi alle leggi vigenti e seguendo i principi, le procedure ed i Protocolli aziendali, Generici e Specifici, di cui al presente Modello.

- **Protocolli Generici**



In linea con quanto sopra riportato, la Società ha adottato ed ha debitamente formalizzato e divulgato al proprio interno i seguenti Protocolli Generici, soggetti a periodico aggiornamento:

- Sistema di deleghe e procure con relativi limiti di spesa;
- Principi di comportamento descritti nel Codice Etico;
- Organigramma aziendale e ordinamento organizzativo;
- Sistema sanzionatorio e disciplinare;
- Formazione del Personale;
- Procedura *Whistleblowing*.

Inoltre, per la medesima finalità, rilevano i seguenti presidi:

- Controllo svolto dalla Società di Revisione;
- Controllo svolto dal Collegio Sindacale;
- Controllo della Funzione di *Compliance*;
- Controllo della Funzione di *Internal Audit*;
- Supporto del Comitato Controllo, Rischi e Sostenibilità al Consiglio di Amministrazione nelle valutazioni e decisioni relative al sistema di controlli interni e di gestione dei rischi e all'approvazione delle relazioni periodiche di carattere finanziario e non finanziario, nonché nella promozione della continua integrazione delle *best practice* nazionali e internazionali nella *corporate governance* della Società e dei fattori ambientali, sociali e di *governance* nelle strategie aziendali volte al perseguimento del successo sostenibile.

- **Protocolli Specifici**

I Protocolli Specifici di Generalfinance si basano sui seguenti principi generali di controllo:

- 1) separazione dei compiti: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- 2) esistenza di procedure formalizzate: devono esistere disposizioni aziendali e/o procedure formalizzate, idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- 3) esistenza di un sistema di deleghe e procure coerente con le responsabilità organizzative assegnate: nell'ambito delle disposizioni aziendali e/o procedure formalizzate, i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere definiti e conosciuti all'interno della società;
- 4) tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informatici: ogni operazione relativa all'area a rischio 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.

Oltre ai protocolli di carattere generale, la Società ha sviluppato e implementato i seguenti Protocolli Specifici per la riduzione del rischio di commissione dei citati Reati:

- **Clausole contrattuali 231**: il protocollo ha l'obiettivo di disciplinare le attività di redazione dei contratti con le terze parti, allo scopo di evitare che, nella prestazione dei servizi

contrattualizzati, possano essere commessi i Reati di cui al Decreto.

- **Procedura di approvvigionamento di beni, servizi, consulenze ed incarichi professionali**, la quale definisce le regole di condotta e procedurali che indicano i comportamenti cui la Società si attiene nella gestione del processo di approvvigionamento affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.
- **Procedura di selezione, assunzione e gestione del personale**: che definisce i comportamenti cui la Società si attiene nello svolgimento delle attività, nonché dei processi ad esse connessi, di selezione, assunzione e gestione delle risorse umane affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.

#### 1.4 CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza esegue verifiche periodiche con riguardo alle specifiche attività sensibili di cui alla presente Parte Speciale, secondo le seguenti modalità: (i) attenendosi alla programmazione da esso prevista nel piano di attività elaborato per ciascun anno di riferimento ovvero (ii) a campione, qualora la verifica non sia ricompresa all'interno del piano annuale di attività, ma l'OdV la ritenga comunque necessaria.

L'Organismo di Vigilanza può, tra l'altro, esaminare a campione:

- i contratti formalizzati con fornitori e/o collaboratori esteri,
- i *report* attinenti al procedimento di selezione dei fornitori e/o collaboratori esteri nonché quelli relativi ai rapporti intrattenuti con i medesimi;
- la documentazione relativa alla selezione del personale della Società, (anche) al fine di verificare che siano poste in essere, dalle funzioni di volta in volta competenti, quelle attività finalizzate a prevenire il compimento dei reati oggetto della presente Parte Speciale.

#### 1.5 FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

La funzione aziendale nella cui competenza ricade la gestione dell'Attività Sensibile dà apposita evidenza documentale di ogni attività a rischio, secondo quanto previsto dalla specifica procedura operativa applicabile. A seconda dell'attività, la funzione competente dovrà effettuare i controlli definiti nella procedura e, in caso di anomalia, inviare all'Organismo di Vigilanza le opportune segnalazioni e i flussi informativi richiesti.



## **PARTE SPECIALE V**

*Omicidio colposo – Lesioni colpose gravi o gravissime, commessi con violazione delle norme in materia di salute e sicurezza sul lavoro (Art. 25 - septies)*

## 1.1 PREMESSA

La presente Parte Speciale si riferisce ai reati che si verificano a seguito della violazione delle norme per la prevenzione degli infortuni sul lavoro o relativi all'igiene ed alla salute e sicurezza sul lavoro, richiamati nell'art. 25-*septies* del Decreto, come modificato dall'articolo 300 del D.Lgs. 81/2008.

L'art. 9 della Legge n. 123/2007 ha introdotto nel Decreto l'art. 25-*septies* che estende la responsabilità amministrativa degli enti ai reati di omicidio colposo e lesioni personali colpose, gravi o gravissime, commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro. L'articolo 300 del D.Lgs. 81/2008 ha, successivamente, sostituito il predetto art. 25-*septies*.

Con il citato intervento normativo per la prima volta viene prevista la responsabilità degli enti per reati di natura colposa. Tale circostanza impone un coordinamento con l'art. 5 del Decreto, che definisce il criterio oggettivo di imputazione della responsabilità dell'ente, subordinandola all'esistenza di un interesse o vantaggio per l'ente.

Il criterio dell'"*interesse*" sembra, infatti, essere incompatibile con i reati di natura colposa, proprio perché non è configurabile rispetto a essi una finalizzazione soggettiva dell'azione.

Nelle ipotesi di commissione dei reati contemplati dall'art. 25-*septies* del Decreto, la responsabilità prevista dal Decreto è configurabile solo se dal fatto illecito ne sia derivato un vantaggio per l'ente, che, nel caso di specie, potrebbe essere rinvenuto in un risparmio di costi o di tempi.

## 1.2 I REATI RICHIAMATI DAL DECRETO E LA RELATIVA MODALITÀ DI COMMISSIONE

- **Omicidio colposo (Art. 589 codice penale)**

Il reato si perfeziona allorquando si cagiona la morte di una persona per colpa.

Ai fini dell'integrazione del reato, non è richiesto l'elemento psicologico del dolo, ovvero la coscienza, volontà e rappresentazione della condotta omicidiaria (*animus occidendi*) ma la mera negligenza, imperizia, imprudenza del soggetto agente, ovvero l'inosservanza, da parte di quest'ultimo di leggi, regolamenti, ordini o discipline (art. 43 c.p.).

- **Lesioni personali colpose (Art. 590 codice penale)**

Il reato si configura nel caso in cui siano cagionate per colpa a una persona lesioni gravi o gravissime; il legislatore ha definito le lesioni come una malattia nel corpo o nella mente, differenziandole profondamente dalle semplici percosse.

Le lesioni si considerano gravi nel caso in cui (art. 583, comma 1, c.p.):

- dal fatto derivi una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore a quaranta giorni;
- il fatto produce l'indebolimento permanente di un senso o di un organo.

Le lesioni si considerano gravissime nel caso in cui (art. 583, comma 2, c.p.):

- dal fatto derivi una malattia certamente o probabilmente insanabile;
- la perdita di un senso;



- la perdita di un arto o una mutilazione che lo renda inservibile;
- la perdita dell'uso di un organo o della capacità di procreare;
- una permanente e grave difficoltà della favella;
- la deformazione, ovvero lo sfregio permanente del viso.

Anche ai fini della configurabilità del reato di lesioni colpose, non è necessario che il soggetto agente abbia agito con la coscienza e volontà di cagionare l'evento lesivo (*animus necandi*), essendo sufficiente la negligenza, l'imprudenza, l'imperizia dello stesso, ovvero l'inosservanza di norme, regolamenti, ordini o discipline.

Entrambi i reati sopra richiamati rilevano, ai fini del Decreto, unicamente nel caso in cui sia ascrivibile al soggetto agente, sotto il profilo dell'elemento soggettivo, la c.d. "colpa specifica", consistente nella violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene e alla salute e sicurezza sul lavoro.

Atteso che, in forza di tale circostanza, assume rilevanza la legislazione prevenzionistica vigente, ai fini della presente Parte Speciale si intende integralmente richiamato il D.Lgs. n. 81/2001 (c.d. Testo Unico della sicurezza, di seguito "Testo Unico") come da ultimo modificato dal D.Lgs. n. 106 del 3 agosto 2009 (e comunque come modificato tempo per tempo).

### 1.3 ATTIVITÀ SENSIBILI

Per quanto attiene l'individuazione e l'analisi dei rischi potenziali, la quale dovrebbe considerare le possibili modalità attuative dei reati in seno all'Ente, si rileva, con riguardo alle fattispecie previste dal D.Lgs. n. 81/2008, che l'analisi delle possibili modalità attuative coincide con la valutazione dei rischi lavorativi effettuata dalla Società sulla scorta della legislazione prevenzionistica vigente ed in particolare dagli artt. 28 e ss. del Testo Unico della Sicurezza, come modificati dal D.Lgs. n. 106 del 3 agosto 2009.

Con precipuo riferimento ai reati oggetto della presente Parte Speciale, si sottolinea che non è possibile escludere aprioristicamente alcun ambito di attività, poiché tali reati potrebbero interessare la totalità delle componenti aziendali. In altri termini, i reati oggetto della presente Parte Speciale potrebbero astrattamente essere commessi in tutti i casi in cui vi sia, in seno alla Società, una violazione degli obblighi e delle prescrizioni in materia di salute e sicurezza sul posto di lavoro.

### 1.4 I PROTOCOLLI PER MITIGARE IL RISCHIO

Tutte le attività a rischio sono svolte conformandosi alle leggi vigenti e seguendo i principi, le procedure e i Protocolli aziendali, Generici e Specifici, di cui al presente Modello.

- **Protocolli Generici**

In linea con quanto sopra riportato, la Società ha adottato ed ha debitamente formalizzato e divulgato al proprio interno i seguenti Protocolli Generici, soggetti a periodico aggiornamento:

- Sistema di deleghe e procure con relativi limiti di spesa;
- Principi di comportamento descritti nel Codice Etico;
- Organigramma aziendale e ordinamento organizzativo;
- Sistema sanzionatorio e disciplinare;
- Formazione del personale;
- Procedura Whistleblowing.

Inoltre, per la medesima finalità, rilevano i seguenti presidi:

- Controllo svolto dal Collegio Sindacale;
- Controllo svolto dalla Società di Revisione;
- Controllo della Funzione di *Compliance*;
- Controllo della Funzione di *Internal Audit*;
- Supporto del Comitato Controllo, Rischi e Sostenibilità al Consiglio di Amministrazione nelle valutazioni e decisioni relative al sistema di controlli interni e di gestione dei rischi e all'approvazione delle relazioni periodiche di carattere finanziario e non finanziario, nonché nella promozione della continua integrazione delle *best practice* nazionali e internazionali nella corporate *governance* della Società e dei fattori ambientali, sociali e di *governance* nelle strategie aziendali volte al perseguimento del successo sostenibile.

- **Protocolli Specifici**

I Protocolli Specifici di Generalfinance si basano sui seguenti principi generali di controllo:

- a) separazione dei compiti: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- b) esistenza di procedure formalizzate: devono esistere disposizioni aziendali e/o procedure formalizzate, idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- c) esistenza di un sistema di deleghe e procure coerente con le responsabilità organizzative assegnate: nell'ambito delle disposizioni aziendali e/o procedure formalizzate, i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere definiti e conosciuti all'interno della società;
- d) tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informatici: ogni operazione relativa all'area a rischio 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.

La Società, al fine di prevenire i reati di cui al presente documento, ha sviluppato e implementato, a titolo meramente esemplificativo e non esaustivo, i seguenti Protocolli Specifici per la riduzione del rischio di realizzazione dei reati poc'anzi analizzati:

- **Clausole contrattuali 231**: il protocollo ha l'obiettivo di disciplinare le attività di redazione dei contratti con le terze parti onde evitare che, nella prestazione dei servizi contrattualizzati, possano essere commessi i Reati di cui al Decreto;
- **Documento Valutazione dei Rischi ("DVR")**;
- **Gestione per la sicurezza e la salute nei luoghi di lavoro**: documento predisposto per la prevenzione dei reati in materia di sicurezza connessi con i delitti di omicidio colposo e lesioni personali colpose gravi e gravissime, che ha lo scopo di definire i principi di riferimento, le relative caratteristiche e le principali modalità operative per l'applicazione della normativa sulla salute e



sicurezza sui luoghi di lavoro dei dipendenti, dei contrattisti e dei clienti e la tutela dell'incolumità pubblica.

#### **1.5 CONTROLLI DELL'ORGANISMO DI VIGILANZA**

L'Organismo di Vigilanza esegue verifiche periodiche con riguardo alle specifiche attività sensibili di cui alla presente Parte Speciale secondo le seguenti modalità: (i) attenendosi alla programmazione da esso prevista nel piano di attività elaborato per ciascun anno di riferimento ovvero (ii) a campione, qualora la verifica non sia ricompresa all'interno del piano annuale di attività, ma l'OdV la ritenga comunque necessaria.

Nello svolgimento dei compiti che gli sono propri, l'Organismo può:

- partecipare agli incontri organizzati dalla Società tra le funzioni preposte alla sicurezza, valutando quali - tra essi - rivestano rilevanza per il corretto svolgimento dei propri compiti;
- accedere a tutta la documentazione e a tutti gli uffici della Società per lo svolgimento delle funzioni che gli sono proprie.

Esso, nell'espletamento delle attività di cui sopra, può avvalersi di tutte le risorse aziendali (a titolo esemplificativo, del Responsabile del Servizio di Prevenzione e Protezione, del Medico Competente, degli incaricati dell'attuazione delle misure di emergenza e primo soccorso).

Laddove l'Organismo di Vigilanza riscontri situazioni di non efficacia ovvero di non applicazione delle procedure adottate dalla Società, ne dà comunicazione al Consiglio di Amministrazione affinché svolga le opportune valutazioni e assuma le determinazioni di propria competenza. Qualora lo ritenga opportuno propone anche le azioni correttive ritenute più adeguate.

#### **1.6 FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA**

La funzione aziendale nella cui competenza ricade la gestione dell'Attività Sensibile dà apposita evidenza documentale di ogni attività a rischio, secondo quanto previsto dalla specifica procedura operativa applicabile. A seconda dell'attività, la funzione competente dovrà effettuare i controlli definiti nella procedura e, in caso di anomalia, inviare all'Organismo di Vigilanza le opportune segnalazioni e i flussi informativi richiesti.

L'Amministratore Delegato ovvero, se nominato, il soggetto destinatario delle deleghe in materia di salute e sicurezza sui luoghi di lavoro, con il coinvolgimento del RSPP, tiene informato l'Organismo di Vigilanza circa l'organizzazione dei presidi in materia di salute e sicurezza, di eventuali infortuni verificatisi e circa malattie professionali accertate o presunte.



## **PARTE SPECIALE VI**

*Delitti informatici e trattamento illecito dei dati (art. 24 bis)*

## 1.1 I REATI RICHIAMATI DAL DECRETO E LA RELATIVA MODALITÀ DI COMMISSIONE

- **Delitti informatici**

Appare opportuno premettere che il termine *“crimine informatico”* indica **qualsiasi reato o violazione del codice civile o penale per la realizzazione del quale il ricorso alla tecnologia informatica è stato un fattore determinante per il compimento dell’azione criminosa**. In realtà, è opportuno attuare una distinzione tra reati telematici *“veri e propri”*, ovvero fattispecie impossibili da porre in essere senza l’ausilio delle tecnologie informatiche, ed i crimini così detti *“tradizionali”* o *“convenzionali”*, in cui l’uso dello strumento informatico è solo un supporto *ad hoc* per il raggiungimento dello scopo.

I reati introdotti nell’ambito della disciplina sulla responsabilità amministrativa degli enti dalla L. n. 48/08, la maggior parte dei quali sono stati novellati dalla Legge n. 238/2021 (c.d. Legge Europea 2019-2020) attraverso l’inasprimento del trattamento sanzionatorio e l’ampliamento della fattispecie tipica oggettiva (in particolar modo, della condotta materiale e dell’oggetto del reato), sono i seguenti:

- **Falsità in un documento informatico pubblico o avente efficacia probatoria (Art. 491-bis codice penale)**

Se alcuna delle falsità previste dal capo III, Titolo VII<sup>1</sup>, del c.p. riguarda un documento informatico<sup>2</sup> pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A mero titolo esemplificativo, il reato potrebbe realizzarsi nel caso in cui un rappresentante della Società (e.g. il legale rappresentante o un suo delegato) compili telematicamente ovvero trasmetta alla Pubblica Amministrazione o ad altro Ente Pubblico (e.g. Autorità di Vigilanza, ivi inclusa l’UIF) un’attestazione mendace (e.g. le dichiarazioni attestanti requisiti finanziari, patrimoniali o occupazionali di Generalfinance, le dichiarazioni su operazioni sospette difformi dal vero, nonché la notifica alla Consob del ritardo nella diffusione di un’informazione privilegiata e la documentazione comprovante le modalità con cui sono state soddisfatte le condizioni previste per il ritardo nella comunicazione o, ancora, l’elenco delle persone aventi accesso alle informazioni privilegiate trasmesso alla predetta Autorità), alteri un messaggio di posta elettronica contenente informazioni rilevanti ai fini economici (e.g. accettazioni contrattuali, disposizioni bancarie, etc.) o in materia di segnalazioni (e.g. invio dei dati S.A.R.A) ovvero formi e veicoli un documento non genuino o veritiero, sottoscritto con firma digitale. Analogamente, la fattispecie potrebbe realizzarsi mediante la cancellazione o l’alterazione di informazioni a valenza probatoria presenti sui sistemi informativi aziendali (e.g. gestione vigilanza, controlli e accertamenti, gestione amministrativa e

---

<sup>1</sup> Capo III - Della falsità in atti, Artt. 476 – 490: • Art. 476. Falsità materiale commessa dal pubblico ufficiale in atti pubblici. • Art. 477. Falsità materiale commessa da pubblico ufficiale in certificati o autorizzazioni amministrative. • Art. 478. Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti. • Art. 479. Falsità ideologica commessa dal pubblico ufficiale in atti pubblici. • Art. 480. Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative. • Art. 481. Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità. • Art. 482. Falsità materiale commessa dal privato. • Art. 483. Falsità ideologica commessa dal privato in atto pubblico. • Art. 484. Falsità in registri e notificazioni. • Art. 485. Falsità in scrittura privata. • Art. 486. Falsità in foglio firmato in bianco. Atto privato. • Art. 487. Falsità in foglio firmato in bianco. Atto pubblico. • Art. 488. Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali. • Art. 489. Uso di atto falso. • Art. 490. Soppressione, distruzione e occultamento di atti veri.

<sup>2</sup> Il **documento informatico** è, secondo la definizione data dall’articolo 1, lett. p) del decreto legislativo n. 82 del 7 marzo 2005, il c.d. Codice dell’Amministrazione Digitale, “la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti”. Sul punto, la relazione al disegno di legge originario (n. 2807) annota: “[...] in considerazione della sopravvenuta inadeguatezza della definizione di documento informatico, inteso come supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi destinati ad elaborarli, si è deciso di accogliere, anche ai fini penali, la più ampia e corretta nozione di documento informatico, già contenuta nel regolamento di cui al decreto del Presidente della Repubblica 10 novembre 1997, n. 513, come ‘rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti’.”

contabile con precipuo riguardo alle scritture contabili; tenuta su supporto informatico del Registro delle persone informate), allo scopo di eliminare le prove di un'irregolarità amministrativa o di un altro reato.

- **Accesso abusivo ad un sistema informatico o telematico (Art. 615-ter codice penale)**

La norma punisce chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Il reato è più gravemente punito:

- se il fatto è commesso da un Pubblico Ufficiale o da un Incaricato di un Pubblico Servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
- se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
- se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti elencati riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è aumentata.

Per commettere il reato è necessaria la violazione di idonee misure di sicurezza, pertanto, si ritiene che debbano essere violati sistemi di "*introducing detection*" tali da impedire l'accesso *invito domino*, o, quanto meno, sistemi in grado di identificare l'utente che abbia effettuato l'accesso.

Integra il delitto di introduzione abusiva in un sistema informatico l'accesso ad un sistema che sia protetto da un dispositivo costituito anche soltanto da una parola chiave (c.d. *password*).

L'accesso abusivo si concretizza non appena vengono superate le misure di sicurezza del sistema, in quanto, l'art. 615ter c.p. punisce la semplice intrusione ancor prima di valutare l'ipotesi di danneggiamento o furto dei dati.

Il reato può anche essere causato da soggetti legittimati all'uso del sistema, autorizzati ad accedere solo a una parte dei dati contenuti in memoria. In tal caso il sistema protetto diviene quella parte di memoria a cui l'accesso non è autorizzato.

La permanenza non autorizzata consiste nel fatto che il soggetto responsabile dell'intrusione si sia trovato anche non volontariamente in una zona protetta del sistema, ma "*vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo*".

L'accesso abusivo può concretizzarsi anche attraverso la detenzione o la diffusione, contro la volontà del proprietario, di codici di accesso personali. Tale fattispecie è stata espressamente prevista e punita dal legislatore all'art. 615quater c.p.

A titolo meramente esemplificativo, si segnala che uno dei Destinatari del Modello potrebbe accedere, utilizzando le credenziali di un altro utente - da questo cedutegli ovvero illegittimamente carpite mediante inganno o raggirò - in un sistema informatico protetto (e.g. gli *account* dei clienti ammessi ad accedere sul portale *online* "GeneralWeb", il *software* aziendale deputato alla gestione della tesoreria, i sistemi di *remote banking* nella titolarità della Società, l'accesso al *software* diagnostico disponibile sul portale Infostat-UIF), al

fine consultare, alterare o trattare in qualsivoglia maniera i dati in esso contenuti, con conseguente vantaggio per la Società. Parimenti, la fattispecie criminosa potrebbe configurarsi qualora un esponente della Società violi il sistema informatico di una società concorrente, di un cliente potenziale (*prospect*) o effettivo ovvero di un debitore ceduto, seppur presidiato da misure di sicurezza informatica e cibernetica, allo scopo di carpire (i) informazioni riservate attinenti al *know how*, alla clientela, ai progetti di operazioni straordinarie o ai *business plan* del *competitor* ovvero (ii) dati inerenti a determinate condizioni economico-finanziarie applicabili ad un potenziale cliente. Ancora, il reato potrebbe realizzarsi laddove un dipendente, l'amministratore del sistema informatico aziendale o un tecnico terzo incaricato, su espressa indicazione di un esponente della Società, permanga indebitamente nel predetto sistema, al di fuori delle proprie mansioni o dell'incarico ricevuto, per apprendere, alterare o eliminare determinati documenti/informazioni aziendali (e.g. i dati contenuti nel portale *online* "GeneralWeb", sul Sistema Gestionale TOR, sul *software* dedicato alla gestione della tesoreria, sul sistema di *remote banking* della Società ovvero sul portale Infostat-UIF), con conseguente vantaggio della Società. Sul punto, si pensi, ad esempio, all'ipotesi di un accesso abusivo al Sistema Gestionale finalizzato a creare una rappresentazione artata degli incassi e, di riflesso, ad alterare il processo di liquidazione della pratica; così come potrebbe acquisire rilievo l'indebito intrattenimento sull'applicativo che gestisce le presenze in azienda per alterare i dati relativi alle voci del cedolino e, conseguentemente, ridurre in modo ingiustificato le erogazioni retributive nei confronti dei dipendenti.

La fattispecie potrebbe, poi, venire in rilievo qualora un esponente aziendale, accedendo indebitamente ai sistemi informativi interni, alteri il corretto funzionamento del processo di caricamento e pubblicazione dei comunicati stampa, i dati e i documenti contenuti nel sito *web* istituzionale rilevanti per il mercato (in particolare, quelli relativi alle *investor relations*) ovvero l'operatività del *plug-in* che, attraverso il collegamento alla piattaforma di Teleborsa, alimenta e rende immediatamente visualizzabile sull'apposita sezione del sito l'andamento del titolo quotato (oltre che i dati storici dello stesso, con la connessa possibilità di determinare il valore corrente ed il ritorno di un precedente investimento in azioni Generalfinance), al fine di far conseguire un vantaggio alla Società (e.g. limitare/ostacolare la conoscibilità dei risultati negativi del titolo ovvero di informazioni/eventi di particolare impatto su di esso).

Il medesimo disvalore assume la condotta dell'esponente aziendale o di un terzo soggetto, incaricato dalla Società, che acceda abusivamente ai sistemi informatici o telematici di Enti Pubblici al fine di acquisire informazioni riservate (e.g. Amministrazione Finanziaria, Autorità Giudiziaria o di Vigilanza).

- **Detenzione, diffusione e installazione abusiva di codici di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (Art. 615-*quater* codice penale)**

La norma punisce chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

A titolo meramente esemplificativo, si segnala che uno dei Destinatari potrebbe diffondere indebitamente ovvero ottenere per mezzo di una condotta fraudolenta, i codici di accesso al sistema informatico di altri utilizzatori autorizzati (e.g. gli *account* dei clienti ammessi ad accedere sul portale *online* "GeneralWeb", il portale Infostat-UIF), con conseguente vantaggio della Società derivante dall'ottenimento di informazioni riservate. Ancora, il reato potrebbe essere commesso ottenendo da un dipendente infedele il codice di

accesso alla rete interna di una società cliente o di un debitore ceduto, con lo scopo di ottenere informazioni sull'effettiva situazione amministrativa, contabile e finanziaria degli stessi, così da avvantaggiarsene. Il reato in commento potrebbe, altresì, configurarsi qualora un esponente della Società ovvero un soggetto esterno che opera per conto della stessa, realizzi un attacco di *social engineering* con l'obiettivo di ottenere le credenziali di accesso ai sistemi informativi interni di una società concorrente.

Inoltre, potrebbe integrare la fattispecie in commento la condotta dei dirigenti della Società che detengano, producano, diffondano, importino, comunichino o, comunque, utilizzino i codici accesso alle caselle *e-mail* dei dipendenti, allo scopo di controllare le attività da essi svolte nell'adempimento delle loro mansioni, anche in violazione di leggi sulla *privacy* o dello Statuto dei lavoratori, al di fuori di esigenze indifferibili, connesse all'attività operativa, alla tutela del patrimonio aziendale e al contrasto di comportamenti illeciti da parte del personale dipendente.

- **Detenzione, diffusione e installazione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Art. 615-quinquies codice penale)**

La norma punisce chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri ovvero installa apparecchiature, dispositivi o programmi informatici funzionali al raggiungimento del predetto scopo.

A titolo meramente esemplificativo, si segnala che uno dei Destinatari del Modello potrebbe mettere a disposizione di terzi, impiegare ovvero ordinare l'impiego di strumenti, apparecchiature o *software* (c.d. *malware*), in grado di danneggiare i dati o i programmi contenuti e protetti in un sistema informatico (e.g. il portale Infostat-UIF, il sistema informativo di un concorrente ovvero le piattaforme *web* di Borsa Italiana e Teleborsa che diffondono al pubblico in tempo reale la quotazione delle azioni della Società e i dati/informazioni ad essa pertinenti), con conseguente vantaggio della Società.

- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617-quater codice penale)**

La norma punisce chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe. La norma punisce, altresì, chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al precedente periodo.

I suddetti Reati sono punibili a querela della persona offesa; tuttavia, si procede d'ufficio se il fatto è commesso:

- 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- 2) da un Pubblico Ufficiale o da un Incaricato di un Pubblico Servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
- 3) da chi esercita, anche abusivamente, la professione di investigatore privato.

A titolo meramente esemplificativo, si segnala che uno dei Destinatari del Modello potrebbe, con artifici e

raggiri - eventualmente sfruttando i permessi e/o le autorizzazioni concesse (a titolo esemplificativo *user id, password, telefono aziendale, badge*) per l'utilizzo del sistema informativo (e.g. il portale *online* "Generalweb", il Sistema Gestionale ovvero il portale Infostat-UIF) - riuscire a venire a conoscenza di comunicazioni o dati riservati ovvero interromperne il flusso. Il reato potrebbe realizzarsi, altresì, qualora un esponente della Società renda di pubblico dominio ovvero alteri la corrispondenza telematica intercorsa tra i rappresentanti di una società concorrente, dopo averla fraudolentemente captata, con l'obiettivo di screditarne l'immagine agli occhi della clientela e del mercato di riferimento. Ancora, la figura delittuosa *de qua* potrebbe acquisire rilievo nell'ipotesi in cui un dipendente impieghi strumenti o sistemi atti a intercettare comunicazioni informatiche o telematiche di un concorrente, di un potenziale/effettivo cliente o investitore, per ottenere informazioni riservate sul *know how*, sulla clientela (c.d. *sniffing*) ovvero sulle sue future scelte di investimento/disinvestimento.

- **Detenzione, diffusione e installazione abusiva di apparecchiature e altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (Art. 617-quinquies codice penale)**

La norma punisce chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi. Come è stato graniticamente sostenuto dalla giurisprudenza di legittimità, all'atto intercettativo (in senso proprio) può essere assimilato il copiare i codici di accesso degli utenti di un sistema informatico o telematico tramite apposite apparecchiature (cfr. Cass. Pen., Sez. II, 09/11/2007, n. 45207).

A titolo meramente esemplificativo si segnala che uno dei Destinatari potrebbe posizionare registratori o strumenti per copiare o archiviare in una postazione informatica, comunicazioni, file o dati al fine di carpire comunicazioni inaccessibili e riservate. Del pari, il reato *de quo* potrebbe essere commesso laddove un esponente della Società si procuri, detenga, produca, riproduca, diffonda, importi, consegna, comunichi o metta a disposizione di altri un'apparecchiatura atta ad intercettare la corrispondenza telematica fra gli esponenti di una società *competitor*, di un potenziale/effettivo cliente o investitore, allo scopo di carpire informazioni riservate di carattere finanziario, patrimoniale ovvero commerciale.

- **Danneggiamento di informazioni, dati e programmi informatici (Art. 635-bis codice penale)**

La norma punisce chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

Il fatto è più grave se commesso con abuso della qualità di operatore del sistema e si procede d'ufficio.

Il reato potrebbe realizzarsi, ad esempio, qualora un esponente di Generalfinance cancelli irreversibilmente i dati contenuti su un sistema informativo aziendale o esterno (e.g. il portale *online* "GeneralWeb", con precipuo riguardo alle informazioni relative ai clienti, il Sistema Gestionale, per quanto concerne le informazioni rappresentative delle condizioni economico-finanziarie, patrimoniali o commerciali della Società, nonché la gestione dei crediti ovvero del *payroll*, ovvero le informazioni regolamentate e i relativi documenti stoccati e diffusi attraverso il circuito SDIR/STORAGE), consentendo a quest'ultima di conseguire un indebito vantaggio.

- **Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (Art. 635-ter codice penale)**

La norma punisce chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

Il reato è più grave se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici. Se il fatto è commesso con violenza alla persona o con minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata. A titolo meramente esemplificativo, si ipotizzi il caso in cui un esponente aziendale manometta documenti informatici dotati di valore probatorio e detenuti dall'Autorità Pubblica competente, nell'ambito di un procedimento penale o sanzionatorio a carico della Società (e.g. i verbali di un accertamento compiuto dall'Agenzia delle Entrate o dalla Guardia di Finanza), ovvero alteri irreversibilmente i dati trasmessi dalla Società all'Autorità Pubblica che vigila sull'operatività aziendale (e.g. Banca d'Italia e Consob).

- **Danneggiamento di sistemi informatici o telematici (Art. 635-quater codice penale)**

La norma punisce chiunque, mediante le condotte di cui all'articolo 635-bis c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

Il reato è più grave se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema. La fattispecie potrebbe realizzarsi, ad esempio, qualora un esponente della Società, servendosi di sofisticate tecniche di ingegneria informatica o per il tramite di società terze, danneggi ovvero istighi altri a danneggiare le infrastrutture tecnologiche di una società concorrente, con l'obiettivo di impedirne l'attività o di danneggiarne l'immagine pubblica.

- **Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635-quinquies codice penale)**

Il reato di danneggiamento di sistemi informatici o telematici è più grave se:

- il danneggiamento di sistemi è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento;
- dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile;
- e ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 c.p. ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

- **Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (Art. 640-quinquies codice penale)**

La norma punisce il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

## 1.2 ATTIVITÀ SENSIBILI

Avuto riguardo alla realtà di Generalfinance, le attività ritenute potenzialmente a rischio di commissione dei

reati sopra richiamati sono individuate come segue:

- gestione della struttura e infrastruttura informatiche della Società, e segnatamente: amministrazione, manutenzione ordinaria e straordinaria dei sistemi informativi aziendali; gestione degli strumenti IT e delle sottosezioni dei sistemi ICT; gestione e assegnazione delle credenziali di accesso ai portali gestionali della Società, nonché a quelli di soggetti terzi correlati all'operatività della Società;
- gestione del sito *web* istituzionale (caricamento, visualizzazione e conservazione dei dati, documenti e informazioni pubblicati, con particolare riguardo a quelli contenuti nelle sezioni “*Investor relations*”, “*Corporate Governance*” e “*Comunicati stampa*”);
- possesso e utilizzo delle credenziali personali e riservate di accesso al sistema informatico e agli applicativi, ai *software* gestionali, al *file server*, ad *internet* e per l'utilizzo della posta elettronica (sia ordinaria che certificata);
- utilizzo degli strumenti informatici (ivi inclusa la firma digitale) e accesso alle reti cablate o *wireless* dell'azienda;
- utilizzo dei *software* gestionali nello svolgimento delle attività tipiche del *core business* aziendale, in particolare: utilizzo del sistema informatico aziendale per l'analisi dell'attività svolta dai clienti cedenti e dei debitori ceduti, nonché possesso e impiego delle credenziali funzionali ad accedere ai portali di terzi per la consultazione delle pratiche aziendali in corso;
- accesso alle informazioni e ai dati sensibili dei clienti della Società (accesso ai sistemi informatici per segnalazione operazioni sospette, nonché accesso e utilizzo di banche dati esterne per finalità AML);
- accesso e gestione dei dati elettronici della Società;
- predisposizione, formalizzazione e trasmissione di documenti digitali.

### 1.3 PROTOCOLLI PER MITIGARE IL RISCHIO

Tutte le attività a rischio sono svolte conformandosi alle leggi vigenti e seguendo i principi, le procedure ed i Protocolli aziendali, Generici e Specifici, di cui al presente Modello.

- **Protocolli Generici**

In linea con quanto sopra riportato, la Società ha adottato ed ha debitamente formalizzato e divulgato al proprio interno i seguenti protocolli generici, soggetti a periodico aggiornamento:

- Sistema di deleghe e procure con relativi limiti di spesa;
- Principi di comportamento descritti nel Codice Etico che, in particolare, sancisce all'art. 6, l'obbligo per la Società di assicurare la riservatezza delle informazioni in proprio possesso e di astenersi dall'utilizzare dati riservati, salvo il caso di espressa e consapevole autorizzazione, nonché di garantire la riservatezza mediante adeguate misure di protezione dei dati trattati dalla Società;
- Formazione del personale;
- Organigramma aziendale e ordinamento organizzativo;
- Sistema sanzionatorio e disciplinare;
- Procedura Whistleblowing;
- *Web filter policy*, presidio di controllo sostanziale volto ad impostare blocchi al tentativo di accesso da parte dell'utente a determinati siti sfruttando la rete aziendale affinché sia garantito l'utilizzo della medesima in ottemperanza delle policy aziendali adottate.

Inoltre, per la medesima finalità, rilevano i seguenti presidi:

- Controllo svolto dal Collegio Sindacale;
- Controllo svolto dalla Società di Revisione;
- Controllo della Funzione di *Compliance*;
- Controllo della Funzione di *Internal Audit*;
- Supporto del Comitato Controllo, Rischi e Sostenibilità al Consiglio di Amministrazione nelle valutazioni e decisioni relative al sistema di controlli interni e di gestione dei rischi e all'approvazione delle relazioni periodiche di carattere finanziario e non finanziario, nonché nella promozione della continua integrazione delle *best practice* nazionali e internazionali nella *corporate governance* della Società e dei fattori ambientali, sociali e di *governance* nelle strategie aziendali volte al perseguimento del successo sostenibile.

- **Protocolli Specifici**

I Protocolli Specifici di Generalfinance si basano sui seguenti principi generali di controllo:

- 4) separazione dei compiti: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- 5) esistenza di procedure formalizzate: devono esistere disposizioni aziendali e/o procedure formalizzate, idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- 6) esistenza di un sistema di deleghe e procure coerente con le responsabilità organizzative assegnate: nell'ambito delle disposizioni aziendali e/o procedure formalizzate, i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere definiti e conosciuti all'interno della società;
- 7) tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informatici: ogni operazione relativa all'area a rischio 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.

Oltre ai Protocolli Generici, la Società ha sviluppato ed implementato i seguenti Protocolli Specifici per la riduzione del rischio di realizzazione dei delitti informatici e di trattamento illecito di dati:

- **Regolamento aziendale per l'utilizzo dei sistemi informativi**, il quale ha lo scopo di riassumere le principali norme comportamentali relative all'utilizzo delle risorse informatiche e telematiche cui ciascun dipendente/collaboratore di Generalfinance si deve attenere nello svolgimento della propria attività lavorativa;
- **Gestione e manutenzione dell'infrastruttura tecnologica e dei sistemi informativi**: la procedura ha l'obiettivo di definire ruoli, le responsabilità, le modalità operative e i principi comportamentali cui tutti i Destinatari devono attenersi affinché, nell'ambito del processo di gestione e manutenzione dell'infrastruttura tecnologica e dei sistemi informativi siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto;
- **Policy in materia di disaster recovery** che descrive le procedure operative da implementare per lo svolgimento dei processi di *backup* e di *disaster recovery* dei sistemi informativi e di tutto il patrimonio di dati concernenti l'attività e l'organizzazione societaria, nonché i sistemi di *storage*, gli

strumenti di *backup* impiegati e le relative configurazioni e procedure di ripristino, al fine di garantire l'affidabilità e il buon funzionamento dell'impianto ICT e delle infrastrutture aziendali, anche qualora si verifichi un danno o un evento distruttivo nei loro confronti;

- **Credit and collection policy** relativamente al corretto utilizzo degli applicativi gestionali che compongono l'infrastruttura informatica di Generalfinance (in particolar modo, TOR e GeneralWeb) nell'ambito della gestione del *core business*;
- **Manuale metodologico (Governance 262/05) – Regolamento del Dirigente Preposto** che, nel definire le linee guida e la prassi operativa per il presidio del rischio di errata informativa finanziaria, disciplina i c.d. *IT General Controls* quali regole di governo e controlli che permettono di valutare il livello minimo di sicurezza che deve essere garantito nella progettazione e nella gestione del sistema informatico al fine di assicurare la riservatezza, integrità e disponibilità delle informazioni amministrativo-contabili, ovvero di garantire la correttezza e completezza delle elaborazioni elettroniche, prevenendo altresì lo svolgimento di attività di verifica e monitoraggio dell'operatività degli *IT General Controls* e l'emissione di una lettera di attestazione periodica da parte del Responsabile della Direzione ICT e Organizzazione;
- **Codice per il trattamento delle informazioni privilegiate**, il quale è volto a disciplinare (i) l'individuazione, la gestione e il trattamento delle informazioni privilegiate della Società, (ii) le procedure da osservare per la comunicazione, sia all'interno che all'esterno dell'organizzazione aziendale, di tali informazioni; (iii) la tenuta e l'aggiornamento dell'elenco delle persone che hanno accesso alle specifiche informazioni rilevanti e delle persone che hanno accesso a quelle privilegiate. In particolare, e per quanto qui d'interesse, il Codice prevede la pubblicazione e la conservazione sul sito *internet* della Società, per un periodo di almeno 5 anni, di tutte le informazioni privilegiate comunicate al pubblico, disponendo che il sito debba consentire agli utenti di accedere alle informazioni pubblicate senza discriminazioni e gratuitamente, che esse siano contenute in una sezione facilmente identificabile che siano indicate chiaramente la data e l'ora della divulgazione e che siano presentate in ordine cronologico.
- **Clausole contrattuali 231**: il protocollo ha l'obiettivo di disciplinare le attività di redazione dei contratti con le terze parti, allo scopo di evitare che, nella prestazione dei servizi contrattualizzati, possano essere commessi i Reati di cui al Decreto.
- **Clear desk, clear screen Policy**: finalizzata a migliorare la sicurezza e la riservatezza delle informazioni gestite dal personale di Generalfinance, sia con riguardo (i) ai documenti trattati e ai supporti di archiviazione rimovibili utilizzati ("clear desk"), sia (ii) agli strumenti di elaborazione delle informazioni ("clear screen"), al fine di ridurre il rischio di accessi non autorizzati, perdita e danneggiamento di informazioni durante e al di fuori del normale orario di lavoro o quando gli uffici o i dispositivi non sono presidiati;
- **Procedura di gestione delle violazioni di dati personali (data breach)**: che ha lo scopo di gestire il flusso delle attività da porre in essere qualora si realizzi una violazione di dati personali (con ciò intendendosi una violazione di sicurezza che comporta accidentalmente o illecitamente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati), disponendo, in particolare, l'obbligo per il titolare del trattamento dei dati di notificare la violazione all'Autorità di controllo competente, senza ingiustificato ritardo. Inoltre, la procedura prevede che, nell'ipotesi in cui la violazione riguardi un asset tecnologico-informatico, vengano eventualmente coinvolti il CIO, il Responsabile Ufficio Sistemi ICT e l'ICT Security Manager o il referente per il sistema informativo, o la società esterna incaricata dell'assistenza informatica, al fine valutare la portata della violazione.



#### **1.4 CONTROLLI DELL'ORGANISMO DI VIGILANZA**

L'Organismo di Vigilanza esegue verifiche periodiche con riguardo alle specifiche attività sensibili di cui alla presente Parte Speciale secondo le seguenti modalità: (i) attenendosi alla programmazione da esso prevista nel piano di attività elaborato per ciascun anno di riferimento ovvero (ii) a campione, qualora la verifica non sia ricompresa all'interno del piano annuale di attività, ma l'OdV la ritenga comunque necessaria.

#### **1.5 FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA**

La funzione aziendale nella cui competenza ricade la gestione dell'Attività Sensibile dà apposita evidenza documentale di ogni attività a rischio e di eventuali criticità (e.g. attacco informatico subito o tentato), secondo quanto previsto dalla specifica procedura operativa applicabile. A seconda dell'attività, la funzione competente dovrà effettuare i controlli definiti nella procedura e, in caso di anomalia, inviare all'Organismo di Vigilanza le opportune segnalazioni e i flussi informativi richiesti.

Più concretamente, le funzioni aziendali nella cui competenza rientra l'attività a rischio dovranno informare l'Organismo di Vigilanza in merito:

- alle decisioni prese in qualsiasi ambito all'interno della struttura organizzativa che non abbiano seguito il normale *iter* autorizzativo previsto dalle procedure interne;
- alle criticità emerse nella gestione della rete informatica e che potrebbero rilevare ai sensi del Decreto.



## **PARTE SPECIALE VII**

*Reati Tributari (Art. 25-quinquiesdecies)*

## 1.1 I REATI RICHIAMATI DAL DECRETO E LA RELATIVA MODALITÀ DI COMMISSIONE

La riforma dei reati tributari, introdotta con la Legge 19 dicembre 2019 n. 157 di conversione del D.L. 26 ottobre 2019, n. 124 (c.d. Decreto Fiscale), ha spinto verso un complessivo irrigidimento dell'intero sistema repressivo dei fenomeni di evasione fiscale incidendo sensibilmente tanto sul D.lgs. 74/2000 ("*Nuova disciplina dei reati in materia di imposta sui redditi e sul valore aggiunto*") - modificando le sanzioni e le soglie di punibilità per quasi tutte le fattispecie di reato ivi previste -, quanto sulla materia della responsabilità amministrativa degli enti ampliando, attraverso l'inserimento dell'art. 25-*quiquiesdecies* al D.lgs. 231/2001, il catalogo dei reati presupposto ricomprendendovi anche gli illeciti tributari.

In particolare, in base all'intervento normativo, vengono ad essere annoverati i delitti di:

- *dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'art. 2, comma 1, D.lgs. 74/2000;*
- *dichiarazione fraudolenta mediante altri artifici previsto dall'art. 3, D.lgs. 74/2000;*
- *emissione di fatture o altri documenti per operazioni inesistenti previsto dall'art. 8, comma 1 e comma 2-bis, D.Lgs. 74/2000;*
- *occultamento o distruzione di documenti contabili previsto dall'art. 10, D.lgs. 74/2000;*
- *sottrazione fraudolenta al pagamento di imposte previsto dall'art. 11, D.lgs. 74/2000;*

Nel caso in cui, a seguito alla commissione di uno dei delitti di cui sopra, l'ente abbia conseguito un profitto di rilevante entità, al comma secondo del nuovo art. 25-*quiquiesdecies* il legislatore ha previsto un aumento della sanzione pecuniaria pari ad un terzo.

Sono, inoltre, applicabili le sanzioni interdittive di cui all'art. 9, comma 2, lett. c) "*divieto di contrarre con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio*", lett. d) "*esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi*" e lett. e) "*divieto di pubblicizzare beni o servizi*"<sup>1</sup>.

Deve ulteriormente segnalarsi come la riforma normativa del 2019 ha altresì introdotto nuove forme di aggressione patrimoniale prevedendo l'estensione della confisca per equivalente del profitto dell'evasione fiscale a carico della persona giuridica che dell'evasione abbia concretamente beneficiato (quindi non più solo a carico dell'autore del reato). Nella specie, nel caso in cui il legale rappresentante o altro organo aziendale realizzi, nell'interesse o a vantaggio dell'ente, uno dei reati tributari indicati dall'art. 25-*quiquiesdecies* sarà sempre applicabile il sequestro preventivo e, in caso di condanna, la confisca di somme di denaro, beni o altre utilità di valore equivalente al risparmio di spesa realizzato grazie all'evasione fiscale.<sup>2</sup>

Recentemente, poi, il legislatore è nuovamente intervenuto sull'art. 25-*quiquiesdecies*: con il D.lgs. 75/2020 (avente ad oggetto l'attuazione della direttiva (UE) 2017/1371 relativa "*alla lotta contro la frode*

1 Art. 25- *quiquiesdecies*, comma 3: "*nei casi previsti dai commi 1, 1-bis e 2, si applicano le sanzioni interdittive di cui all'art. 9, comma 2, lett. c), d) ed e)*".

2 Art. 19 D.lgs. 231/2001 "*nei confronti dell'ente è sempre disposta, con la sentenza di condanna, la confisca del prezzo o del profitto del reato*" (comma 1), quando ciò non sia possibile la confisca "*può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato*" (comma 2).

che lede gli interessi finanziari dell'Unione mediante il diritto penale" - cd. direttiva PIF) vi ha introdotto il comma 1-bis<sup>3</sup>, che estende ulteriormente il novero dei reati tributari che possono determinare la responsabilità amministrativa dell'ente includendovi anche i delitti di dichiarazione infedele, di omessa dichiarazione e di indebita compensazione (artt. 4, 5 e 10 *quater* del D.lgs. 74/2000) laddove commessi:

- (i) nell'ambito di sistemi fraudolenti transfrontalieri (ovverossia commessi in parte anche nel territorio di altro Stato membro dell'Unione europea) e
- (ii) con il fine di evadere l'imposta sul valore aggiunto per un importo superiore a dieci milioni di euro.

Ancora più di recente il D.lgs. n. 156/2022 – recante "Disposizioni correttive e integrative del decreto legislativo 14 luglio 2020, n. 75, di attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale" – ha novellato l'art. 25 *quinquiesdecies*, comma 1-bis, del Decreto 231 prevedendo, in termini più puntuali e "tipicizzanti", che i delitti di dichiarazione infedele, omessa dichiarazione e indebita compensazione rilevano ai fini della responsabilità dell'ente solo se commessi al fine di evadere l'imposta sul valore aggiunto e nell'ambito di sistemi fraudolenti transfrontalieri (*i.e.* se connessi al territorio di almeno uno Stato membro dell'Unione europea) da cui consegue (nocumento effettivo) o possa conseguire un danno complessivo (nocumento potenziale) pari o superiore a dieci milioni di euro.

Il citato intervento di riforma ha, inoltre, interpolato il comma 1-bis nell'art. 6 del D.lgs. n. 74/2000, in virtù del quale i delitti di dichiarazione fraudolenta (artt. 2 e 3) – fuori dei casi di concorso nel reato di emissione di fatture o documenti per operazioni inesistenti (art. 8) – e di dichiarazione infedele (art. 4) sono ora punibili anche a titolo di tentativo, qualora la condotta incriminata dalle predette norme sia posta in essere al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri, connessi al territorio di almeno un altro Stato membro dell'Unione europea, dai quali consegue o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro.

La punibilità in forma tentata dei delitti menzionati, sulla scorta del combinato disposto della disposizione in commento e dell'art. 26 del Decreto 231, si traduce in un'estensione delle fattispecie che valgono a far insorgere la responsabilità delle persone giuridiche.

- **Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (Art. 2, comma 1 e comma 2-bis, D.lgs. 74/2000)**

Il delitto è previsto dall'art. 2, comma 1, D.lgs. 74/2000 e comporta l'irrogazione di una sanzione pecuniaria fino a cinquecento quote, e dall'art. 2, comma 2-bis, D.lgs. 74/2000, che comporta l'irrogazione di una sanzione pecuniaria fino a quattrocento quote.

La norma punisce chi, allo scopo di evadere l'imposta, indica elementi passivi fittizi nella dichiarazione annuale obbligatoria dei redditi o dell'IVA e a tal fine si avvale di fatture o di altrui documenti riferiti ad operazioni inesistenti.

A titolo esemplificativo, il reato sussiste sia nell'ipotesi di inesistenza oggettiva (il caso in cui l'operazione non sia stata mai posta in essere nella realtà), che di sovrapproduzione qualitativa (il caso della fattura che attesti la cessione di beni e/o servizi aventi un prezzo maggiore rispetto a quelli forniti), quanto di inesistenza soggettiva (il caso in cui l'operazione oggetto dell'imposizione fiscale sia stata eseguita ma tra

---

<sup>3</sup> Art. 25-*quinquiesdecies*, comma 1-bis "*in relazione alla commissione dei delitti previsti dal D.lgs. 74/2000, se commessi nell'ambito dei sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, si applicano all'ente le sanzioni pecuniarie: a) per il delitto di dichiarazione infedele previsto dall'art. 4, la sanzione pecuniaria fino a trecento quote; b) per il delitto di omessa dichiarazione previsto dall'art. 5, la sanzione pecuniaria fino a quattrocento quote; per il delitto di indebita compensazione previsto dall'art. 10 quater, la sanzione pecuniaria fino a quattrocento quote*".

soggetti diversi da quelli figuranti cartolarmente come parti del rapporto).

- **Dichiarazione fraudolenta mediante altri artifici (Art. 3 D.lgs. 74/2000)**

Il delitto è previsto dall'art. 3 D.lgs. 74/2000 e comporta l'irrogazione di una sanzione pecuniaria fino a cinquecento quote. La norma punisce chi, allo scopo di evadere l'imposta, indica elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi o crediti e ritenute fittizie nella dichiarazione annuale obbligatoria dei redditi o dell'IVA e a tal fine compie operazioni simulate oggettivamente o soggettivamente ovvero si avvale di documenti falsi o altri mezzi fraudolenti. A titolo esemplificativo, integra il reato l'utilizzo di qualsiasi mezzo fraudolento ovvero qualsiasi condotta artificiosa attiva o omissiva che, in violazione di uno specifico obbligo giuridico, determini una falsa rappresentazione della realtà idonea ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria.

- **Emissione di fatture o altri documenti per operazioni inesistenti (Art. 8, comma 1 e comma 2-bis D.lgs. 74/2000)**

Il delitto è previsto dall'art. 8, comma 1 e comma 2-bis, D.lgs. 74/2000, i quali comportano, rispettivamente, l'irrogazione di una sanzione pecuniaria fino a cinquecento e quattrocento quote. La norma punisce chi, allo scopo di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

- **Occultamento o distruzione di documenti contabili (Art. 10 D.lgs. 74/2000)**

Il delitto è previsto dall'art. 10 D.lgs. 74/2000 e comporta l'irrogazione di una sanzione pecuniaria fino a quattrocento quote. La norma punisce chi, allo scopo di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge, in tutto o in parte, scritture contabili o documenti la cui conservazione è obbligatoria.

A titolo esemplificativo, è il caso in cui le scritture contabili non vengano custodite né presso la sede della società, né presso il commercialista, con la chiara intenzione di non volerle esibire ai verificatori e di sottrarle al loro esame attraverso il trasferimento in luoghi diversi rispetto a quelli cui dovrebbero ordinariamente trovarsi.

- **Sottrazione fraudolenta al pagamento di imposte (Art. 11 D.lgs. 74/2000)**

Il delitto è previsto dall'art. 11 D.lgs. 74/2000 e comporta l'irrogazione di una sanzione pecuniaria fino a quattrocento quote. La norma punisce chi aliena o compie altri atti fraudolenti su propri o altrui beni idonei a rendere, in tutto o in parte, inefficace la procedura di riscossione coattiva, al fine di sottrarsi al pagamento delle imposte sui redditi o sul valore aggiunto e dei conseguenti interessi e sanzioni amministrative.

- **Dichiarazione infedele (Art. 4 D.lgs. 74/2000)**

Il delitto è previsto dall'art. 4 D.lgs. 74/2000 e comporta, se commesso nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, l'applicazione a carico dell'ente della sanzione pecuniaria fino a trecento quote.

In generale, la fattispecie delittuosa si configura quando qualcuno, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi inesistenti quando congiuntamente:

- a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila;
- b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di

elementi passivi inesistenti, è superiore al 10% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione o, comunque, è superiore a due milioni.

Si badi che il delitto in commento rileva ai fini della responsabilità dell'ente solo laddove sia commesso al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri (connessi al territorio di almeno un altro Stato membro dell'Unione europea) da cui consegua o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro.

- **Omessa dichiarazione (Art. 5 D.lgs. 74/2000)**

Il delitto è previsto dall'art. 5 D.lgs. 74/2000 e comporta, se commesso nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, l'applicazione a carico dell'ente della sanzione pecuniaria fino a quattrocento quote.

In generale, la fattispecie delittuosa si configura quando qualcuno, al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, ad euro cinquantamila. È punito altresì chiunque non presenti, essendovi obbligato, la dichiarazione di sostituto di imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.

Si tenga a mente che tale fattispecie acquista rilievo ai fini della responsabilità dell'ente qualora sia commesso al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri (connessi al territorio di almeno un altro Stato membro dell'Unione europea) da cui consegua o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro.

- **Indebita compensazione (Art. 10 quater D.lgs. 74/2000)**

Il delitto è previsto dall'art. 10 quater D.lgs. 74/2000 e comporta, se commesso nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, l'applicazione a carico dell'ente della sanzione pecuniaria fino a quattrocento quote.

In generale, la fattispecie delittuosa si configura quando qualcuno non versa le somme dovute utilizzando in compensazione, ai sensi dell'art. 17 D.lgs. 241/1997:

- a) crediti non spettanti, per un importo annuo superiore a cinquantamila euro;
- b) crediti inesistenti, per un importo annuo superiore a cinquantamila euro.

Anche la norma incriminatrice *de qua* assurge a reato-presupposto della responsabilità dell'ente soltanto se la condotta sanzionata sia commessa al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri (connessi al territorio di almeno un altro Stato membro dell'Unione europea) da cui consegua o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro.

## 1.2 ATTIVITÀ SENSIBILI

Le aree maggiormente a rischio sono quelle che coinvolgono i processi di tenuta della documentazione contabile e, nel complesso, le attività dichiarative volte alla determinazione dei tributi che ogni società tenuta a svolgere.

Riguardo alle fattispecie di Reato sopra descritte, i Processi sensibili individuati nell'ambito della Società sono i seguenti:

- (i) nell'ambito dei processi di gestione della contabilità e dei dati per la predisposizione del bilancio e di altre comunicazioni sociali:
  - l'acquisizione, elaborazione, valutazione ed illustrazione dei dati e delle informazioni necessarie

- alla predisposizione del bilancio e delle altre comunicazioni ai soci, ai creditori, alla società di revisione, alle autorità ed al pubblico, relative alla situazione economica, patrimoniale e finanziaria della Società, ivi compresi i dati previsionali, obiettivi quantitativi e dati contabili di periodo, nonché le comunicazioni circa le altre informazioni riguardanti la Società;
- la predisposizione del bilancio e delle comunicazioni ai soci, ai creditori, alla società di revisione, alle autorità ed eventualmente al pubblico, relative alla situazione economica, patrimoniale e finanziaria della Società, ivi compresi i dati previsionali, obiettivi quantitativi e dati contabili di periodo, nonché le comunicazioni circa le altre informazioni riguardanti la Società;
  - l'attività di preparazione delle riunioni assembleari, svolgimento e verbalizzazione delle assemblee;
  - la custodia delle scritture contabili e dei libri sociali;
  - la gestione dei rapporti con i Soci, la Società di Revisione e le Autorità Pubbliche di Vigilanza (il rischio si potrebbe verificare in tutte le fasi di collaborazione o contatto con gli organi di controllo interno e con i revisori contabili);
  - le operazioni sul capitale;
  - le operazioni della Società nelle quali gli amministratori abbiano un interesse, per conto proprio o altrui.
- (ii) gestione delle attività di pianificazione fiscale;
- (iii) gestione dei flussi finanziari in entrata e in uscita;
- (iv) gestione delle consulenze e degli incarichi professionali nonché dei relativi pagamenti;
- (v) gestione del ciclo attivo;
- (vi) gestione del ciclo passivo (selezione e gestione dei fornitori);
- (vii) gestione delle liberalità, sponsorizzazioni e omaggi;
- (viii) gestione dei rimborsi spesa.

### 1.3 I PROTOCOLLI PER MITIGARE IL RISCHIO

Tutte le attività a rischio sono svolte conformandosi alle leggi vigenti e seguendo i principi, le procedure ed i Protocolli aziendali, Generici e Specifici, di cui al presente Modello.

- **Protocolli Generici**

In linea con quanto sopra riportato, la Società ha adottato ed ha debitamente formalizzato e divulgato al proprio interno i seguenti Protocolli Generici, soggetti a periodico aggiornamento:

- Sistema di deleghe e procure con relativi limiti di spese;
- Principi di comportamento descritti nel Codice Etico;
- Organigramma aziendale e ordinamento organizzativo;
- Sistema sanzionatorio e disciplinare;
- Formazione del Personale;
- Procedura *Whistleblowing*.

Inoltre, per la medesima finalità, rilevano i seguenti presidi:

- Controllo svolto dal Collegio Sindacale;
- Controllo svolto dalla Società di Revisione;
- Controllo svolto dalla Funzione di *Compliance*;
- Controllo svolta dalla Funzione di *Internal Audit*;
- Supporto del Comitato Controllo, Rischi e Sostenibilità al Consiglio di Amministrazione

nelle valutazioni e decisioni relative al sistema di controlli interni e di gestione dei rischi e all'approvazione delle relazioni periodiche di carattere finanziario e non finanziario, nonché nella promozione della continua integrazione delle best practice nazionali e internazionali nella corporate governance della Società e dei fattori ambientali, sociali e di governance nelle strategie aziendali volte al perseguimento del successo sostenibile.

- **Protocolli Specifici**

I Protocolli Specifici di Generalfinance si basano sui seguenti principi generali di controllo:

- 1) separazione dei compiti: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- 2) esistenza di procedure formalizzate: devono esistere disposizioni aziendali e/o procedure formalizzate, idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- 3) esistenza di un sistema di deleghe e procure coerente con le responsabilità organizzative assegnate: nell'ambito delle disposizioni aziendali e/o procedure formalizzate, i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere definiti e conosciuti all'interno della società;
- 4) tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informatici: ogni operazione relativa all'area a rischio 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.

I Protocolli Specifici implementati dalla Società per la riduzione del rischio di commissione di realizzazione dei Reati Tributari sono i seguenti:

- **Protocollo Reati Tributari**, il cui obiettivo è la definizione di regole di condotta che indichino i comportamenti che i Destinatari devono e non devono tenere nelle attività di tenuta della documentazione contabile e nello svolgimento di tutte le attività dichiarative volte alla determinazione ed al versamento dei tributi, affinché siano prevenuti comportamenti idonei a realizzare i Reati;
- **Clausole Contrattuali 231**, che ha l'obiettivo di disciplinare le attività di redazione dei contratti con le terze parti, allo scopo di evitare che, nella prestazione dei servizi contrattualizzati, possano essere commessi Reati;
- **Protocollo gestione delle liberalità, donazioni, sponsorizzazioni e omaggi**, il cui obiettivo è la definizione di regole di condotta che indichino i comportamenti cui i Destinatari devono attenersi nell'ambito del processo di gestione delle liberalità (intendendosi con esse le donazioni, le sponsorizzazioni e gli omaggi) affinché siano prevenuti comportamenti idonei a realizzare i Reati;
- **Procedura di approvvigionamento di beni, servizi, consulenze ed incarichi professionali** che è volta a definire le regole di condotta e procedurali che indicano i comportamenti cui i Destinatari devono attenersi nella gestione del processo di approvvigionamento, in tutte le sue fasi operative (dalla definizione del fabbisogno di acquisto sino alla registrazione delle fatture passive, l'autorizzazione e la registrazione dei pagamenti), affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto.

- **Procedura gestione della tesoreria**, la quale definisce le regole di condotta che indicano i comportamenti cui i Destinatari devono attenersi nell'ambito dei processi connessi all'amministrazione della tesoreria aziendale e, in particolare, degli investimenti e disinvestimenti; degli affidamenti bancari e approvvigionamenti; della gestione della liquidità nonché della gestione amministrativa di incassi e pagamenti affinché siano prevenuti comportamenti idonei a realizzare i Reati;
- **Procedura gestione dei rapporti con i soci e con gli organi di controllo**, la quale definisce i comportamenti cui i Destinatari devono attenersi nelle attività connesse con la gestione dei rapporti con i soci e gli organi di controllo societario affinché siano prevenuti comportamenti idonei a realizzare i Reati;
- **Procedura di gestione della contabilità e redazione del bilancio fiscale (Policy redazione bilancio di esercizio) e Regolamento in materia di pianificazione e controllo di gestione**, la quale definisce le regole cui i Destinatari devono attenersi nella gestione dei processi legati alla tenuta della contabilità, alla redazione del bilancio fiscale e all'adempimento degli obblighi fiscali, nonché di tutte quelle attività connesse alla pianificazione strategica, alla predisposizione del *budget* e al controllo di gestione affinché siano prevenuti comportamenti idonei a realizzare i Reati.
- **Vademecum per i rimborsi spese (gestione trasferte e note spese)**: obiettivo della procedura è la definizione di regole di condotta che indichino i comportamenti che i Destinatari devono e non devono tenere nell'attività di gestione dei rimborsi spese a dipendenti e spese di rappresentanza, affinché siano prevenuti comportamenti idonei a realizzare i Reati;
- **Procedura per la gestione dei flussi finanziari** (Regolamento tracciabilità flussi finanziari), che ha lo scopo di definire le regole per la gestione e l'autorizzazione dei flussi finanziari in entrata ed in uscita dalla Società. In particolare, formalizza e definisce le scelte operative e i processi interni preordinati al rispetto delle norme in materia di tracciabilità dei flussi finanziari, con riferimento al pagamento di crediti che abbiano formato oggetto di cessione a favore di Generalfinance.

#### 1.4 CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza esegue verifiche periodiche con riguardo alle specifiche attività sensibili di cui alla presente Parte Speciale secondo le seguenti modalità: (i) attenendosi alla programmazione da esso prevista nel piano di attività elaborato per ciascun anno di riferimento ovvero (ii) a campione, qualora la verifica non sia ricompresa all'interno del piano annuale di attività, ma l'OdV la ritenga comunque necessaria.

#### 1.5 FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

La funzione aziendale nella cui competenza ricade la gestione dell'Attività Sensibile dà apposita evidenza documentale di ogni attività a rischio, secondo quanto previsto dalla specifica procedura operativa applicabile. A seconda dell'attività, la funzione competente dovrà effettuare i controlli definiti nella procedura e, in caso di anomalia, inviare all'Organismo di Vigilanza le opportune segnalazioni e i flussi informativi richiesti.



## **PARTE SPECIALE VIII**

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

## 1.1 I REATI RICHIAMATI DAL DECRETO E LA RELATIVA MODALITÀ DI COMMISSIONE

Il sempre più crescente sviluppo dell'economia digitale e delle nuove tecnologie di pagamento ha determinato un esponenziale incremento delle ipotesi di frode (spesso a carattere transfrontaliero) che minano non soltanto la sicurezza economica, ma anche la regolarità dell'implementazione del mercato unico digitale. A fronte di tali criticità il legislatore sovranazionale, prima, e quello nazionale, poi, hanno consolidato nel tempo un presidio di tutela e sanzionatorio, volto a contrastare la frode e la contraffazione dei mezzi di pagamento diversi dai contanti.

Più di recente, il legislatore euro-unitario ha adottato la Direttiva (UE) 2019/713 mercé la quale ha posto in capo agli Stati membri l'obbligo di introdurre misure necessarie per reprimere: i) l'utilizzazione fraudolenta di uno strumento di pagamento diverso dai contanti che sia oggetto di illecita acquisizione, appropriazione ovvero contraffatto o falsificato; ii) le manifestazioni criminose correlate all'utilizzazione fraudolenta di strumenti di pagamento materiali e immateriali diversi dal contante; iii) l'effettuare un trasferimento di denaro, valore monetario o di valute virtuale, arrecando illecitamente a terzi una perdita patrimoniale, a cui corrisponde l'intento di procurarsi un ingiusto profitto, introducendo, alterando, cancellando, trasmettendo o sopprimendo dati informatici; iv) la fabbricazione o l'ottenimento, per sé o per altri, di dati informatici o di altri mezzi progettati o adattati per commettere una delle condotte sopraelencate; v) l'istigazione, il favoreggiamento o il concorso negli illeciti fin qui descritti. Inoltre, la Direttiva ha previsto che, nell'ambito degli ordinamenti nazionali, le persone giuridiche possano essere ritenute responsabili dei reati *de quibus* commessi a loro vantaggio da qualsiasi soggetto che agisca a titolo individuale o che occupi una posizione preminente nell'organizzazione dell'ente collettivo.

Dal canto suo, il legislatore italiano – in esecuzione della Legge di delegazione europea 2020/2021 – ha recepito la Direttiva in commento con il D.Lgs. 8 novembre 2021, n. 184, che ha apportato modifiche sostanziali sia al codice penale che al Decreto 231, in particolar modo interpolando in quest'ultimo *corpus* normativo l'art. 25-*octies*.1: la predetta norma estende la responsabilità amministrativa degli enti ai reati riguardanti strumenti di pagamento diversi dai contanti.

I reati contemplati dall'inedito art. 25-*octies*.1 sono i seguenti:

- **Indebito utilizzo e falsificazione di carte di credito e di pagamento (Art. 493-*ter* codice penale)**

La fattispecie incriminatrice, così come novellata dal citato D.Lgs. n. 184/2021, prevede e punisce due ipotesi criminose autonome e tra loro alternative:

- i. per un verso, l'indebito utilizzo, da parte di chi non è titolare, di carte di credito o di pagamento, ovvero di qualsiasi altro documento analogo che abiliti al prelievo di denaro contante, all'acquisto di beni o alla prestazione di servizi, al fine di trarne profitto per sé o per altri;
- ii. per altro verso, la falsificazione o l'alterazione degli strumenti di pagamento immateriali, di carte di credito o di pagamento ovvero di qualsiasi altro strumento o documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, il possesso, la cessione o l'acquisizione di tali strumenti, carte o documenti di provenienza illecita o, comunque, falsificati o alterati, nonché ordini di pagamento prodotti con essi, sempre al fine di trarne profitto per sé o per altri.

A ben vedere, l'art. 493-*ter* c.p. tutela non soltanto il patrimonio del titolare della carta di credito, ma anche gli interessi pubblici sottesi alla sicurezza delle transazioni commerciali, alla speditezza del traffico giuridico e alla fiducia nell'utilizzazione da parte dei consociati di siffatti strumenti di pagamento. Da ciò discende la

non operatività della causa di giustificazione del consenso dell'avente diritto (art. 50 c.p.), essendo irrilevante il consenso eventualmente espresso dal titolare dello strumento di pagamento all'utilizzo dello stesso, e ciò proprio in ragione della natura plurioffensiva del reato in commento (cfr. Cass. Pen., Sez. II, 16/02/2021, n. 18609). Di contro, la fattispecie può ritenersi esclusa nei soli casi in cui il terzo agisca nell'esclusivo interesse del titolare, eseguendo materialmente l'operazione per cui è stato autorizzato dal titolare (*i.e.* l'autorizzazione assume rilevanza solo nelle ipotesi in cui sia apprezzabile, con tutta evidenza, attraverso la dimostrazione dei rapporti esistenti tra le parti e delle circostanze in cui sia intervenuta tale autorizzazione).

Come già accennato, la norma incriminatrice è stata modificata dal D.Lgs. n. 184/2021 che ne ha esteso l'oggetto materiale su cui ricadono le condotte analizzate, con l'effetto di ricomprendersi *"ogni altro mezzo di pagamento diverso dal contante"*, ovverosia 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"* (art. 1 del D.Lgs. cit.). Al riguardo, preme segnalare che i primi commentatori sono dell'avviso che nell'alveo di tale nozione possono essere ricondotti sia i mezzi di pagamento immateriali (e.g. sistemi di *remote banking*, *Satispay*, *Paypal*, *PagoPA*, ecc.) e le valute digitali<sup>1</sup>, sia le c.d. criptovalute (che, seppur prive di valore legale, vengono sempre più riconosciute, nella prassi sociale, come effettivi strumenti di pagamento).

A mero titolo esemplificativo, il reato potrebbe essere commesso da uno dei Destinatari del Modello che utilizzi gli strumenti di pagamento diversi dal contante (e.g. ricorso al sistema di *remote banking*, uso della carta di credito aziendale o della carta carburante connessa all'autovettura aziendale) per operazioni/finalità differenti da quelle espressamente autorizzate dalla Società e per le quali è stata concessa la disponibilità di tali strumenti, allorché tale condotta sia stata resa possibile dall'assenza di misure di sicurezza/verifica (come in caso di libero o agevole accesso ai *token* collegati al sistema di *remote banking* o al possesso materiale delle carte di pagamento), dall'inidoneità delle misure di sicurezza logica poste a presidio di tali strumenti ovvero sia stata realizzata da un esponente aziendale nella prospettiva di far conseguire un vantaggio alla Società (e.g. compiendo con tali strumenti indebite elargizioni a funzionari della Pubblica Amministrazione, chiamati a vigilare sull'operatività di Generalfinance, o a potenziali clienti/*partner* ovvero consentendo ad essi la materiale utilizzabilità degli strumenti stessi). Al contempo, la figura delittuosa potrebbe configurarsi nell'ipotesi in cui uno dei Destinatari del Modello alteri il funzionamento di una carta di credito o di altra carta elettronica che abiliti all'acquisto di beni (e.g. mutando artificialmente il *plafond*, impedendo la registrazione degli acquisti) ovvero del sistema di *remote banking* (e.g. intervenendo sulle procedure autorizzative delle disposizioni di pagamento), giovandosi dell'assenza di misure di sicurezza/verifica oppure agendo per la finalità sopra prospettata, *id est* far conseguire un vantaggio anche alla Società.

- **Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (Art. 493-quater codice penale)**

La norma punisce, 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 a sé o a

---

<sup>1</sup> L'art. 1, lett. d) del D.Lgs. n. 184/2021 così definisce la valuta virtuale: *"una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata o scambiata elettronicamente"*.

altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati ovvero sono appositamente adattati a tale scopo.

Si tratta di un'incriminazione di recente conio, introdotta nel codice penale dal D.Lgs. n. 184/2021, il cui perno è costituito da congegni prodromici e funzionali alla commissione di ulteriori condotte illecite che si traducono nell'indebito utilizzo degli strumenti di pagamento diversi dal contante (e.g. la realizzazione di un *software* che consenta di produrre o alterare le carte di credito digitali ovvero di commettere sofisticate truffe *on-line*). La destinazione teleologica delle apparecchiature, dei dispositivi o programmi informatici alla commissione dei reati relativi ai mezzi di pagamento in questione – la quale va desunta, in termini univoci, dalle loro peculiarità per caratteristiche tecnico-costruttive o di progettazione – sostanzia non soltanto l'oggetto materiale del reato, ma anche il contenuto del dolo specifico, corrispondente al fine di fare uso di tali strumenti ovvero di consentire ad altri di farne uso per lo scopo surrichiamato.

A mero titolo esemplificativo, il reato potrebbe essere configurato qualora uno dei Destinatari del Modello realizzi, introduca, metta a disposizione o, comunque, utilizzi dispositivi o programmi informatici idonei ad alterare il funzionamento degli strumenti di pagamento diversi dal contante che sono nella titolarità della Società (e.g. carta di credito/debito aziendali, altre carte elettroniche che abilitano all'acquisto di beni o alla ricezione di servizi come la carta carburante o la tessera ViaCard, *remote banking*), con l'effetto di occultare la tracciabilità delle transazioni/erogazioni/acquisti o, più in generale, dei flussi finanziari ovvero di realizzare operazioni di trasferimento di denaro in modo fraudolento o al di fuori delle ipotesi e dei *range* economici autorizzati, se tale condotta si riveli funzionale a far conseguire un vantaggio per la Società (e.g. elargendo somme a funzionari della Pubblica Amministrazione, chiamati a vigilare su Generalfinance, per fini illeciti o impedendo la registrazione degli acquisti/transazioni così da omettere il pagamento del giusto corrispettivo verso il soggetto erogatore dei beni/servizi) ovvero sia stata agevolata dall'assenza di appositi presidi di sicurezza/verifica.

La probabilità di verificazione di tale fattispecie è inferiore rispetto al rischio associato al precedente reato-presupposto.

- **Frode informatica aggravata (Art. 640-ter, comma 2, codice penale)**

La fattispecie circostanziata in parola, anch'essa introdotta nell'ambito dell'intervento riformatore di cui al D.Lgs. n. 184/2021, reprime le ipotesi di ingiusto arricchimento ottenuto tramite l'impiego fraudolento di un sistema informatico da cui consegua, quale esito ultimo e necessario per la configurabilità della figura criminosa, un trasferimento di denaro, valore monetario o valuta virtuale. In particolare, la condotta può sostanziarsi:

- i) nella alterazione, in qualsiasi modo realizzata, del funzionamento di un sistema informatico o telematico (e.g. *remote banking*) di modo da poter disporre un trasferimento di denaro o di altro valore monetario, anche virtuale, di cui beneficia il soggetto agente a danno del titolare del sistema oggetto di manipolazione;
- ii) nell'intervento senza diritto (quindi, abusivo) su dati, informazioni o programmi contenuti nel sistema informatico/telematico o ad esso pertinenti, che determini, agevoli o, comunque, consenta di compiere un trasferimento di denaro e di ogni altro valore dematerializzato.

Esemplificando, il reato potrebbe essere integrato dalla condotta di uno dei Destinatari del Modello che intervenga sul funzionamento dei sistemi informatici collegati all'operatività e alla rendicontazione delle carte di credito/debito aziendali, mutando artificialmente il *plafond* ovvero impedendo la registrazione

delle transazioni effettuate con conseguente vantaggio per la Società (e.g. riconoscendo un corrispettivo inferiore a quello dovuto per i servizi e i beni ceduti dal soggetto erogatore, con conseguente minore esborso della Società). La medesima condotta potrebbe esplicarsi nell'alterazione dei sistemi deputati alla gestione da remoto dei conti correnti societari, impedendo la tracciabilità dei flussi in ingresso e in uscita (e.g. al fine di vulnerare la corretta consuntivazione dei dati funzionali all'erogazione e alla liquidazione della pratica nell'ambito dell'attività *core* di Generalfinance e, conseguentemente, di realizzare un minor esborso delle somme contrattualmente dovute), mutando la profilazione dei soggetti autorizzati a disporre i pagamenti o di quelli che hanno la facoltà di mero accesso all'*home banking* ovvero realizzando pagamenti indebiti/privi di giustificazione (e.g. attribuire indebitamente le somme afferenti ad una pratica ad altro cliente) in modo idoneo a dissimulare le evidenze documentali di tali movimentazioni. In via strumentale, potrebbe altresì venire in rilievo l'alterazione del funzionamento dell'applicativo gestionale dedicato alla Tesoreria, del *software* "Sepafast" ovvero dei dati in esso contenuti, rilevanti ai fini della procedura di caricamento della lista delle disposizioni di pagamento (e.g. l'identificazione del beneficiario e del suo IBAN, il codice identificativo unico della pratica cui si riferisce l'erogazione, la divisa in cui sarà eseguito il pagamento), al fine di realizzare un indebito trasferimento di denaro per le finalità e con le modalità sopra rappresentate.

- **Ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio**

Quale previsione di chiusura e residuale il comma 2 dell'art. 25-*octies*.1 D.Lgs. cit. prevede che possa fondare la responsabilità amministrativa da reato dell'ente, salvo che il fatto integri un altro illecito amministrativo sanzionato più gravemente, ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, qualora abbia ad oggetto strumenti di pagamento diversi dai contanti.

A mero titolo esemplificativo e non esaustivo, si ipotizzi il caso in cui un esponente della Società induca un cliente (effettivo o *prospect*) o altro *stakeholder* a consegnare o comunicargli le chiavi di accesso da remoto al proprio conto corrente o alla propria carta di credito/debito, prospettando tale passaggio quale condizione di garanzia necessaria per la concessione dell'affidamento/delibera del Fido ovvero per la stipula di un contratto.

Si tratta, in ogni caso, di un rischio reato che presenta una minore possibilità di verifica, ma che non può essere esclusa aprioristicamente, anche in considerazione della genericità dell'individuazione legislativa dei *predicate crime*.

## 1.2 ATTIVITÀ SENSIBILI

Avuto riguardo alla realtà di Generalfinance, le attività ritenute potenzialmente a rischio di commissione dei reati-presupposto sopra richiamati sono individuate come segue:

- utilizzo delle carte di credito/debito aziendali;
- utilizzo di carte elettroniche che abilitano all'acquisto di altri beni o servizi (e.g. carta carburante, Telepass, Viacard, etc.);
- accesso e utilizzo dei sistemi informatici per la gestione della tesoreria e dei conti correnti (*i.e.* servizi di *remote banking*) nell'ambito dei pagamenti e flussi finanziari in ingresso e in uscita, nonché inserimento dati nei sistemi gestionali finalizzati alla disposizione e all'esecuzione dei pagamenti/bonifici;
- assegnazione e utilizzo delle credenziali personali e riservate di accesso al sistema informatico, ai



software gestionali e, in particolar modo, ai servizi di *remote banking*, nonché gestione della rete/infrastruttura informatica con particolare riguardo al funzionamento degli applicativi gestionali e all'assegnazione delle credenziali di accesso ai predetti sistemi informativi.

### 1.3 PROTOCOLLI PER MITIGARE IL RISCHIO

Tutte le attività a rischio sono svolte conformandosi alle leggi vigenti e seguendo i principi, le procedure ed i Protocolli aziendali, Generici e Specifici, di cui al presente Modello.

- **Protocolli Generici**

In linea con quanto sopra riportato, la Società ha adottato ed ha debitamente formalizzato e divulgato al proprio interno i seguenti protocolli generici, soggetti a periodico aggiornamento:

- Sistema di deleghe e procure con relativi limiti di spesa;
- Principi di comportamento descritti nel Codice Etico;
- Formazione del personale;
- Organigramma aziendale e ordinamento organizzativo;
- Sistema sanzionatorio e disciplinare;
- Procedura Whistleblowing;
- *Web filter policy*, presidio di controllo sostanziale volto ad impostare blocchi al tentativo di accesso da parte dell'utente a determinati siti sfruttando la rete aziendale affinché sia garantito l'utilizzo della medesima in ottemperanza delle policy aziendali adottate.

Inoltre, per la medesima finalità, rilevano i seguenti presidi:

- Controllo svolto dal Collegio Sindacale;
- Controllo svolto dalla Società di Revisione;
- Controllo svolto dalla Funzione di *Compliance*;
- Controllo svolto dalla Funzione di *Internal Audit*;
- Supporto del Comitato Controllo, Rischi e Sostenibilità al Consiglio di Amministrazione nelle valutazioni e decisioni relative al sistema di controlli interni e di gestione dei rischi e all'approvazione delle relazioni periodiche di carattere finanziario e non finanziario, nonché nella promozione della continua integrazione delle *best practice* nazionali e internazionali nella *corporate governance* della Società e dei fattori ambientali, sociali e di *governance* nelle strategie aziendali volte al perseguimento del successo sostenibile.

- **Protocolli Specifici**

I Protocolli Specifici di Generalfinance si basano sui seguenti principi generali di controllo:

- 1) separazione dei compiti: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- 2) esistenza di procedure formalizzate: devono esistere disposizioni aziendali e/o procedure formalizzate, idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- 3) esistenza di un sistema di deleghe e procure coerente con le responsabilità organizzative assegnate: nell'ambito delle disposizioni aziendali e/o procedure formalizzate, i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere definiti e conosciuti

- all'interno della società;
- 4) tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informatici: ogni operazione relativa all'area a rischio 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;
  - 5) chiara identificazione dei soggetti intestatari/utilizzatori degli strumenti di pagamento aziendali diversi dal contante, delle modalità e del regime di autorizzazione dei pagamenti e di consuntivazione/rendicontazione degli stessi;
  - 6) implementazione di appositi strumenti elettronici di supporto all'attività di verifica dell'autenticità e della liceità della provenienza degli strumenti di pagamento diversi dal contante, nonché di garanzia delle misure di sicurezza logica poste a presidio di tali strumenti;
  - 7) predisposizione di blocchi in relazione all'installazione e all'utilizzo di hardware e software non approvati e non coerenti con l'attività professionale espletata dai singoli dipendenti;

Oltre ai Protocolli Generici, la Società ha sviluppato e implementato i seguenti Protocolli Specifici per la riduzione del rischio di realizzazione dei reati:

- **Procedura per la gestione dei flussi finanziari (Regolamento tracciabilità flussi finanziari)**: il cui scopo è formalizzare e definire le scelte operative e i processi interni preordinati al rispetto delle norme in materia di tracciabilità dei flussi finanziari, con particolare riferimento alla regolazione delle attività di predisposizione, disposizione ed esecuzione di pagamento attraverso i sistemi di *remote/corporate banking*;
- **Procedura gestione della tesoreria**: obiettivo della procedura è la definizione di regole di condotta e operative che indichino i comportamenti cui i Destinatari devono attenersi nell'ambito dei processi connessi all'amministrazione della tesoreria aziendale e, in particolare, degli investimenti e disinvestimenti, degli affidamenti bancari e approvvigionamenti, della gestione della liquidità, della gestione amministrativa di incassi e pagamenti (flussi in ingresso e in uscita), nonché dell'utilizzo delle linee di *funding*, affinché siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto e sia correttamente regolato l'impiego del servizio di *remote/corporate banking*;
- **Credit and collection policy (già Processo del credito)**, con particolare riguardo alle parti in cui viene previsto e regolato l'impiego degli strumenti di *remote/corporate banking*, oltre che l'interfaccia con esso del Sistema Gestionale e dei suoi applicativi, nell'ambito dell'attività *core* della Società e, in particolare, dell'erogazione della pratica (al termine della quale viene accreditato al Cedente l'importo oggetto di anticipazione del credito ceduto), della liquidazione della pratica (che esita nell'accredito al Cedente delle somme non erogate, maturate a seguito del pagamento effettuato dal Debitore Ceduto), e del monitoraggio degli incassi;
- **Regolamento aziendale per l'utilizzo dei sistemi informativi**, il quale ha lo scopo di riassumere le principali norme comportamentali e procedurali relative all'utilizzo delle risorse informatiche e telematiche cui ciascun dipendente/collaboratore di Generalfinance si deve attenere nello svolgimento della propria attività lavorativa;
- **Gestione e manutenzione dell'infrastruttura tecnologica e dei sistemi informativi**: la procedura ha l'obiettivo di definire ruoli, le responsabilità, le modalità operative e i principi comportamentali cui tutti i Destinatari devono attenersi affinché, nell'ambito del processo di gestione e



manutenzione dell'infrastruttura tecnologica e dei sistemi informativi siano prevenuti comportamenti idonei a realizzare i Reati di cui al Decreto;

- **Vademecum per i rimborsi spese**, laddove sono previsti l'impiego della carta di credito aziendale per il pagamento delle spese relative alle trasferte (e.g. trasferte aeree) e la conservazione della documentazione giustificativa;
- **Clausole contrattuali 231**, il protocollo ha l'obiettivo di disciplinare le attività di redazione dei contratti con le terze parti, allo scopo di evitare che, nella prestazione dei servizi contrattualizzati, possano essere commessi i Reati di cui al Decreto.

#### 1.4 CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza esegue verifiche periodiche con riguardo alle specifiche attività sensibili di cui alla presente Parte Speciale secondo le seguenti modalità: (i) attenendosi alla programmazione da esso prevista nel piano di attività elaborato per ciascun anno di riferimento ovvero (ii) a campione, qualora la verifica non sia ricompresa all'interno del piano annuale di attività, ma l'OdV la ritenga comunque necessaria.

#### 1.5 FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

La funzione aziendale nella cui competenza ricade la gestione dell'Attività Sensibile dà apposita evidenza documentale di ogni attività a rischio, secondo quanto previsto dalla specifica procedura operativa applicabile. A seconda dell'attività, la funzione competente dovrà effettuare i controlli definiti nella procedura e, in caso di anomalia, inviare all'Organismo di Vigilanza le opportune segnalazioni e i flussi informativi richiesti.

Più concretamente, le funzioni aziendali nella cui competenza rientra l'attività a rischio dovranno informare l'Organismo di Vigilanza in merito:

- alle decisioni prese in qualsiasi ambito all'interno della struttura organizzativa che non abbiano seguito il normale *iter* autorizzativo previsto dalle procedure interne;
- alle criticità emerse nella gestione e che potrebbero rilevare ai sensi del Decreto.



## **PARTE SPECIALE IX**

*Delitti e illeciti di market abuse (art. 25-sexies)*

## 1.1 I REATI RICHIAMATI DAL DECRETO E LA RELATIVA MODALITÀ DI COMMISSIONE

I reati-presupposto contemplati dall'art. 25-*sexies* sono i seguenti:

- **Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (Art. 184 D.Lgs. n. 58/1998)**
- **Manipolazione del mercato (Art. 185 D.Lgs. n. 58/1998)**

Inoltre, gli articoli 187-*bis* e 187-*ter* del D.Lgs. n. 58/1998 (TUF) prevedono, rispettivamente, gli illeciti amministrativi di "Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate" e "Manipolazione del mercato", le cui condotte equivalgono a quelle punite penalmente dalle norme incriminatrici di cui agli artt. 184 e 185 del TUF.

Per quanto attiene a questi illeciti deve segnalarsi che la responsabilità dell'Ente discende dalla previsione, contenuta all'art. 187-*quinquies* del TUF, che rimanda agli stessi principi, condizioni ed esenzioni del D.Lgs. n. 231/2001, stabilendo che la responsabilità per tali illeciti ricada in capo all'Ente solo laddove lo stesso non riesca a fornire, a propria discolpa, la prova secondo cui l'autore dell'illecito ha agito esclusivamente nell'interesse proprio o di un terzo.

Tutte le norme in questione tendono a garantire l'integrità, la trasparenza, la correttezza e l'efficienza dei mercati finanziari in ottemperanza al principio secondo cui tutti gli investitori debbono operare in posizione di uguaglianza in relazione ai profili di: i) accesso all'informazione; ii) conoscenza del meccanismo di fissazione del prezzo e iii) conoscenza delle origini delle informazioni pubbliche.

Più in particolare, l'art. 182 del TUF prevede che le fattispecie di *market abuse* si applichino a fatti concernenti:

1. strumenti finanziari ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;
2. strumenti finanziari ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alla negoziazione in un sistema multilaterale di negoziazione italiano o di altro Paese dell'Unione europea;
3. strumenti finanziari negoziati su un sistema organizzato di negoziazione;
4. strumenti finanziari non previsti dai punti precedenti, il cui prezzo o valore dipende dal prezzo o dal valore di uno strumento finanziario menzionato negli stessi punti ovvero ha un effetto su tale prezzo o valore, compresi, ma non in via esclusiva, i *credit default swap* e i contratti differenziali;
5. condotte od operazioni, comprese le offerte, relative alle aste su una piattaforma d'asta autorizzata, come un mercato regolamentato di quote di emissioni o di altri prodotti oggetto d'asta correlati, anche quando i prodotti oggetto d'asta non sono strumenti finanziari, ai sensi del regolamento (UE) n. 1031/2010 della Commissione, del 12 novembre 2010;
6. i contratti a pronti su merci che non sono prodotti energetici all'ingrosso, idonei a provocare una sensibile alterazione del prezzo o del valore degli strumenti finanziari di cui all'articolo 180, comma 1, lettera a) del TUF;
7. gli strumenti finanziari, compresi i contratti derivati o gli strumenti derivati per il trasferimento del rischio di credito, idonei a provocare una sensibile alterazione del prezzo o del valore di un contratto a pronti su merci, qualora il prezzo o il valore dipendano dal prezzo o dal valore di tali strumenti finanziari;

8. gli indici di riferimento (*benchmark*).

Le predette condotte sono sanzionate secondo la legge italiana, anche se commesse in territorio estero, qualora ineriscano strumenti finanziari ammessi o per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o in un sistema multilaterale di negoziazione italiano o a strumenti finanziari negoziati su un sistema organizzato di negoziazione italiano.

Alla luce di tali considerazioni di ordine sistematico, si analizzano, di seguito, gli elementi costitutivi delle fattispecie criminose contemplate dall'art. 25-*sexies*.

- **Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (Art. 184 D.Lgs. n. 58/1998)**

Soggetto attivo del reato è chiunque sia in possesso di informazioni privilegiate in ragione:

- della sua qualità di membro di organi di amministrazione, direzione o controllo della società emittente gli strumenti finanziari; e/o
- della sua qualità di azionista di una società emittente; e/o
- dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio; e/o
- della preparazione o dell'esecuzione di attività delittuose;

nonché chiunque altro acquisisca informazioni privilegiate per cause diverse rispetto a quelle indicate ai punti che precedono.

La condotta criminosa sanzionata dalla norma in commento si sostanzia alternativamente:

- nell'acquistare, vendere o compiere altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni privilegiate (*insider trading*);
- nel raccomandare o indurre altri, sulla base di tali informazioni, al compimento di taluna delle operazioni indicate al punto che precede (*tuyautage*);
- nel comunicare tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato effettuato ai sensi dell'articolo 11 del regolamento (UE) n. 596/2014 (d'ora in poi solo: MAR) (*tipping*).

Le disposizioni dell'art. 184 T.U.F. si applicano anche quando i fatti riguardano condotte od operazioni, comprese le offerte, relative alle aste su una piattaforma d'asta autorizzata, come un mercato regolamentato di quote di emissioni o di altri prodotti oggetto d'asta correlati, anche quando i prodotti oggetto d'asta non sono strumenti finanziari.

Gli strumenti finanziari oggetto delle condotte tipizzate sono quelli enucleati all'art. 180, comma 1, del TUF, trattasi, invero, di quelli: (i) ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di altro Paese dell'Unione europea; (ii) ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un sistema multilaterale di negoziazione italiano o di altro Paese dell'Unione europea, purché l'ammissione sia stata richiesta ovvero autorizzata dall'emittente; (iii) negoziati su un sistema organizzato di negoziazione italiano o di altro Paese dell'Unione europea; nonché (iv) negoziati su un sistema organizzato di negoziazione italiano o di altro Stato membro.

Affinché il reato in parola possa dirsi configurato, è necessario che l'agente sia in possesso di informazioni privilegiate che, in virtù del rinvio operato dall'art. 180, comma 1, lett. b-ter, T.U.F. all'art. 7, paragrafi da 1 a

4, del MAR, sono così identificabili:

- informazioni aventi un carattere preciso, che non sono state rese pubbliche, concernenti – direttamente o indirettamente – uno o più emittenti o uno o più strumenti finanziari, e che, se rese pubbliche, potrebbero avere un effetto significativo sui prezzi di tali strumenti finanziari o sui prezzi di strumenti finanziari derivati collegati;
- informazioni relative agli strumenti derivati su merci, aventi un carattere preciso, che non sono state rese pubbliche, concernenti - direttamente o indirettamente - uno o più di tali strumenti derivati o concernenti direttamente il contratto a pronti su merci collegato, e che, se rese pubbliche, potrebbero avere un effetto significativo sui prezzi di tali strumenti derivati o sui contratti a pronti su merci collegati e qualora si tratti di informazioni che si possa ragionevolmente attendere che siano comunicate o che debbano essere obbligatoriamente comunicate conformemente alle disposizioni legislative o regolamentari dell'Unione o nazionali, alle regole di mercato, ai contratti, alle prassi o alle consuetudini, convenzionali sui pertinenti mercati degli strumenti derivati su merci o a pronti;
- informazioni attinenti alle quote di emissioni o ai prodotti oggetto d'asta correlati, aventi un carattere preciso, che non sono state rese pubbliche, concernenti - direttamente o indirettamente - uno o più di tali strumenti e che, se rese pubbliche, potrebbero avere un effetto significativo sui prezzi di tali strumenti o sui prezzi di strumenti finanziari derivati collegati;
- nel caso di persone incaricate dell'esecuzione di ordini relativi a strumenti finanziari, le informazioni trasmesse da un cliente e connesse agli ordini pendenti in strumenti finanziari del cliente, aventi un carattere preciso e concernenti - direttamente o indirettamente - uno o più emittenti o uno o più strumenti finanziari e che, se rese pubbliche, potrebbero avere un effetto significativo sui prezzi di tali strumenti finanziari, sul prezzo dei contratti a pronti su merci collegati o sul prezzo di strumenti finanziari derivati collegati.

In ogni caso, l'informazione è di carattere preciso quando: i) è riferita ad una serie di circostanze esistenti ovvero che possono ragionevolmente verificarsi in futuro ovvero a un evento che si è verificato o che può, ragionevolmente, verificarsi in futuro<sup>1</sup>; ii) permette di trarre conclusioni *ex ante* sulla sorte del possibile effetto di detto complesso di circostanze o di detto evento sui prezzi degli strumenti finanziari o del relativo strumento finanziario derivato, dei contratti a pronti su merci collegati o dei progetti oggetto d'asta sulla base delle quote di emissioni.

Per converso, non valgono a costituire informazioni privilegiate:

- le voci e i *rumores*;
- le informazioni che si limitano a notificare un adempimento (es. pubblicazione del calendario concernente eventi societari, divulgazione dell'esito delle delibere assembleari, formalizzazione dell'intervenuta variazione del capitale sociale);
- gli studi e le valutazioni, se basati su informazioni già pubbliche.

Potrebbe, invece, costituire informazione privilegiata quella che anticipa un'operazione straordinaria della società, diffusa dalla stampa come *rumores* di mercato, ma recante un grado di dettaglio tale da renderla riconducibile a fonti qualificate.

Allo stesso modo, costituisce informazione privilegiata la notizia dell'imminente diffusione di uno studio o di una ricerca che, una volta diffusa, abbia caratteristiche tali da influire in modo sensibile sui prezzi degli strumenti finanziari oggetto della ricerca.

Da ultimo, giova evidenziare che l'elemento soggettivo richiesto per l'integrazione del reato è il dolo generico

---

<sup>1</sup> Cass. Pen., Sez. V, sent. n. 49362/2012.

integrato dalla consapevolezza di essere in possesso di informazioni privilegiate e dalla volontà di utilizzarle con le modalità sin d'ora descritte.

A mero titolo esemplificativo, il reato potrebbe essere commesso da uno dei Destinatari del Modello che, nell'ambito della propria attività professionale, acquisisca informazioni confidenziali e rilevanti, quali possono essere quelle relative alla programmazione o al compimento di un'importante operazione commerciale (e.g. l'acquisizione di un cliente di particolare rilevanza), finanziaria (e.g. l'emissione di cambiali finanziarie) ovvero straordinaria da parte della Società (e.g. l'acquisto o la vendita di *asset*), ancora coperte da riserbo, e comunichi tali informazioni ad altri, al di fuori del normale esercizio del lavoro, nella prospettiva di far conseguire un vantaggio a Generalfinance (e.g. favorire la conclusione di una futura *partnership* con una determinata controparte ovvero incrementare l'andamento del titolo). Al contempo, la figura delittuosa potrebbe configurarsi nell'ipotesi in cui un esponente aziendale comunichi indebitamente ad un soggetto terzo le informazioni relative all'approvazione delle situazioni infra-annuali prima della loro divulgazione al pubblico, sollecitandolo a investire nelle azioni della Società, con l'effetto di alterare la parità degli investitori, ovvero nell'ipotesi in cui, sfruttando la conoscenza di tali dati, effettui egli stesso delle operazioni in conto proprio sui predetti titoli azionari, in violazione delle prescrizioni dettate dalla normativa in materia di *internal dealing*.

- **Manipolazione del mercato (Art. 185 D.Lgs. n. 58/1998)**

A differenza della fattispecie di "*Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate*" – per la quale, come visto, sono richieste specifiche qualità soggettive dell'agente (quali, ad esempio, la carica ricoperta ovvero l'attività lavorativa) –, commette il reato di cui all'art. 185 del TUF chiunque realizzi la condotta oggetto della fattispecie che può essere integrata dalla:

- diffusione di notizie non veritiere (manipolazione informativa);
- realizzazione di operazioni simulate (manipolazione operativa);
- attuazione di altri artifici (manipolazione operativa o mista);

condotte, tutte queste, che occorre (i) siano concretamente idonee a provocare una sensibile alterazione del prezzo dello strumento finanziario, ovvero (ii) si pongano ad un livello maggiore rispetto ai normali oscillamenti del mercato secondo un giudizio di prognosi postuma.

Dunque, affinché possa dirsi integrato il reato di cui all'art. 185 del TUF non è necessario che l'autore ponga in essere comportamenti ulteriori e diretti a trarre vantaggio dalla manipolazione stessa.

Gli strumenti finanziari, oggetto della fattispecie, sono quelli enucleati all'art. 180, comma 1, del TUF, ossia i medesimi analizzati *supra* nella parte relativa all'art. 184 del TUF.

Più nel dettaglio, la condotta di manipolazione informativa può dirsi integrata nell'ipotesi in cui siano state diffuse notizie non veritiere ovvero fuorvianti ad una platea di soggetti indeterminata. Al contrario, qualora la diffusione sia rivolta ad una sola persona ovvero ad un numero ristretto di soggetti, potrebbe configurarsi la condotta di manipolazione informativa mista. Può, invece, assumere rilevanza l'ipotesi in cui la notizia venga ricevuta da un soggetto che, con alta probabilità, la veicolerà ad una pluralità di altri utenti (si pensi, invero, al caso segnalato all'Autorità Giudiziaria dalla Consob relativo al comportamento dell'intermediario di un collocamento di un prestito obbligazionario emesso su un mercato lussemburghese che aveva fornito una *credit opinion*, contenente alcuni elementi di falsità, ad un numero limitato di investitori).

Ai fini della punibilità, rileva qualsiasi tipo di esternazione di notizie tali da influire sul prezzo di uno strumento finanziario.



Sebbene non esista un elenco di notizie rilevanti, ovvero la possibilità di definire in astratto quando una notizia debba considerarsi tale, la Società ha individuato la seguente casistica – esemplificativa e non esaustiva – di tipi di informazioni potenzialmente rilevanti:

- assetti proprietari;
- composizione del management;
- piani di incentivazione del management;
- attività dei revisori;
- operazioni sul capitale;
- emissione di strumenti finanziari;
- caratteristiche degli strumenti finanziari emessi;
- acquisizioni, fusioni, scissioni, *joint venture*;
- ristrutturazioni e riorganizzazioni aziendali;
- operazioni su strumenti finanziari, *buy-back e accelerated book-building*;
- procedure concorsuali;
- contenzioso legale e fiscale;
- revoca di affidamenti bancari;
- svalutazioni / rivalutazioni di attività o di strumenti finanziari in portafoglio;
- brevetti, licenze, diritti, marchi, ecc.;
- insolvenze di importanti debitori;
- acquisto o vendita di asset;
- andamento della gestione;
- variazioni dei risultati contabili di periodo attesi (*profit warning e earning surprise*);
- ricevimento o annullamento di ordini importanti; stipula o interruzione di contratti rilevanti;
- ingresso in nuovi (o uscita da) mercati;
- modifica dei piani di investimento;
- *policy* di distribuzione di dividendi;
- informazioni che Generalfinance apprende dalle autorità di vigilanza nell'ambito di un *Supervisory Review and Evaluation Process (SREP)* effettuato ai sensi dell'articolo 97 della Direttiva 2013/36/EU (CRD IV).

Ad ogni modo, occorre significare che la comunicazione al pubblico di notizie false aventi ad oggetto le operazioni di cui sopra integra il reato di manipolazione informativa solo al ricorrere dell'elemento psicologico della fattispecie (dolo generico).

La manipolazione operativa, invece – come già anticipato *supra* – può essere effettuata mediante il compimento di operazioni simulate e/o altri artifici.

La prima tipologia di manipolazione operativa si verifica nell'ipotesi in cui le parti pongono in essere operazioni che appaiono diverse rispetto a quella originariamente voluta, ovvero nei casi di:

- compravendita di strumenti finanziari che non comporta una reale modifica della proprietà;
- inserimento di ordine con prezzi superiori o inferiori ai prezzi di mercato e loro cancellazione prima dell'esecuzione.

Per quanto attiene, invece, alla manipolazione operativa realizzata mediante altri artifici, sebbene i contorni della fattispecie non risultino precisamente individuati dal legislatore, la giurisprudenza di legittimità si è più volte pronunciata puntualizzando che per *“artificiosità non si intende necessariamente illiceità intrinseca dei mezzi utilizzati. L'inganno può infatti essere realizzato attraverso condotte apparentemente lecite, ma che*

*combinare tra loro, ovvero realizzate in determinate circostanze di tempo e di luogo, intenzionalmente realizzano una distorsione del gioco della domanda e dell'offerta in modo tale che il pubblico degli investitori sia indotto in errore circa lo spontaneo e corretto processo di formazione dei prezzi*<sup>2</sup>.

Ad ogni modo, anche la mancata diffusione di notizie soggette all'obbligo di *disclosure* può configurarsi quale artificio idoneo a determinare una sensibile alterazione del prezzo degli strumenti finanziari ai quali la notizia si riferisce.

A mero titolo esemplificativo, il reato di manipolazione del mercato potrebbe essere configurato qualora un esponente aziendale, attraverso l'emissione di appositi comunicati stampa e/o l'adulterazione delle informative di natura finanziaria, diffonda al pubblico dati artificiosamente alterati circa l'andamento del *business* societario (e.g. alterando le informazioni concernenti il volume dei crediti acquistati dalle imprese clienti – il c.d. *turnover* – ovvero le anticipazioni effettuate dalla Società a favore di queste ultime), così da creare un quadro informativo falso della situazione economico-finanziaria e patrimoniale di Generalfinance, suscettibile di fornire indicazioni decettive e svianti in merito alle azioni della stessa. Ancora, potrebbe venire in rilievo la condotta di uno dei Destinatari del Modello che all'apertura o alla chiusura delle giornate di mercato, acquisti o vendita strumenti finanziari di Generalfinance, con l'effetto (anche solo probabile) di fuorviare gli investitori che agiscono sulla base dei prezzi esposti, compresi quelli di apertura e di chiusura.

## 1.2 ATTIVITÀ SENSIBILI

Riguardo alle fattispecie criminose sopra descritte, i processi sensibili individuati nell'ambito delle attività della Società sono:

### **A) Informazioni Rilevanti e/o Privilegiate e comunicazioni esterne**

1. elaborazione, detenzione, gestione/trattamento e diffusione delle Informazioni Rilevanti e/o Privilegiate;
2. gestione del Registro delle Persone Informate e del Registro delle Specifiche Informazioni Rilevanti (*Relevant Information List - RIL*);
3. gestione, controllo e divulgazione delle informazioni societarie e delle comunicazioni verso e dall'esterno (anche con il supporto degli *advisor* esterni), tra cui:
  - i. gestione dei rapporti con gli organi di stampa, i *mass media*, le agenzie di *rating* e gli analisti finanziari, nonché con le associazioni di categoria;
  - ii. gestione dei comunicati stampa (elaborazione, approvazione, emissione e conservazione degli stessi);
  - iii. gestione del sito *web* istituzionale (caricamento, visualizzazione e conservazione dei dati, documenti e informazioni ivi pubblicati, con particolare riguardo a quelli contenuti nelle sezioni "*Investor relations*", "*Corporate Governance*" e "Comunicati stampa");
  - iv. realizzazione dei sondaggi di mercato;
  - v. formazione e diffusione del calendario degli eventi societari (c.d. calendario finanziario);
  - vi. gestione dei rapporti con il gestore del sistema di diffusione e stoccaggio delle informazioni regolamentate autorizzato dalla Consob (SDIR): Teleborsa.
4. gestione dei rapporti con gli azionisti, gli investitori, potenziali o effettivi, e la comunità finanziaria

<sup>2</sup> Così in Cass. Pen., 20 gennaio 2009, n. 2063.

(c.d. *investor relations*), nonché con Borsa Italiana;

5. gestione dei rapporti e delle informative/segnalazioni dirette alle Autorità di Vigilanza (in particolare, Consob) anche in occasione di verifiche, ispezioni ed accertamenti;

#### **B) Pianificazione strategico-finanziaria, comunicazioni sociali e informativa societaria**

6. pianificazione strategica e finanziaria;
7. formazione, gestione e controllo delle comunicazioni sociali normativamente previste (e.g. bilancio d'esercizio, Informativa al Pubblico "Terzo Pilastro") e, più in generale, dell'informativa societaria, ivi incluse le attività di:
  - i. elaborazione/agggregazione, analisi, diffusione (sia interna che esterna) e conservazione dei dati relativi alla situazione economica, finanziaria e patrimoniale della Società (e.g. esposizione ai rischi, monitoraggio degli incassi, *turnover*);
  - ii. predisposizione di note e prospetti informativi destinati al pubblico (e.g. resoconto intermedio di gestione, relazione finanziaria annuale, semestrale e trimestrale);
  - iii. predisposizione, aggiornamento e diffusione del Piano Industriale;

#### **C) Operazioni societarie, gestione del capitale ed esercizio dei diritti sociali**

8. gestione delle operazioni di mercato relative agli strumenti finanziari quotati emessi dalla Società (anche per il tramite di intermediari abilitati): attività di negoziazione in conto proprio; acquisto, vendita o altre operazioni compiute direttamente o indirettamente su di essi; nonché gestione del patrimonio aziendale, delle operazioni sul capitale sociale/straordinarie e relativi adempimenti;
9. regolamentazione e gestione dell'esercizio dei diritti sociali connessi alla proprietà delle azioni della Società e relativi adempimenti, con particolare riguardo alla maggiorazione del diritto di voto e alla formazione/comunicazione di patti parasociali;
10. gestione delle operazioni di *internal dealing* e relativi adempimenti;
11. gestione delle operazioni con parti correlate e relativi adempimenti.

Sono altresì state individuate altre Attività Sensibili relative ai **processi strumentali** e strettamente connessi ovvero funzionali agli ambiti operativi su indicati, e segnatamente:

12. instaurazione e sviluppo dei rapporti commerciali;
13. gestione dei rapporti con gli organi di controllo e con la Società di revisione, nonché degli adempimenti societari;
14. gestione delle risorse finanziarie/flussi finanziari e tenuta della contabilità generale;
15. approvvigionamento di beni, servizi, consulenze ed incarichi professionali.

### **1.3 PROTOCOLLI PER MITIGARE IL RISCHIO**

Tutte le attività a rischio sono svolte conformandosi rigorosamente alla legislazione e alla normativa secondaria (regolamenti, linee guida e orientamenti di fonte Consob ed ESMA), sia nazionali che europee, vigenti in materia di gestione/negoziazione degli strumenti finanziari quotati e di prevenzione dei *market abuse*, al Regolamento dei mercati organizzati e gestiti da Borsa Italiana S.p.A. e, ancora, ai canoni e alle raccomandazioni dettati dal Codice di autodisciplina delle società quotate, nonché seguendo lo Statuto

sociale, i principi, le procedure ed i Protocolli aziendali, Generici e Specifici, di cui al presente Modello.

- **Protocolli Generici**

In linea con quanto sopra riportato, la Società ha adottato ed ha debitamente formalizzato e divulgato al proprio interno i seguenti protocolli generici, soggetti a periodico aggiornamento:

- Sistema di deleghe e procure con relativi limiti di spesa;
- Principi di comportamento descritti nel Codice Etico (con particolare riguardo ai principi e alle regole di condotta previsti agli artt. 12, 15, 16, 17, 18, 19, 20, 23, 24 e 25 del Codice);
- Formazione del personale;
- Organigramma aziendale e ordinamento organizzativo;
- Sistema sanzionatorio e disciplinare;
- Procedura *Whistleblowing*.

Inoltre, per la medesima finalità, rilevano i seguenti presidi:

- Controllo svolto dal Collegio Sindacale;
- Controllo svolto dalla Società di Revisione;
- Controllo svolto dalla Funzione di *Compliance*;
- Controllo svolto dalla Funzione di *Internal Audit*;
- Controllo svolta dalla Funzione di *Risk Management*;
- Supporto del Comitato Controllo, Rischi e Sostenibilità al Consiglio di Amministrazione nelle valutazioni e decisioni relative al sistema di controllo interno e di gestione dei rischi e all'approvazione delle relazioni periodiche di carattere finanziario e non finanziario, nonché nella promozione della continua integrazione delle *best practice* nazionali e internazionali nella *corporate governance* della Società e dei fattori ambientali, sociali e di *governance* nelle strategie aziendali volte al perseguimento del successo sostenibile. Ad esso sono state attribuite anche le funzioni di comitato per le operazioni con parti correlate, fatta eccezione per le decisioni relative ad operazioni aventi a oggetto le remunerazioni degli amministratori e dei dirigenti con responsabilità strategiche;
- Supporto del Comitato Nomine e Remunerazione al Consiglio di Amministrazione nell'elaborazione della politica di remunerazione, nel monitorare la concreta applicazione di tale politica e nel verificare l'effettivo raggiungimento degli obiettivi di *performance*, nonché nell'autovalutazione del Consiglio stesso e dei suoi comitati, nella definizione della loro composizione ottimale e nell'individuazione di una lista per l'elezione dell'organo amministrativo, secondo modalità che ne assicurino una formazione e una presentazione trasparente.

- **Protocolli Specifici**

I Protocolli Specifici di Generalfinance si basano sui principi generali di controllo e sui presidi preventivo-organizzativi di seguito indicati:

- 1) separazione dei compiti: si richiede l'applicazione del principio di segregazione delle attività tra chi autorizza, chi esegue e chi controlla (segregazione di funzioni);
- 2) esistenza di procedure formalizzate: devono esistere disposizioni aziendali e/o procedure formalizzate, idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili, nonché modalità di archiviazione della documentazione rilevante, in ossequio

alla normativa, primaria e secondaria, nazionale ed euro-unitaria e alle *best practice* vigenti in tema di prevenzione dei *market abuse*;

- 3) esistenza di un sistema di deleghe e procure coerente con le responsabilità organizzative assegnate: nell'ambito delle disposizioni aziendali e/o procedure formalizzate, i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere definiti e conosciuti all'interno della società;
- 4) tracciabilità e verificabilità ex post delle comunicazioni/operazioni/transazioni tramite adeguati supporti documentali/informatici: ogni comunicazione/operazione/transazione relativa all'area a rischio 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 comunicazioni/operazioni/registrazioni effettuate;
- 5) elaborazione e implementazione di misure organizzative di sicurezza logica e fisica atte a garantire la corretta gestione delle Informazioni Specifiche Rilevanti e di quelle Privilegiate sia all'interno che all'esterno della Società, oltre che di misure finalizzate al monitoraggio di situazioni che possono dare origine a conflitti di interesse e all'eventuale imposizione di ulteriori e specifiche restrizioni al compimento di determinate operazioni;
- 6) previsione, tramite apposite clausole contrattuali, di specifici obblighi di riservatezza a carico di outsourcer/consulenti/fornitori che, in virtù dell'attività professionale prestata, possano venire a conoscenza di Informazioni Specifiche Rilevanti e/o Informazioni Privilegiate;
- 7) svolgimento di controlli ex post ovvero contemporaneamente sull'andamento dei titoli azionari di Generalfinance nelle giornate di mercato, finalizzati a rilevare/segnalare eventuali profili di criticità;
- 8) istituzionalizzazione e designazione di figure e funzioni organizzative aziendali specializzate, deputate a gestire i principali processi afferenti alle aree esposte al rischio di verifica dei fenomeni di *market abuse* (*i.e.* la gestione delle Informazioni Privilegiate e la gestione delle *c.d. Investor Relations*, dei rapporti con la comunità finanziaria e Borsa Italiana), ad implementare e garantire la corretta applicazione delle regole procedurali e di condotta adottate dalla Società per la mitigazione del rischio, in *compliance* con la normativa, primaria e secondaria, nazionale ed euro-unitaria e le *best practice* vigenti in materia.

Trattasi, in particolare, delle seguenti figure:

- **Referente Informativo (e suo sostituto)** che, nominato ai sensi dell'art. 2.6.1 del Regolamento dei Mercati organizzati e gestiti da Borsa Italiana, rappresenta il soggetto a cui quest'ultima può rivolgersi per ottenere informazioni su Generalfinance ritenute utili per il buon funzionamento del mercato oppure per richiedere la diffusione di dati o notizie necessari alla corretta informazione del mercato;
  - **Investor Relator**: è il soggetto incaricato da Generalfinance di curare la tenuta dei rapporti con gli investitori, coadiuvando l'Amministratore Delegato nel dialogo con i soggetti interessati per i quali rappresenta il primo punto di contatto;
  - **Funzione Gestione Informazioni Privilegiate (FGIP)** la quale è responsabile dell'adempimento degli incombeni connessi agli obblighi normativi in materia di gestione delle Specifiche Informazioni Rilevanti e/o delle Informazioni Privilegiate, alla tenuta del Registro delle Persone Informate e del Registro delle Specifiche Informazioni Rilevanti e delle persone che hanno accesso alle medesime (*Relevant Information List – RIL*).
- Inoltre, e con particolare riguardo alla tutela della trasparenza dell'informazione finanziaria, si

segnala che Generalfinance ha nominato, ai sensi dell'art. 154-bis del TUF:

- o il **Dirigente preposto alla redazione dei documenti contabili societari**, cui spetta la responsabilità del sistema di controllo interno in materia di informativa finanziaria che si traduce, inter alia, nell'attestazione della corrispondenza degli atti e delle comunicazioni di Generalfinance diffusi al mercato, concernenti l'informativa contabile (anche infra-annuale) della Società, alle risultanze documentali, ai libri e alle scritture contabili della stessa (cfr., al riguardo, par. 3.3. della Parte Generale del Modello).

Oltre ai Protocolli Generici, la Società ha sviluppato e implementato i seguenti Protocolli Specifici per la prevenzione e la riduzione del rischio di realizzazione dei delitti di *market abuse* e delle condotte ad essi strumentali/propedeutiche:

#### **A) Informazioni Rilevanti e/o Privilegiate e comunicazioni esterne**

- **Codice per il trattamento delle Informazioni Privilegiate:** obiettivo del Codice è quello di disciplinare l'individuazione, la gestione e il trattamento delle Informazioni Privilegiate riguardanti la Società, enucleando le regole operative e di condotta da osservare nella tenuta e nella comunicazione di dette informazioni, sia all'interno che all'esterno del contesto aziendale. In particolare, il Codice identifica: (i) le informazioni che devono essere qualificate come privilegiate; (ii) i soggetti destinatari della normativa e i responsabili delle attività di elaborazione e divulgazione dei dati rilevanti; (iii) le modalità di diffusione e di comunicazione al mercato delle Informazioni Privilegiate, con particolare riguardo all'elaborazione/pubblicazione dei comunicati stampa, all'utilizzo dello SDIR e all'aggiornamento del sito *web* istituzionale; (iv) l'iter da osservare per l'attivazione della procedura del ritardo nella comunicazione al pubblico e la verifica della sussistenza della condizioni legittimanti lo stesso, con conseguente obbligo di informarne per iscritto la Consob e di trasmettere all'Autorità, previa richiesta espressa di quest'ultima, la documentazione comprovante la spiegazione delle modalità con cui sono state soddisfatte le condizioni previste per il ritardo; (v) la realizzazione dei sondaggi di mercato; nonché (vi) i principi di comportamento cui devono attenersi tutti i soggetti e le strutture organizzative aziendali a vario titolo coinvolti nel trattamento delle Informazioni Privilegiate e delle informazioni riservate.

In tal senso, viene analiticamente disciplinata l'istituzione e la gestione del registro delle persone che hanno accesso alle Informazioni Privilegiate (il c.d. *Registro Insider*), mediante: (i) l'identificazione dei soggetti responsabili della tenuta del predetto Registro; (ii) i criteri per l'individuazione delle persone da iscriverci; (iii) il contenuto e la notifica della loro iscrizione; (iv) le modalità, il funzionamento e l'aggiornamento del Registro. Il Codice prevede, inoltre, l'istituzione del Registro delle persone che hanno accesso a specifiche Informazioni Rilevanti che, sulla base di una valutazione in concreto, hanno una sufficiente probabilità di divenire, in un secondo momento, Informazioni Privilegiate.

- **Politica per la gestione del dialogo con gli azionisti e gli altri soggetti interessati** che regola le modalità di svolgimento del rapporto dialettico e istituzionale tra i soggetti interessati all'operatività/andamento aziendale (ad esempio, gli azionisti, i titolari o portatori di altri strumenti finanziari emessi da Generalfinance, gli investitori istituzionali attuali e potenziali, i gestori di attivi, gli operatori del mercato finanziario, gli analisti finanziari, i *proxy advisor* e le agenzie di *rating*) e la Società su materie/tematiche di competenza del Consiglio di Amministrazione al di fuori dell'informativa resa e delle interlocuzioni instaurate con gli azionisti in relazione e/o in occasione delle Assemblee. In tal senso, il documento definisce: (i) i referenti aziendali che svolgono tali attività (principalmente il CEO, coadiuvato dal CFO e *Investor Relator*); (ii) il ruolo di indirizzo, supervisione e monitoraggio che esercita il Consiglio di Amministrazione; (iii) gli argomenti, i contenuti e le



tempistiche dei dialoghi con i soggetti interessati, affinché la divulgazione delle informazioni relative alla Società sia rispettosa degli obblighi normativi, con particolare riferimento ai divieti di comunicazione selettiva delle Informazioni Privilegiate.

Fra le altre cose, la Politica stabilisce che il dialogo con tali soggetti non può aver luogo durante i c.d. *black-out period*, ossia nei 30 giorni precedenti la riunione del Consiglio di Amministrazione chiamato ad approvare le relazioni finanziarie intermedie e le relazioni finanziarie di fine anno che la Società è tenuta a pubblicare ai sensi delle disposizioni normative o delle regole della sede di negoziazione delle azioni sociali.

## **B) Pianificazione strategico-finanziaria, comunicazioni sociali e informativa societaria**

- **Procedura gestione della contabilità e redazione del bilancio fiscale (Policy redazione bilancio di esercizio):** obiettivo della procedura è la definizione di regole di condotta e operative che indichino i comportamenti cui i Destinatari devono attenersi nella gestione dei processi legati alla tenuta della contabilità, alla redazione del bilancio, nonché di tutte quelle attività connesse alla pianificazione strategica, alla predisposizione del *budget* e al controllo di gestione, al fine di tutelare la solidità, la trasparenza e la correttezza dell'informazione societaria.
- **Regolamento in materia di Pianificazione e di Controllo di Gestione** che descrive e detta le regole del processo di pianificazione e controllo di gestione di cui la Società si è dotata per supportare adeguatamente le decisioni operative e strategiche attraverso strumenti di misurazione dell'efficacia e dell'efficienza, e in particolare: piani, documenti di programmazione, indicatori di *performance*, contabilità analitica, sistema di *reporting* interno, bilancio consolidato e bilancio sociale.
- **Manuale Metodologico (Governance 262/05) - Regolamento del Dirigente Preposto** che è volto a descrivere e definire le linee guida e la prassi operativa che la struttura organizzativa aziendale deve seguire per presidiare e neutralizzare il rischio di errata informativa finanziaria, prevedendo controlli interni a livello societario, controlli dei processi amministrativo-finanziari e controlli sul governo dei sistemi e degli strumenti informativi che compongono la struttura e l'infrastruttura informatiche di Generalfinance .
- **Regolamento in materia di redazione dell'Informativa al pubblico di "Terzo Pilastro":** scopo del Regolamento aziendale è quello di definire e di formalizzare le modalità che la Società deve adottare per la predisposizione dell'Informativa di Terzo Pilastro – la quale ha ad oggetto l'adeguatezza patrimoniale della Società, la sua esposizione ai rischi e le caratteristiche generali dei sistemi interni di gestione e controllo ed è prevista dal Regolamento (UE) 575/2013 (CRR) – nonché di individuare le responsabilità delle funzioni preposte alla predisposizione della stessa.
- **Policy di Governance del Processo ICAAP:** obiettivo della *Policy* è quello di documentare e formalizzare il processo di controllo prudenziale (ovverosia: il processo ICAAP) mediante il quale la Società compie una valutazione, sia attuale che prospettica, della propria adeguatezza patrimoniale tenendo in considerazione: i) i rischi assunti nello svolgimento della propria attività; ii) gli obiettivi strategici; iii) la struttura di governo e controllo; iv) il sistema di gestione dei rischi; v) le variabili di contesto. In essa sono, altresì, definiti ruoli e responsabilità degli organi e delle funzioni aziendali coinvolti nella gestione dei rischi e le metodologie di valutazione dell'esposizione.  
La Società trasmette annualmente alla Banca d'Italia, entro il 30 aprile, la rendicontazione ICAAP riferita al 31 dicembre dell'anno precedente.
- **Policy in materia di classificazione e valutazione delle esposizioni creditizie:** scopo della *Policy* è quello di formalizzare e definire le scelte operative e i processi preordinati ad una corretta

classificazione e valutazione delle esposizioni creditizie della Società, conformemente a quanto stabilito sia dalla normativa di Vigilanza sia dal principio contabile IFRS 9, il quale fissa le regole relative alla classificazione ed alla misurazione degli strumenti finanziari, sempre nella prospettiva di garantire la solidità e la correttezza dell'informativa finanziaria.

### **C) Operazioni societarie, gestione del capitale ed esercizio dei diritti sociali**

- **Codice di Comportamento in materia di *internal dealing*:** il Codice ha lo scopo di dare attuazione alle disposizioni europee e nazionali applicabili in materia di obblighi di comunicazione al pubblico e alla Consob – oltre che alla Società stessa – di operazioni concernenti strumenti finanziari o strumenti finanziari collegati (incluse quelle di acquisto, vendita, sottoscrizione o scambio degli stessi) realizzate nell'ambito societario da parte di determinati soggetti, e segnatamente: gli azionisti che detengono una partecipazione pari almeno al 10% del capitale sociale, i componenti del Consiglio di Amministrazione e del Collegio Sindacale, il *top management*, nonché le persone fisiche e giuridiche ad essi strettamente legate.

Oltre a fissare (i) gli obblighi di comunicazione dei soggetti rilevanti, degli azionisti rilevanti e delle persone strettamente legate in merito alla realizzazione delle predette operazioni, (ii) le modalità e le tempistiche di notifica, nonché (iii) la funzione aziendale preposta a garantire l'osservanza delle regole ivi previste, il Codice fissa i divieti al compimento delle operazioni in questione (con particolare riguardo ai c.d. *black out period*) e la possibilità di porre ulteriori divieti/limitazioni ad opera del Consiglio di Amministrazione.

- **Regolamento del voto maggiorato** che delinea la disciplina di dettaglio sul voto maggiorato, prevedendo, in particolare, le modalità di iscrizione, tenuta e aggiornamento dell'elenco in cui sono iscritti i titolari del diritto reale legittimante che hanno chiesto la maggiorazione del voto (c.d. Elenco Speciale), nel rispetto della normativa applicabile, in modo da assicurare il tempestivo scambio di informazioni tra gli azionisti di Generalfinance, la Società stessa e gli intermediari abilitati alla tenuta dei conti sui quali sono registrate le azioni. Inoltre, il Regolamento fissa gli obblighi di comunicazione verso il pubblico e la Consob a cui la Società deve periodicamente adempiere, avendo riguardo ai dati identificativi degli azionisti che richiedono l'iscrizione nell'Elenco Speciale e l'ammontare complessivo dei diritti di voto.
- **Procedura per le operazioni con parti correlate:** la procedura dispone le condizioni e le modalità di istruzione e realizzazione/approvazione di operazioni con parti correlate da parte della Società, ai sensi dell'art. 2391-*bis* c.c. e in conformità alla normativa primaria (europea e nazionale) e a quella regolamentare emanata dalla Consob, distinguendo tra operazioni di minore rilevanza e quelle di maggiore rilevanza e prevedendo altresì (i) l'istituzione di un registro nel quale vengono iscritte le parti correlate e, soprattutto, (ii) gli obblighi di comunicazione al pubblico e alla Consob che devono essere puntualmente assolti dalla Società; unitamente al **Regolamento del Comitato Controllo, Rischi e Sostenibilità** laddove sancisce, in senso analogo alla Procedura, che il Comitato deve esprimere il proprio parere (motivato e non vincolante) prima che l'organo competente (Assemblea, Consiglio di Amministrazione o Dirigente con responsabilità strategiche) approvi il compimento di operazioni poste in essere dalla Società, anche per il tramite di entità da essa controllate, con parti correlate, pronunciandosi sull'interesse della Società alla singola operazione e sulla convenienza e correttezza sostanziale delle condizioni previste dalla normativa.
- **Politica di remunerazione** che stabilisce i principi e le linee guida sulla base dei quali sono determinati i compensi fissi e variabili (ancorati a componenti di breve e lungo termine) dei membri del Consiglio

di Amministrazione, dell'organo di controllo e dei Dirigenti con Responsabilità Strategiche, oltre che i benefici non monetari e i piani di incentivazione basati su strumenti finanziari diversi dalle *stock option*; unitamente al **Regolamento del Comitato Nomine e Remunerazione** che svolge funzioni istruttorie, propositive e consultive nei confronti del Consiglio di Amministrazione in materia di remunerazione degli amministratori, dei sindaci e del *top management* e, ancora, in merito alla composizione e dimensione del Consiglio stesso, mediante la formulazione di pareri, raccomandazioni e proposte.

#### **D) Attività strumentali**

- **Procedura gestione dei rapporti con i soci e con gli organi di controllo:** obiettivo della procedura è la definizione di regole di condotta e operative che indichino i comportamenti cui i Destinatari devono attenersi nelle attività connesse con la gestione dei rapporti con i soci e gli organi di controllo societario.
- **Procedura gestione della tesoreria** che ha come scopo la definizione di regole di condotta e procedurali che indichino i comportamenti cui i Destinatari devono attenersi nell'ambito dei processi connessi all'amministrazione della tesoreria aziendale e, in particolare, degli investimenti e disinvestimenti, degli affidamenti bancari e approvvigionamenti, della gestione della liquidità, nonché della gestione amministrativa di incassi e pagamenti.
- **Procedura per la gestione dei flussi finanziari (Regolamento tracciabilità flussi finanziari)**, volta a formalizzare e definire le scelte operative e i processi interni preordinati al rispetto delle norme in materia di tracciabilità dei flussi finanziari con particolare riferimento al pagamento dei crediti che hanno formato oggetto di cessione a favore di Generalfinance, in considerazione del *core business* societario.
- **Procedura approvvigionamento di beni, servizi, consulenze ed incarichi professionali:** obiettivo della procedura è la definizione di regole di condotta e procedurali che indichino i comportamenti cui i Destinatari devono attenersi nella gestione del processo di approvvigionamento in tutte le sue fasi.
- **Clausole Contrattuali 231:** il Protocollo ha l'obiettivo di disciplinare le attività di redazione dei contratti con le terze parti, allo scopo di evitare che, nella prestazione dei servizi contrattualizzati, possano essere commessi i Reati di cui al Decreto.

**Per quanto attiene alla gestione dei rapporti con l'Autorità di Vigilanza trovano applicazione gli ulteriori Protocolli Specifici contemplati nella Parte Speciale I – “Reati Corruttivi”.**

**Con riguardo all'utilizzo dei sistemi e degli strumenti informatici e telematici (sia interni che esterni alla Società) nell'ambito delle attività sensibili si osservano, altresì, i Protocolli Specifici richiamati dalla Parte Speciale IV – “Reati Informatici”.**

#### **1.4 CONTROLLI DELL'ORGANISMO DI VIGILANZA**

L'Organismo di Vigilanza esegue verifiche periodiche con riguardo alle specifiche attività sensibili di cui alla presente Parte Speciale secondo le seguenti modalità: (i) attenendosi alla programmazione da esso prevista nel piano di attività elaborato per ciascun anno di riferimento ovvero (ii) a campione, qualora la verifica non sia ricompresa all'interno del piano annuale di attività, ma l'OdV la ritenga comunque necessaria (ad esempio, verifica a campione in ordine al processo di gestione e tenuta del Registro delle Persone Informate).

#### **1.5 FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA**



La funzione aziendale nella cui competenza ricade la gestione dell'Attività Sensibile dà apposita evidenza documentale di ogni attività a rischio, secondo quanto previsto dalla specifica procedura operativa applicabile. A seconda dell'attività, la funzione competente dovrà effettuare i controlli definiti nella procedura e, in caso di anomalia, inviare all'Organismo di Vigilanza le opportune segnalazioni e i flussi informativi richiesti.

In ogni caso, le funzioni aziendali nella cui competenza rientra l'attività a rischio dovranno informare l'Organismo di Vigilanza in merito:

- alla realizzazione di operazioni straordinarie, sul capitale e/o su strumenti finanziari;
- alla realizzazione di operazioni di *internal dealing* e a quelle con parti correlate;
- al bilancio annuale, corredato della nota integrativa, nonché ad ogni altra informativa diretta al pubblico concernente la situazione economica, finanziaria e patrimoniale della Società;
- alle comunicazioni, da parte del Collegio Sindacale e della Società di Revisione, relative ad ogni criticità emersa, anche se risolta;
- all'avvio, agli sviluppi e agli esiti di procedimenti di verifica e/o sanzionatori a cura della Consob;
- alle decisioni prese in qualsiasi ambito all'interno della struttura organizzativa che non abbiano seguito il normale *iter* autorizzativo previsto dalle procedure interne;
- alle criticità emerse nella gestione delle attività sensibili e che potrebbero rilevare ai sensi del Decreto (a mero titolo esemplificativo, anomalie riguardanti la tenuta dei registri previsti dalle procedure interne sopra richiamate ovvero evidenze di operazioni sospette).