



Compagnia Privata

Modello 231

**Modello di organizzazione, gestione e controllo ex D.Lgs. 8 giugno 2001 n. 231
di Compagnia Privata SIM S.p.A.**

*(Approvato, nella presente versione, dal Consiglio di Amministrazione con delibera del 26
settembre 2025)*

INDICE

DEFINIZIONI.....	6
CAPITOLO 1 IL DECRETO LEGISLATIVO N. 231/2001.....	8
1.1 Il Decreto Legislativo n. 231/2001 e la normativa di riferimento.....	8
1.2 Presupposti di esclusione della responsabilità dell'ente.....	9
CAPITOLO 2 – LE LINEE GUIDA DI CONFINDUSTRIA.....	11
2.1 Individuazione dei rischi e protocolli	11
2.2 Il “sistema di controllo preventivo”	11
CAPITOLO 3 – ADOZIONE DEL MODELLO DA PARTE DI COMPAGNIA PRIVATA	13
3.1 La Società	13
3.2 Il Codice Etico	13
3.3 Adozione del Modello	13
3.4 Funzione e scopo del Modello.....	14
3.5 Caratteristiche del Modello.....	14
3.6 La costruzione del Modello e la sua struttura	15
3.7 I principi ispiratori del Modello.....	16
3.8 Destinatari del Modello	19
3.9 Assetto organizzativo e contratti di <i>outsourcing</i>	20
3.10 Impianto procedurale	20
CAPITOLO 4 – L'ORGANISMO DI VIGILANZA	21
4.1 Identificazione dell'Organismo di Vigilanza.....	21
4.2 Durata in carica	23
4.3 Funzione, poteri e compiti dell'Organismo di Vigilanza	24
4.4 Flussi informativi dell'OdV verso il vertice aziendale.....	25
4.5 Flussi informativi verso l'OdV: informazioni di carattere generale e informazioni specifiche obbligatorie. Il sistema di <i>whistleblowing</i>	26
4.6 Raccolta e conservazione delle informazioni	29
4.7 Verifiche sull'adeguatezza del Modello	29
CAPITOLO 5 – FORMAZIONE E DIFFUSIONE DEL MODELLO	30
5.1 Formazione e informazione degli Organi Sociali e dei Dipendenti	30
5.2 Selezione ed informazione dei Consulenti, dei Fornitori e dei <i>Partner</i>	31
CAPITOLO 6 – SISTEMA DISCIPLINARE.....	32
6.1 principi generali	32
6.2 Misure nei confronti dei Dipendenti.....	32
6.3 Misure nei confronti degli Amministratori	34
6.4 Misure nei confronti dei Sindaci	34
6.5 Misure nei confronti dei Consulenti, dei Fornitori e dei <i>Partner</i>	34
6.6 Misure nei confronti dei componenti dell'OdV	35
PARTI SPECIALI.....	36
PARTE SPECIALE – I – Reati nei rapporti con la Pubblica Amministrazione e Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	37
CAPITOLO I.1 - LE FATTISPECIE DI REATO.....	38
CAPITOLO I.2 - CRITERI PER LA DEFINIZIONE DI P.A. E DI SOGGETTI INCARICATI DI UN PUBBLICO SERVIZIO.	45
I.2.1 Enti della pubblica amministrazione	45
I.2.2 Pubblici Ufficiali	46

I.2.3 Incaricati di un pubblico servizio	47
CAPITOLO I.3 – LE ATTIVITÀ SENSIBILI NEI RAPPORTI CON LA P.A.	49
I.3.1 Attività Sensibili nei rapporti con la P.A.	49
I.3.2 Attività Strumentali alla commissione di reati di tipo corruttivo	49
CAPITOLO I.4 - PRINCÌPI GENERALI DI COMPORTAMENTO	50
I.4.1 Il sistema in linea generale	50
I.4.2 Il sistema di deleghe e procure	50
I.4.3 Principi generali di comportamento	51
CAPITOLO I.5 - PRINCÌPI SPECIFICI DI COMPORTAMENTO	55
CAPITOLO I.6 – FLUSSI INFORMATIVI NEI CONFRONTI DELL’ORGANISMO DI VIGILANZA	66
PARTE SPECIALE – II – Reati Societari (ivi inclusi i Reati di corruzione tra privati)	67
CAPITOLO II.1 - LE FATTISPECIE DI REATO	68
II.1.1 Le ipotesi di falsità	68
II.1.2 La tutela del capitale sociale	68
B.1.3 La tutela del corretto funzionamento della società	70
II.1.4 La tutela penale contro le frodi	71
II.1.5 La corruzione tra privati (art. 2635 c.c.)	71
II.1.6 Istigazione alla corruzione tra privati (art. 2635-bis c.c.)	72
CAPITOLO II.2.1 – LE ATTIVITÀ SENSIBILI NELL’AMBITO DEI REATI SOCIETARI	74
CAPITOLO II.2.2 – LE ATTIVITÀ SENSIBILI E STRUMENTALI NELL’AMBITO DEI REATI DI CORRUZIONE TRA PRIVATI	75
II.3.1 Il sistema in linea generale	76
CAPITOLO II.3.1 - PRINCÌPI GENERALI DI COMPORTAMENTO	77
CAPITOLO II.4.1 - PRINCÌPI SPECIFICI DI COMPORTAMENTO IN RELAZIONE AI REATI SOCIETARI	80
CAPITOLO II.4.2 - PRINCÌPI SPECIFICI DI COMPORTAMENTO IN RELAZIONE ALLE FATTISPECIE DI CORRUZIONE TRA PRIVATI	85
CAPITOLO II.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL’ORGANISMO DI VIGILANZA	92
PARTE SPECIALE – III – Reati e illeciti amministrativi riconducibili ad abusi di mercato	93
CAPITOLO III.1 - LE FATTISPECIE DI REATO	94
III.1.1 La definizione di “informazione privilegiata”	94
III.1.2 I reati di abuso di mercato	96
III.1.3 Gli illeciti amministrativi ex art. 187- <i>quinqies</i> del TUF	97
CAPITOLO III.2 – LE ATTIVITÀ SENSIBILI IN RELAZIONE AI REATI DI ABUSO DI MERCATO ...	99
CAPITOLO III.3 – PRINCÌPI GENERALI DI COMPORTAMENTO	100
CAPITOLO III.4 – PRINCÌPI SPECIFICI DI COMPORTAMENTO	101
CAPITOLO III.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL’ORGANISMO DI VIGILANZA .	105

PARTE SPECIALE – IV – Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio, reati aventi finalità di terrorismo e trasferimento fraudolento di valori	106
CAPITOLO IV.1 - LE FATTISPECIE DI REATO	107
IV.1.1 Le fattispecie dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio	107
IV.1.2 I delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori	112
IV.1.3 I delitti con finalità di terrorismo	113
CAPITOLO IV.2 – LE ATTIVITÀ SENSIBILI	117
CAPITOLO IV.3 - PRINCIPI GENERALI DI COMPORTAMENTO	118
IV.3.1 Il sistema in linea generale	118
CAPITOLO IV.4 – PRINCIPI SPECIFICI DI COMPORTAMENTO	121
CAPITOLO IV.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA. 129	
PARTE SPECIALE – V – Delitti di criminalità organizzata e reati transnazionali.....	130
CAPITOLO V.1 - LE FATTISPECIE DEI REATO	131
CAPITOLO V.2 – LE ATTIVITÀ SENSIBILI IN RELAZIONE AI REATI DI CRIMINALITÀ ORGANIZZATA.....	133
CAPITOLO V.3 – PRINCIPI GENERALI DI COMPORTAMENTO	134
CAPITOLO V.4 – PRINCIPI SPECIFICI DI COMPORTAMENTO	135
CAPITOLO V.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA..	136
PARTE SPECIALE – VI – Reati di omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, impiego di cittadini di paesi terzi il cui soggiorno è irregolare, delitti contro la personalità individuale e reati ambientali ..	137
CAPITOLO VI.1 - LE FATTISPECIE DEI REATO	138
VI.1.1 Reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies del D.Lgs. 231/2001).....	138
VI.1.2 Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 25-duodecies del D.Lgs. 231/2001).....	139
VI.1.3 Intermediazione illecita e sfruttamento del lavoro (art. art. 25-quinquies del D.Lgs. 231/2001).....	140
VI.1.4 Reati ambientali (art. art. 25-undecies del D.Lgs. 231/2001).....	140
CAPITOLO VI.2 – LE ATTIVITÀ SENSIBILI	142
CAPITOLO VI.3 – PRINCIPI GENERALI DI COMPORTAMENTO.....	143
CAPITOLO E.4 – PRINCIPI SPECIFICI DI COMPORTAMENTO	145
CAPITOLO VI.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA. 149	
PARTE SPECIALE – VII – Delitti informatici e delitti in violazione del diritto d'autore	150
CAPITOLO VII.1 - LE FATTISPECIE DI REATO	151
VII.1.1 I delitti informatici	151

VII.1.2 I delitti in violazione del diritto d'autore	156
CAPITOLO VII.2 – LE ATTIVITÀ SENSIBILI IN RELAZIONE AI DELITTI INFORMATICI E IN VIOLAZIONE DEL DIRITTO D'AUTORE	159
CAPITOLO VII.3 – PRINCÌPI GENERALI DI COMPORTAMENTO	160
CAPITOLO VII.4 – PRINCÌPI SPECIFICI DI COMPORTAMENTO	162
CAPITOLO VII.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	168
PARTE SPECIALE – VIII – Reati tributari.....	169
CAPITOLO VIII.1 - LE FATTISPECIE DI REATO	170
CAPITOLO VIII.2 – LE ATTIVITÀ SENSIBILI NELL'AMBITO DEI REATI TRIBUTARI	173
CAPITOLO VIII.3 – PRINCÌPI GENERALI DI COMPORTAMENTO	174
CAPITOLO VIII.4 - PRINCÌPI SPECIFICI DI COMPORTAMENTO	176
CAPITOLO VIII.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	179

DEFINIZIONI

- Compagnia Privata o la Società o la SIM: Compagnia Privata Società di Intermediazione Mobiliare S.p.A., con sede legale in Piazza Filippo Meda, 1, 20121, Milano.
- Attività Sensibili: le attività svolte da Compagnia Privata nel cui ambito sussiste il rischio di commissione dei Reati.
- Consulenti: i soggetti che agiscono in nome e/o per conto di Compagnia Privata in forza di un contratto di mandato o di altro rapporto contrattuale di collaborazione.
- Destinatari: i Dipendenti, i collaboratori a qualunque titolo, gli Organi Sociali, i Consulenti, i Fornitori e i *Partner* di Compagnia Privata.
- Dipendenti: i soggetti aventi un rapporto di lavoro subordinato con Compagnia Privata o coloro che svolgono attività lavorativa per Compagnia Privata in forza di un contratto con la stessa (ivi compresi i dirigenti e gli stagisti).
- D.Lgs. 231/2001 o il Decreto o il Decreto 231: il Decreto Legislativo 8 giugno 2001, n. 231 e sue successive modifiche o integrazioni.
- Esponenti: gli amministratori di Compagnia Privata e gli amministratori e i dipendenti del Gruppo che svolgono attività per conto o nell'interesse di Compagnia Privata.
- Fornitori: tutti i fornitori di beni e servizi di Compagnia Privata.
- Legge sul Diritto d'Autore o L.A.: Legge 22 aprile 1941, n. 633 relativa alla protezione del diritto d'autore e di altri diritti connessi al suo esercizio.
- Linee Guida: le Linee Guida per la costruzione del modello di organizzazione, gestione e controllo ex D.Lgs. 231/2001 approvate da Confindustria in data 7 marzo 2002 e successive modifiche e integrazioni.
- Modello: il presente documento, vale a dire il modello di organizzazione, gestione e controllo previsto dal D.Lgs. 231/2001.
- Organi Sociali: il Consiglio di Amministrazione e il Collegio Sindacale di Compagnia Privata e i rispettivi membri.
- Organismo di Vigilanza od OdV: l'organismo interno di controllo di Compagnia Privata, preposto alla vigilanza sul funzionamento e sull'osservanza del Modello nonché alla rilevazione dell'opportunità di un suo aggiornamento.
- P.A.: la Pubblica Amministrazione, inclusi i pubblici ufficiali e gli incaricati di un pubblico servizio.
- Partner: le controparti contrattuali di Compagnia Privata, sia persone fisiche sia persone giuridiche, con cui la società addivenga ad una qualunque forma di collaborazione contrattualmente regolata (associazione temporanea d'impresa, *joint venture*, consorzi,



collaborazione in genere), ove destinati a cooperare con Compagnia Privata nell'ambito delle Attività Sensibili.

- Reati o Reati Presupposto: le fattispecie di reati (e illeciti amministrativi) ai quali si applica la disciplina prevista dal D.Lgs. 231/2001, anche a seguito di sue successive modificazioni ed integrazioni.
- TUF: il D.Lgs. 24 febbraio 1998, n. 58 recante il "*Testo Unico delle disposizioni in materia di intermediazione finanziaria*")

CAPITOLO 1 IL DECRETO LEGISLATIVO N. 231/2001

1.1 Il Decreto Legislativo n. 231/2001 e la normativa di riferimento

In data 8 giugno 2001 è stato emanato – in esecuzione della delega di cui all’art. 11 della legge 29 settembre 2000 n. 300 – il D.Lgs. 231/2001, entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali cui l'Italia ha aderito.

Il D.Lgs. 231/2001, recante la *“Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica”* ha introdotto per la prima volta in Italia la responsabilità in sede penale degli enti per alcuni reati commessi nell’interesse o a vantaggio degli stessi, da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell’ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso e, infine, da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati. Tale responsabilità si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto.

La nuova responsabilità introdotta dal Decreto 231 mira a coinvolgere nella punizione di taluni illeciti penali il patrimonio degli enti che abbiano tratto un interesse o un vantaggio dalla commissione dell’illecito. Per tutti gli illeciti commessi è sempre prevista l’applicazione di una sanzione pecuniaria; per i casi più gravi sono previste anche misure interdittive quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la Pubblica Amministrazione, l’interdizione dall’esercizio dell’attività, l’esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi.

Quanto alla tipologia di Reati destinati a comportare il suddetto regime di responsabilità amministrativa a carico degli Enti, il Decreto - nel suo testo originario - si riferiva ad una serie di reati commessi nei rapporti con la Pubblica Amministrazione. Nel corso degli anni una serie di interventi legislativi ha però ampliato il novero dei Reati ricomprendendovi numerose fattispecie previste nel nostro ordinamento.

Ad oggi, quindi, tra i c.d. reati presupposto sono contemplati:

- (i) i reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del Decreto);
- (ii) i reati di falsità in monete, in carte di pubblico credito e in valori di bollo e in strumenti o segni di riconoscimento (art. 25-*bis* del Decreto);
- (iii) alcune fattispecie di cd. reati societari (art. 25-*ter* del Decreto)
- (iv) i reati con finalità di terrorismo o di eversione dell’ordine democratico (art. 25-*quater* del Decreto);
- (v) i reati di pratiche di mutilazione degli organi genitali femminili (art. 25 *quater*-1 del Decreto);
- (vi) i reati contro la personalità individuale (art. 25-*quinqüies* del Decreto);

- (vii) i reati e gli illeciti amministrativi di abuso di mercato (art. 25-*sexies* del Decreto);
- (viii) reati transnazionali (introdotti dalla Legge 16 marzo 2006, n. 146);
- (ix) i reati di omicidio colposo e lesioni gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-*septies* del Decreto);
- (x) i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25-*octies* del Decreto);
- (xi) i delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-*octies*.1 c.p.);
- (xii) i delitti informatici e il trattamento illecito dei dati (art. 24-*bis* del Decreto);
- (xiii) i delitti di criminalità organizzata (art. 24-*ter* del Decreto);
- (xiv) i delitti contro l'industria e il commercio (art. 25 *bis*-1 del Decreto);
- (xv) i delitti in materia di violazione del diritto d'autore (art. 25-*novies* del Decreto);
- (xvi) l'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-*decies* del Decreto);
- (xvii) i reati ambientali (art. 25-*undecies* del Decreto);
- (xviii) l'impiego di cittadini di paesi terzi il cui permesso di soggiorno è irregolare (art. 25-*duodecies* del Decreto);
- (xix) i reati di razzismo e xenofobia (art. 25-*terdecies* del Decreto);
- (xx) i reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-*quaterdecies* del Decreto);
- (xxi) i reati tributari (art. 25-*quinqesdecies* del Decreto);
- (xxii) i reati di contrabbando (art. 25-*sexiesdecies* del Decreto);
- (xxiii) reati contro il patrimonio culturale (art. 25-*septiesdecies*);
- (xxiv) riciclaggio di beni culturali e devastazione e saccheggio di beni culturali paesaggistici (art. 25-*duodevicies*);
- (xxv) delitti contro gli animali.

1.2 Presupposti di esclusione della responsabilità dell'ente

Il D.Lgs. 231/2001 prevede, agli articoli 6 e 7, una forma di esonero dalla responsabilità qualora la società dimostri di aver adottato ed efficacemente attuato un Modello di organizzazione, gestione e controllo idoneo a prevenire la realizzazione dei cd. reati presupposto.

Il Modello deve rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito esiste la possibilità di commissione dei reati;

- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e sull'osservanza del Modello (ivi incluso un sistema di *whistleblowing*);
- introdurre un sistema disciplinare privato idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Ai fini dell'esonero da responsabilità, il D.Lgs. 231/2001 prevede altresì che:

1. la società abbia provveduto all'istituzione di un organo di controllo interno all'ente con il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello nonché di curarne l'aggiornamento (c.d. Organismo di Vigilanza);
2. l'organismo di controllo non sia colpevole di omessa o insufficiente vigilanza in merito all'attuazione e all'osservanza del Modello;
3. la società abbia predisposto un sistema di verifica periodica e di eventuale aggiornamento del Modello;
4. l'autore del reato abbia agito eludendo fraudolentemente le disposizioni del Modello.

Lo stesso Decreto dispone che il Modello può essere adottato, garantendo le esigenze di cui sopra, sulla base di codici di comportamento (quali le Linee Guida emanate da Confindustria) redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia.

CAPITOLO 2 – LE LINEE GUIDA DI CONFINDUSTRIA

2.1 Individuazione dei rischi e protocolli

Nella predisposizione del presente Modello, la Società si è ispirata anche ai principi di cui alle Linee Guida predisposte da Confindustria nella loro ultima versione di giugno 2021.

Gli elementi che le Linee Guida indicano come fondamentali nella costruzione del Modello sono riconducibili alle seguenti attività:

- individuazione delle Attività Sensibili, volta a verificare in quale area/settore aziendale sia possibile la realizzazione dei Reati;
- predisposizione di un sistema di controllo in grado di prevenire i rischi attraverso l'adozione di apposite procedure.

Le componenti più rilevanti del sistema di controllo sono individuate nei seguenti strumenti:

- il codice etico;
- sistema organizzativo;
- procedure aziendali;
- poteri autorizzativi e di firma;
- sistemi di controllo e gestione;
- comunicazione e formazione.

Le componenti del sistema di controllo devono essere ispirate ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- documentazione dei controlli;
- previsione di un adeguato sistema sanzionatorio;
- individuazione dei requisiti dell'Organismo di Vigilanza, riassumibili come segue:
 - a) autonomia e indipendenza;
 - b) professionalità;
 - c) continuità di azione.
- obblighi di informazione dell'Organismo di Vigilanza.

2.2 Il “sistema di controllo preventivo”

Le componenti principali del sistema di controllo preventivo ai fini esimenti dalla responsabilità ex D.Lgs. 231/2001 individuate da Confindustria sono:

a) per i reati di natura dolosa:

- l'adozione di un modello organizzativo;
- l'esistenza di un sistema organizzativo sufficientemente formalizzato e chiaro, soprattutto nella definizione dell'attribuzione delle responsabilità;
- l'esistenza di un *corpus* di procedure manuali ed informatiche tali da regolamentare lo svolgimento delle attività prevedendo gli opportuni punti di controllo;
- la previsione di specifici poteri autorizzativi e di firma assegnati in coerenza con le responsabilità organizzative e gestionali definite;
- la presenza di un sistema di controllo sulla gestione in grado di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità generale e/o particolare;
- la comunicazione al personale deve essere capillare, efficace, autorevole (cioè emessa da un livello adeguato), chiara e dettagliata, periodicamente ripetuta;
- lo svolgimento di attività di formazione del personale coinvolto nelle aree maggiormente esposte al rischio di commissione dei reati c.d. presupposto.

b) per i reati di omicidio colposo e lesioni personali colpose commessi con violazione delle norme di tutela della salute e sicurezza sul lavoro:

oltre a quelle già sopra menzionate, le componenti del sistema di controllo devono prevedere:

- lo svolgimento di attività di formazione e addestramento adeguati alle mansioni di ciascun lavoratore/operatore;
- la comunicazione ed il coinvolgimento di tutti i soggetti interessati per consentire consapevolezza ed impegno adeguati a tutti i livelli;
- l'armonizzazione della gestione operativa dei rischi per la salute e sicurezza sul lavoro con quella complessiva dei processi aziendali;
- la previsione di un sistema di monitoraggio della sicurezza le cui modalità e responsabilità devono essere stabilite contestualmente alla definizione delle modalità e responsabilità della gestione operativa.

Le componenti sopra descritte devono integrarsi in un unico complesso sistema che rispetti i seguenti principi di controllo:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione e transazione;
- applicazione del principio di separazione delle funzioni ("nessuno può gestire in autonomia un intero processo");
- documentazione (anche attraverso la redazione di verbali scritti) dei controlli effettuati.

CAPITOLO 3 – ADOZIONE DEL MODELLO DA PARTE DI COMPAGNIA PRIVATA

3.1 La Società

Compagnia Privata è una società costituita nel 1990, che ha sede legale in Milano, Piazza Filippo Meda n. 1, e ha per oggetto – da statuto sociale – *“l’esercizio dei servizi di investimento e dei servizi accessori di cui al D.Lgs. 24.2.1998 n. 58, art. 1, commi 5 e 6, senza detenzione, anche temporanea, di disponibilità liquide e strumenti finanziari della clientela e senza assunzione di rischi in proprio”*.

La Società è iscritta al n. 45 dell’apposito albo Consob ed è autorizzata allo svolgimento dei servizi di investimento ai sensi del D.Lgs. 24 febbraio 1998, n. 58 (“**TUF**”), con delibera Consob n. 11761 del 22.12.1998 (ex n. 5730 del 11 dicembre 1991). In particolare, Compagnia Privata può esercitare:

- esecuzione di ordini per conto dei clienti limitatamente alla sottoscrizione e compravendita di strumenti finanziari di propria emissione, con le seguenti limitazioni operative: senza detenzione, neanche temporanea, delle disponibilità liquide e degli strumenti finanziari della clientela e senza assunzione di rischi da parte della società stessa (Delibera n. 20439 del 15/05/2018);
- Gestione di portafogli, con le seguenti limitazioni operative: senza detenzione, neanche temporanea, delle disponibilità liquide e degli strumenti finanziari della clientela e senza assunzione di rischi da parte della società stessa (Delibera n. 20439 del 15/05/2018);
- Consulenza in materia di investimenti, con le seguenti limitazioni operative: senza detenzione, neanche temporanea, delle disponibilità liquide e degli strumenti finanziari della clientela e senza assunzione di rischi da parte della società stessa (Delibera n. 20439 del 15/05/2018).

Quale servizio rientrante nel novero dei “servizi accessori” di cui all’art. 1, comma 6, TUF, la Società esercita la ricerca in materia di investimenti, l’analisi finanziaria e altre forme di raccomandazione generale riguardanti operazioni relative a strumenti finanziari.

La Società è caratterizzata da una struttura organizzativa molto semplice e snella.

3.2 Il Codice Etico

La Società ha da tempo provveduto ad adottare un codice etico (il “**Codice Etico**”).

Il Codice Etico, parte integrante del Modello, forma con esso un *corpus* di norme interne che definiscono formalmente l’insieme dei valori etici, di integrità e trasparenza che ispirano la Società in ogni suo rapporto nonché nell’esercizio dei propri diritti, doveri e responsabilità.

Il Codice Etico della Società, che qui si intende integralmente richiamato, costituisce altresì un fondamento essenziale del Modello, le cui disposizioni si integrano con quanto in quest’ultimo sancito.

3.3 Adozione del Modello

Nell'ottica di adeguare il proprio sistema organizzativo alla *best practice* in essere in materia e di prevenire il rischio di commissione di Reati al proprio interno, la Società ha da molti anni adottato un Modello, di volta in volta aggiornandolo alle novità organizzative e normative intervenute.

La Società ha, inoltre, istituito un Organismo di Vigilanza cui è stato attribuito il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di curarne l'aggiornamento.

3.4 Funzione e scopo del Modello

La Società è sensibile alle aspettative del proprio azionista e degli *stakeholders* in quanto è consapevole del valore che agli stessi può derivare da un sistema di controllo interno idoneo a prevenire la commissione di Reati di cui al Decreto.

L'adozione e l'efficace attuazione del Modello migliorano il sistema di *corporate governance* della Società, in quanto limitano il rischio di commissione dei reati e aumentano le possibilità di beneficiare dell'esimente prevista dal D.Lgs. 231/2001; pertanto, scopo del presente Modello è la predisposizione di un sistema strutturato ed organico di prevenzione, dissuasione e controllo finalizzato alla riduzione del rischio di commissione dei Reati mediante l'individuazione delle Attività Sensibili e dei principi di comportamento che devono essere rispettati dai Destinatari.

Il Modello ha inoltre la finalità di:

- sensibilizzare tutti i Destinatari e diffondere a tutti i livelli della Società le regole comportamentali contenute nello stesso;
- determinare, in tutti coloro che operano in nome e per conto della Società nelle Attività Sensibili, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano disciplinare, penale e amministrativo nonché la consapevolezza di poter determinare – in caso di comportamenti non conformi alle prescrizioni del Modello e alle altre norme e procedure/regole aziendali (oltre che alla legge) – illeciti passibili di conseguenze penalmente rilevanti non solo per se stessi, ma anche per la Società;
- ribadire che tali forme di comportamento illecito sono fortemente condannate dalla Società in quanto (anche nel caso in cui la stessa fosse apparentemente in condizione di trarne vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etico-sociali cui la Società intende attenersi nell'espletamento della propria attività;
- consentire alla Società, grazie ad un'azione di monitoraggio sulle attività Sensibili, di intervenire tempestivamente per prevenire o contrastare la commissione dei Reati stessi.

3.5 Caratteristiche del Modello

Caratteristiche del presente Modello sono l'efficacia, la specificità e l'attualità.

L'efficacia

L'efficacia del Modello dipende dalla sua idoneità in concreto ad elaborare meccanismi di decisione e di controllo tali da eliminare – o quantomeno ridurre significativamente – il rischio di responsabilità da Reato. Tale idoneità è garantita dall'esistenza sia di meccanismi di controllo idonei a identificare le anomalie del sistema sia di strumenti di intervento tempestivo per contrastare efficacemente dette anomalie.

La specificità

La specificità del Modello ne determina l'efficacia:

1. specificità delle Attività Sensibili ex art. 6, comma 2, lett. a), D.Lgs. 231/2001, che impone una “mappatura” delle attività nel cui ambito possono essere commessi i reati;
2. specificità dei processi di formazione delle decisioni dell'ente e dei processi di attuazione nelle Attività Sensibili ex art. 6, comma 2, lett. b), D.Lgs. 231/2001.

L'attualità

Il Modello è idoneo a ridurre i rischi da Reato solo se costantemente adattato alla struttura e all'attività d'impresa, per questo motivo la disposizione di cui all'art. 6, D.Lgs. 231/2001 attribuisce all'Organismo di Vigilanza il compito di curare l'aggiornamento del Modello.

L'art. 7 del Decreto, invece, stabilisce che è necessaria una verifica periodica del Modello per una sua efficace attuazione; del pari si deve procedere ad una sua modifica allorquando siano scoperte violazioni oppure intervengano modifiche nell'attività o nella struttura organizzativa della società/ente.

3.6 La costruzione del Modello e la sua struttura

Si descrivono qui di seguito brevemente le fasi in cui si è articolato il lavoro di individuazione delle Attività Sensibili, sulle cui basi si è poi dato luogo alla predisposizione del Modello (e di cui si è tenuto conto – valutandone la tenuta e le eventuali necessità di modifica – anche in occasione dei successivi aggiornamenti del documento).

1. Identificazione delle Attività Sensibili ed Effettuazione della “Gap Analysis”

Obiettivo di questa fase è stata l'analisi del contesto aziendale, al fine di identificare in quale area/settore di attività e secondo quale modalità si possano realizzare i Reati.

L'identificazione delle cosiddette Attività Sensibili, al fine della loro corretta gestione, è stata attuata attraverso il previo esame della documentazione aziendale rilevante *ratione materiae* (statuto, verbali del Consiglio di Amministrazione, sistema di deleghe e procure, contratti principali con fornitori e consulenti, ecc.) e una serie di interviste con i soggetti chiave nell'ambito della struttura aziendale.

Dallo svolgimento di tale processo di analisi è stato possibile individuare, all'interno della struttura aziendale, una serie di Attività Sensibili maggiormente esposte al rischio astratto di commissione di uno dei Reati.

Successivamente a tale fase di indagine, si è proceduto a verificare le modalità di gestione e di controllo delle Attività Sensibili e la loro conformità ai principi di controllo interno comunemente accolti e sono state individuate le azioni di miglioramento da attuare al fine di pervenire alla definizione per la Società del Modello ex D.Lgs. 231/01.

2. Predisposizione del Modello.

Il presente Modello è costituito dai seguenti documenti:

- i. una “Parte Generale”, contenente l’insieme delle regole e dei principi generali dettati dal Modello;
- ii. n. 8 “Parti Speciali” predisposte per alcune categorie di Reato Presupposto ritenute astrattamente ipotizzabili in relazione all’attività svolta dalla Società a valle dell’analisi dei rischi, ossia:
 - Parte Speciale I – Reati commessi nei rapporti con la Pubblica Amministrazione e Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria;
 - Parte Speciale II – Reati societari (ivi inclusi i Reati di corruzione tra privati);
 - Parte Speciale III – Reati e illeciti amministrativi riconducibili ad abusi di mercato;
 - Parte Speciale IV – Reati di ricettazione riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio, reati aventi finalità di terrorismo e trasferimento fraudolento di valori;
 - Parte Speciale V – Delitti di criminalità organizzata e reati transnazionali;
 - Parte Speciale E – Reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, impiego di cittadini di paesi terzi il cui soggiorno è irregolare, delitti contro la personalità individuale e reati ambientali;
 - Parte Speciale VII – Delitti informatici e delitti in violazione del diritto d’autore;
 - Parte Speciale VIII – Reati tributari.

In particolare, ciascuna delle anzidette Parti Speciali ha la funzione di:

- a) identificare i principi comportamentali specifici che i Destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello e, in particolare, della limitazione del rischio di commissione della specifica tipologia di Reati da ognuna di esse considerato;
- b) fornire all’Organismo di Vigilanza e ai responsabili delle altre funzioni aziendali che con lo stesso cooperano, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica previste.

3.7 I principi ispiratori del Modello

Nella predisposizione del presente Modello si è tenuto conto del contenuto del sistema procedurale, della prassi aziendale e dei sistemi di controllo in essere presso la Società, ove considerati idonei a valere anche come misure di prevenzione dei Reati e strumenti di controllo sulle Attività Sensibili. Il Modello si pone, pertanto, quale ulteriore componente del sistema di controllo interno adottato dalla Società.

Il presente Modello non costituisce un “*quid novi*”: l’attività di impresa svolta dalla Società, infatti, è sin dalla costituzione caratterizzata da un proprio sistema (un modello), nonché da un assetto organizzativo consolidato. Per la Società si è trattato, quindi, di effettuare un’analisi delle strutture organizzative interne già attive e operanti, nonché dei presidi già in essere, per verificarne la rispondenza al dettato del Decreto ed eventualmente potenziarli.

In particolare, quali specifici strumenti già esistenti e diretti a programmare la formazione e l’attuazione delle decisioni della Società anche in relazione ai Reati da prevenire, la Società ha individuato i seguenti:

1. i principi di *corporate governance* generalmente seguiti dalla Società;
2. la documentazione e le disposizioni inerenti alla struttura gerarchico-funzionale aziendale e organizzativa della Società;
3. la normativa aziendale che la Società ha predisposto nell’ambito delle Attività Sensibili (ad esempio, la documentazione aziendale in materia di sicurezza sul lavoro);
4. la formazione del personale;
5. il sistema sanzionatorio di cui al CCNL.

Le regole, le procedure e i principi di cui agli strumenti sopra elencati – anche laddove non riportati dettagliatamente nel presente Modello – fanno parte del più ampio sistema di organizzazione e controllo che lo stesso intende integrare.

I principi cardine cui il Modello si ispira, oltre a quanto sopra indicato, sono:

1. le Linee Guida Confindustria e le *best practice* in materia, in base alle quali è stata predisposta la mappatura delle **Attività Sensibili** di Compagnia Privata;
2. i requisiti indicati dal D. Lgs. n. 231/2001, tra cui:
 - l’attribuzione a un **organismo di vigilanza** interno alla Società del compito di attuare in modo efficace e corretto il Modello anche attraverso il monitoraggio dei comportamenti aziendali ed il diritto ad una informazione costante sulle attività rilevanti ai fini del D. Lgs. n. 231/2001;
 - la messa a disposizione dell’organismo di vigilanza di **risorse aziendali** di numero e valore ragionevole e proporzionato ai compiti affidati allo stesso e ai risultati attesi e ragionevolmente ottenibili;
 - l’attività di **verifica del funzionamento** del Modello con conseguente aggiornamento periodico (controllo *ex post*);

- l'attività di **sensibilizzazione e diffusione** a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
3. i principi generali di un adeguato sistema di controllo interno e in particolare:
- la **verificabilità e documentabilità** di ogni operazione rilevante ai fini del D. Lgs. n. 231/2001 per consentire l'individuazione di precisi "punti" di responsabilità e della "motivazione" delle scelte stesse (la cosiddetta "*tracciabilità delle scelte*");
 - il rispetto dei principi della **separazione delle funzioni e segregazione dei ruoli** (la cosiddetta "*segregation of duties*");
 - la previsione che, nell'assumere decisioni, si prescinda da valutazioni meramente soggettive, facendosi invece riferimento, laddove possibile, a **criteri precostituiti** (la cosiddetta "*oggettivazione dei processi decisionali*");
 - la definizione di **poteri autorizzativi** coerenti con le responsabilità assegnate;
 - la previsione di **appositi flussi informativi nei confronti dell'Organismo di Vigilanza e da parte di questo nei confronti degli Organi Sociali**;
4. il sistema dei controlli interni, che monitora le aree in cui è maggiore il rischio di commissione dei Reati.

3.7.1. Il sistema di deleghe e procure

In linea di principio, il sistema di deleghe e procure deve essere caratterizzato da elementi di "sicurezza" ai fini della prevenzione dei Reati e, al contempo, consentire comunque la gestione efficiente dell'attività aziendale.

Si intende per "*delega*" quell'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative.

Si intende per "*procura*" il negozio giuridico unilaterale con cui la Società attribuisce dei poteri di rappresentanza nei confronti dei terzi.

Ai titolari di una funzione aziendale che necessitano, per lo svolgimento dei loro incarichi, di poteri di rappresentanza viene conferita una "*procura*" di estensione adeguata e coerente con le funzioni ed i poteri di gestione attribuiti al titolare attraverso la "*delega*".

a) Requisiti essenziali del sistema di deleghe

I requisiti essenziali del sistema di deleghe, ai fini di un'efficace prevenzione dei Reati sono i seguenti:

- a) tutti coloro (Dipendenti e Organi Sociali) che intrattengono per conto della Società rapporti con la P.A. devono essere formalmente individuati (tramite delega formale, *job description*, ecc.); le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;

- b) ciascuna delega deve definire in modo specifico e inequivoco:
- i poteri del delegato;
 - il soggetto (organo o individuo) cui il delegato riporta gerarchicamente o funzionalmente o *ex lege* o statutariamente;
- c) i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
- d) il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli.

b) Requisiti essenziali del sistema di procure

I requisiti essenziali del sistema di attribuzione delle **procure**, ai fini di un'efficace prevenzione dei Reati sono i seguenti:

- a) le procure funzionali sono conferite in conformità con il ruolo ricoperto dal soggetto procurato all'interno della Società e – laddove il contenuto delle stesse non fosse esaustivo – sono accompagnate da una lettera di istruzioni nella quale sono indicate le specifiche attività in relazione alle quali viene conferita la procura;
- b) le procure devono essere tempestivamente aggiornate in caso di assunzione di nuove responsabilità, trasferimento a diverse mansioni incompatibili con quelle per cui era stata conferita, dimissioni, licenziamento, ecc.;
- c) le procure che attribuiscono un potere di firma singola fissano limiti di spesa; sono, inoltre, accompagnate da apposita disposizione che fissi, oltre ai limiti di spesa, l'ambito nel quale può essere esercitato il potere di rappresentanza.

3.8 Destinatari del Modello

Le regole contenute nel presente Modello si rivolgono ai seguenti soggetti:

- a) persone che rivestono funzioni di rappresentanza, amministrazione o direzione della Società ivi compresi i componenti degli Organi Sociali;
- b) persone che esercitano, anche di fatto, la gestione e il controllo della Società stessa;
- c) i Dipendenti e, in ogni caso, i soggetti sottoposti alla direzione o alla vigilanza dei soggetti di cui sopra;
- d) limitatamente a quanto specificamente indicato nei relativi accordi contrattuali, ai Consulenti, Fornitori, *Partner* e, in genere, a tutti coloro che operano in nome o per conto o comunque nell'interesse della Società.

I contenuti del Modello sono comunicati ai Destinatari con modalità idonee ad assicurarne l'effettiva conoscenza, secondo quanto indicato al successivo Capitolo 5 della presente Parte Generale. I

Destinatari sono tenuti a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di correttezza e diligenza derivanti dal rapporto giuridico da essi instaurato con la Società.

3.9 Assetto organizzativo e contratti di *outsourcing*

Ai fini dell'attuazione del Modello, riveste fondamentale importanza l'assetto organizzativo della Società, in base al quale vengono individuate le strutture organizzative essenziali, le rispettive aree di competenza e le principali responsabilità alle stesse attribuite.

Qualora la Società si avvalga di servizi rilevanti svolti soggetti terzi, tali prestazioni devono essere disciplinate da un contratto scritto.

I contratti di *outsourcing* devono prevedere:

- 1) una descrizione dettagliata delle attività esternalizzate;
- 2) adeguati poteri di verifica e controllo spettanti alla Società;
- 3) le modalità di tariffazione dei servizi resi;
- 4) l'obbligo dell'*outsourcer*, quale Destinatario del Modello, di dare esecuzione all'attività nel rispetto delle previsioni del Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. n. 231/2001 adottato dalla Società;
- 5) la facoltà di risolvere il contratto tra le parti in caso di violazione dell'obbligo di dare esecuzione all'attività nel rispetto delle previsioni del Modello.

3.10 Impianto procedurale

Ai fini di dare ulteriore e più efficace attuazione ai principi e alle regole comportamentali previste dal Modello, la Società adotta anche una serie di procedure tese a disciplinare in maggiore dettaglio alcuni aspetti dell'operatività e della gestione di taluni processi aziendali.

Queste procedure sono da intendersi quale parte integrante del Modello, di cui costituiscono a tutti gli effetti protocolli operativi.

CAPITOLO 4 – L'ORGANISMO DI VIGILANZA

4.1 Identificazione dell'Organismo di Vigilanza

Ai sensi dell'art. 6, lett. b), D.Lgs. 231/2001, condizione indispensabile per la concessione dell'esimente dalla responsabilità amministrativa è l'attribuzione a un organismo della Società, dotato di autonomi poteri di iniziativa e di controllo, del compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento.

Sul tema le Linee Guida, interpretando le disposizioni del Decreto, suggeriscono l'individuazione dell'OdV in un organo caratterizzato da autonomia, indipendenza, efficienza operativa e continuità di azione, nonché in possesso di professionalità e onorabilità adeguate al ruolo.

I singoli requisiti che devono caratterizzare l'Organismo di Vigilanza sono i seguenti.

a) Autonomia e indipendenza

Il requisito di autonomia e indipendenza presuppone che l'OdV risponda, nello svolgimento di questa sua funzione, solo al massimo vertice gerarchico (ad esempio il Consiglio di Amministrazione).

In sede di costituzione dell'OdV, la sua indipendenza è assicurata dall'obbligo, in capo all'organo amministrativo, di approvare una dotazione annua adeguata di risorse finanziarie, anche su proposta dell'Organismo di Vigilanza stesso, della quale quest'ultimo potrà disporre per ogni esigenza necessaria al corretto svolgimento dei propri doveri (ad esempio consulenze specialistiche, trasferte, ecc.).

L'indipendenza, infine, presuppone che i membri dell'Organismo di Vigilanza non si trovino in una posizione, neppure potenziale di conflitto d'interessi con la Società, né siano titolari all'interno della stessa di funzioni di tipo operativo che ne minerebbero l'obiettività di giudizio nel momento delle verifiche sul rispetto del Modello.

b) Onorabilità e cause di ineleggibilità

Non possono essere eletti membri dell'Organismo di Vigilanza e, se lo sono, decadono necessariamente ed automaticamente dalla carica, i seguenti soggetti:

- i. coloro che si trovano nelle condizioni previste dall'art. 2382 c.c., ovvero sia gli inabilitati, interdetti, falliti o condannati ad una pena che comporti l'interdizione, anche temporanea, da uffici pubblici o l'incapacità ad esercitare uffici direttivi;
- ii. coloro che siano stati sottoposti a misure di prevenzione disposte dall'autorità giudiziaria ai sensi della Legge 27 dicembre 1956, n. 1423 (cosiddetta "*Legge sulle misure di prevenzione nei confronti delle persone pericolose per la sicurezza e per la pubblica moralità*") o della Legge 31 maggio 1965, n. 575 (cosiddetta "*Legge antimafia*");
- iii. coloro che sono stati condannati a seguito di sentenza ancorché non ancora definitiva, o emessa ex artt. 444 e ss. c.p.p. o anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:

- 1) per uno dei delitti previsti nel titolo XI, del libro V, c.c. (Disposizioni penali in materia di società e consorzi) e nel Regio Decreto 16 marzo 1942, n. 267, e sue successive modifiche od integrazioni;
 - 2) a pena detentiva, non inferiore ad un anno, per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento (tra questi si segnalano, a titolo esemplificativo e non esaustivo, i reati di abusivismo bancario e finanziario di cui agli artt. 130 e seguenti del Testo Unico Bancario, i reati di falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate di cui all'art. 453 c.p., i reati di fraudolento danneggiamento dei beni assicurati e mutilazione fraudolenta della propria persona di cui all'art. 642 c.p.);
 - 3) per un delitto contro la pubblica amministrazione, o alla reclusione per un tempo non inferiore ad un anno per un delitto contro la fede pubblica, contro il patrimonio, contro l'ordine pubblico, contro l'economia pubblica ovvero per un delitto in materia tributaria;
 - 4) alla reclusione per un tempo non inferiore a due anni per un qualunque delitto non colposo;
 - 5) in ogni caso e a prescindere dall'entità della pena, per uno o più illeciti tra quelli tassativamente previsti dal D.Lgs. 231/2001;
- iv. coloro che hanno rivestito la qualifica di componente dell'organismo di vigilanza in società nei cui confronti siano state applicate, con sentenza passata in giudicato, le sanzioni previste dall'art. 9, comma 2, D.Lgs. 231/2001, per fatti commessi durante il periodo in cui essi rivestivano il ruolo di componente, ove risulti dagli atti l'omessa o insufficiente vigilanza da parte dell'organismo di vigilanza, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;
- v. coloro nei cui confronti siano state applicate le sanzioni amministrative accessorie previste dall'art. 187-*quater* TUF.

c) *Comprovata professionalità, capacità specifiche in tema di attività ispettiva e consulenziale*

L'Organismo di Vigilanza deve possedere, al suo interno, competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite alla sua indipendenza, ne garantiscono l'obiettività di giudizio; è necessario, pertanto, che all'interno dell'Organismo di Vigilanza siano presenti soggetti con professionalità adeguate in materia economica, di controllo e gestione dei rischi aziendali. L'Organismo di Vigilanza potrà, inoltre, anche avvalendosi di professionisti esterni, dotarsi di risorse competenti in materia giuridica di organizzazione aziendale, revisione, contabilità e finanza.

d) *Continuità d'azione*

L'Organismo di Vigilanza svolge in modo continuativo le attività necessarie per la vigilanza in merito alla corretta applicazione del Modello con adeguato impegno e con i necessari poteri di indagine; cura l'attuazione del Modello assicurandone il costante aggiornamento.

L'OdV non svolge mansioni operative che possano condizionare e contaminare quella visione d'insieme sull'attività aziendale che ad esso si richiede.

4.2 Durata in carica

Il Consiglio di Amministrazione provvede alla nomina dell'Organismo di Vigilanza mediante apposita delibera consiliare: a tal riguardo, al momento della nomina dovranno essere forniti nel corso della riunione consiliare adeguati chiarimenti in merito alla professionalità di ogni componente, il cui *curriculum vitae* verrà allegato al relativo verbale.

L'OdV viene individuato in composizione monocratica e nominato per un periodo pari a 3 anni.

Alla scadenza dell'incarico, l'OdV potrà continuare a svolgere le proprie funzioni e a esercitare i poteri di propria competenza, come in seguito meglio specificati, sino alla nomina dei nuovi componenti da parte del Consiglio di Amministrazione.

Al fine di garantire i requisiti di indipendenza e di autonomia, dal momento della nomina e per tutta la durata della carica, i componenti dell'Organismo:

- a) non devono rivestire incarichi esecutivi o delegati nel Consiglio di Amministrazione della Società;
- b) non devono svolgere funzioni operative o di *business* all'interno della Società;
- c) non devono intrattenere significativi rapporti d'affari con la Società, con società da essa controllate o ad essa collegate (fatto salvo il rapporto di lavoro subordinato), né intrattenere significativi rapporti d'affari con gli amministratori muniti di deleghe (amministratori esecutivi);
- d) non devono avere rapporti con o far parte del nucleo familiare degli amministratori esecutivi, dovendosi intendere per nucleo familiare quello costituito dal coniuge non separato legalmente, dai parenti e affini entro il quarto grado;
- e) non devono risultare titolari, direttamente o indirettamente, di partecipazioni nel capitale della Società;
- f) devono avere e mantenere i requisiti di onorabilità indicati nella lettera b) del paragrafo 4.1 che precede.

I componenti dell'Organismo di Vigilanza sono tenuti a sottoscrivere, all'atto della nomina e poi periodicamente, una dichiarazione attestante l'esistenza e la successiva persistenza dei requisiti di indipendenza di cui sopra e, comunque, a comunicare immediatamente al Consiglio di Amministrazione della Società e agli altri componenti dell'Organismo di Vigilanza l'insorgere di eventuali condizioni ostative.

Rappresentano ipotesi di decadenza automatica le incompatibilità di cui alle precedenti lettere da a) a e), le circostanze di cui alla lettera f), la sopravvenuta incapacità e la morte; fatte salve le ipotesi di

decadenza automatica, i membri dell'Organismo non possono essere revocati dal Consiglio di Amministrazione se non per giusta causa.

Rappresentano ipotesi di giusta causa di revoca:

- a) una sentenza di condanna della Società ai sensi del Decreto o una sentenza di patteggiamento, passata in giudicato, con applicazione delle sanzioni di cui all'art. 9, comma 2, del D.Lgs. 231/2001, ove risulti dagli atti l'omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;
- b) la violazione degli obblighi di riservatezza di cui si dirà *infra*;
- c) la mancata partecipazione a più di tre riunioni consecutive senza giustificato motivo;
- d) grave negligenza nell'adempimento dei propri compiti;
- e) in caso di soggetti interni alla struttura aziendale, le eventuali dimissioni o licenziamento.

In caso di dimissioni o di decadenza automatica di un componente dell'Organismo di Vigilanza, quest'ultimo ne darà comunicazione tempestiva al Consiglio di Amministrazione, che prenderà senza indugio le decisioni del caso.

4.3 Funzione, poteri e compiti dell'Organismo di Vigilanza

All'OdV della Società è affidato il compito di vigilare:

- 1) sull'osservanza delle prescrizioni del Modello da parte dei Destinatari;
- 2) sull'idoneità ed efficacia del Modello in relazione alla struttura della Società e ai suoi eventuali mutamenti;
- 3) sull'opportunità di aggiornamento del Modello, in relazione alle mutate condizioni strutturali e alle novità legislative e regolamentari.

Quanto agli aspetti più operativi, è affidato all'OdV della Società il compito di:

- verificare l'efficienza ed efficacia del Modello organizzativo adottato ai sensi del D. Lgs. 231/2001;
- sviluppare sistemi di controllo e monitoraggio tesi alla ragionevole prevenzione delle irregolarità ai sensi del D. Lgs. 231/2001;
- verificare il rispetto degli *standard* di comportamento e delle procedure previste dal Modello e rilevare gli eventuali scostamenti comportamentali, mediante analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie Attività Sensibili; per lo svolgimento delle attività di verifica e di controllo, di cui al presente punto e dei precedenti, l'OdV, potrà avvalersi delle attività di verifica delle funzioni di controllo eventualmente nominate dalla Società;

- riferire periodicamente al Consiglio di Amministrazione (e al Collegio Sindacale) circa lo stato di attuazione e l'operatività del Modello;
- promuovere e/o sviluppare, di concerto con le funzioni aziendali a ciò preposte, programmi di informazione e comunicazione interna, con riferimento al Modello, agli *standard* di comportamento e alle procedure adottate ai sensi del D.Lgs. 231/2001;
- promuovere e/o sviluppare l'organizzazione, di concerto con le funzioni aziendali preposte, di corsi di formazione e la predisposizione di materiale informativo utili alla comunicazione e divulgazione dei principi etici e degli standard cui la Società si ispira nello svolgimento delle proprie attività;
- fornire chiarimenti in merito al significato e all'applicazione delle previsioni contenute nel Modello;
- assicurare l'aggiornamento del sistema di identificazione, mappatura e classificazione delle Attività Sensibili;
- raccogliere, elaborare e conservare le informazioni, comprese le segnalazioni, rilevanti in merito al rispetto del Modello;
- effettuare periodicamente verifiche ed ispezioni mirate su determinate operazioni e atti specifici, posti in essere nelle Attività Sensibili come individuate nel Modello;
- segnalare al Consiglio di Amministrazione, per gli opportuni provvedimenti, quelle violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo alla Società;
- formulare proposte al Consiglio di Amministrazione, di eventuali aggiornamenti e adeguamenti del Modello adottato e dei suoi elementi costitutivi, in conseguenza di:
 - significative violazioni delle prescrizioni del Modello;
 - significative modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento dell'attività d'impresa;
 - modifiche nello svolgimento delle attività aziendali;
 - modifiche normative.
- introdurre, se necessario e fermo restando quanto previsto nel presente documento, altre regole operative relative, ad esempio, alla cadenza delle proprie riunioni, alle eventuali specifiche mansioni affidate ai singoli componenti ovvero alla gestione delle informazioni acquisite nell'esercizio dell'incarico.

Tutte le attività poste in essere dall'OdV nello svolgimento dei suoi compiti non sono soggette al sindacato di alcun altro organismo o struttura della Società.

4.4 Flussi informativi dell'OdV verso il vertice aziendale

L'OdV riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità.

L'OdV ha due differenti tipologie di flussi informativi:

- la prima, su base continuativa, e non appena ve ne sia la necessità, direttamente verso l'Amministratore/i Delegato/i;
- la seconda, su base periodica, tramite apposita relazione scritta (almeno annuale), nei confronti del Consiglio di Amministrazione (nonché, in copia, all'attenzione del Collegio Sindacale).

Tali flussi informativi hanno ad oggetto:

1. l'attività svolta dall'OdV;
2. le eventuali criticità (e spunti per il miglioramento) emerse sia in termini di comportamenti o eventi interni alla Società, sia in termini di efficacia del Modello. Qualora l'OdV rilevi criticità riferibili a qualcuno dei soggetti referenti, la corrispondente segnalazione è da destinarsi prontamente ad uno degli altri soggetti sopra individuati.

Il Consiglio di Amministrazione ha la facoltà di convocare in qualsiasi momento l'OdV che, a sua volta, ha la facoltà di richiedere, attraverso le funzioni o i soggetti competenti, la convocazione dei predetti organi per motivi urgenti.

4.5 Flussi informativi verso l'OdV: informazioni di carattere generale e informazioni specifiche obbligatorie. Il sistema di *whistleblowing*

L'art. 6, comma 2, lett. d) del Decreto 231 richiede la previsione nel Modello di obblighi informativi nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello stesso (vale a dire, l'Organismo di Vigilanza). L'obbligo di un flusso informativo strutturato è concepito quale strumento per garantire l'attività di vigilanza sull'efficacia ed effettività del Modello e per l'eventuale accertamento a posteriori delle cause che hanno reso possibile il verificarsi dei reati previsti dal Decreto 231.

L'efficacia dell'attività di vigilanza trova fondamento in un sistema strutturato di segnalazioni ed informazioni provenienti da tutti i Destinatari del Modello, con riferimento a tutti gli atti, comportamenti o eventi, di cui vengano a conoscenza, che potrebbero determinare una violazione del Modello o che, più in generale, siano potenzialmente rilevanti ai fini del Decreto 231.

Come previsto dalle Linee Guida di Confindustria e dalle *best practice*, i flussi informativi nei confronti dell'Organismo di Vigilanza fanno riferimento alle seguenti categorie di informazioni:

- flussi informativi *ad hoc* (attinenti a criticità attuali o potenziali che è opportuno portare immediatamente a conoscenza dell'OdV, come meglio specificato *infra*);
- informativa periodica (attinente a numerosi e diversi aspetti in merito ai quali è opportuno che l'OdV riceva informazioni a cadenza prestabilita – di norma annuale o semestrale –, per lo

svolgimento dell'attività di monitoraggio sul rispetto delle regole di comportamento previste nelle singole Parti Speciali del Modello, come meglio spiegato *infra*).

4.5.1. Flussi informativi ad hoc

I flussi informativi *ad hoc* indirizzati all'OdV attengono a criticità attuali o potenziali e possono consistere in:

a) *notizie occasionali in relazione alle quali è opportuna un'informativa immediata nei confronti dell'Organismo di Vigilanza*. L'obbligo di informazione ha per oggetto:

- i provvedimenti e/o le notizie provenienti dall'Autorità Giudiziaria, o da qualsiasi altra Autorità, dai quali si evinca lo svolgimento di indagini/accertamenti, riguardanti la Società, anche nei confronti di ignoti, per uno dei Reati;
- le richieste di assistenza legale da parte dei dirigenti e/o dei Dipendenti in caso di avvio di procedimento giudiziario per uno dei Reati;
- le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del sistema disciplinare previsto nel Modello con evidenza specifica dei procedimenti disciplinari attivati e delle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- i *report* e le relazioni da cui possano emergere elementi con profili di criticità rispetto all'osservanza delle norme di cui al D.Lgs. 231/2001;
- l'eventuale esistenza di situazioni di conflitto di interesse tra uno dei Destinatari e la Società;
- eventuali infortuni sul luogo di lavoro con prognosi uguale o superiore a 40 giorni, ovvero provvedimenti assunti dall'Autorità Giudiziaria o da altre Autorità in merito alla materia della sicurezza e salute sul lavoro;
- eventuali incidenti o accadimenti che possano comportare un rischio ambientale;

b) *informazioni di qualsiasi provenienza, concernenti la possibile commissione di reati o comunque di violazioni del Modello*.

L'obbligo di informazione ha per oggetto:

- la commissione di Reati o il compimento di atti idonei alla realizzazione degli stessi;
- la commissione di illeciti amministrativi rilevanti ai sensi del D.Lgs. 231/2001;
- comportamenti non in linea con il Modello e con i relativi protocolli;
- variazioni o carenze delle procedure nell'ambito delle Attività Sensibili;
- mancato rispetto delle procedure aziendali nell'ambito delle Attività Sensibili;
- variazioni o carenze nella struttura aziendale;

- operazioni che presentino profili di rischio per la commissione di Reati.

L'OdV valuta le segnalazioni ricevute e determina le eventuali iniziative, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e/o ogni altro soggetto che riterrà utile, motivando per iscritto ogni conclusione raggiunta.

Al fine di facilitare il flusso di segnalazioni ed informazioni verso l'OdV, è prevista un'apposita casella *e-mail* (ekaterina.kukushka@ctep.it), la quale è appositamente comunicata ai Destinatari.

Inoltre, al fine di garantire il massimo grado di riservatezza nelle segnalazioni, anche ai sensi di quanto precisato ai paragrafi che seguono, sono istituiti ulteriori canali di segnalazione.

L'OdV può, inoltre, chiedere alla società di revisione informazioni in merito alle attività da questa svolte, di interesse ai fini dell'attuazione del Modello e del controllo sul rispetto dello stesso

4.5.2. Whistleblowing

Con riferimento all'istituto del cosiddetto "*whistleblowing*" previsto dall'art. 6, comma 2-*bis* del D.Lgs. 231/2001, la Società prevede un canale di segnalazione interna, il divieto di ritorsione e un sistema disciplinare conformi al D.Lgs. 10 marzo 2023, n. 24 ("**Decreto Whistleblowing**").

Le violazioni che possono essere segnalate ai sensi del Decreto *Whistleblowing* sono quelle di cui il segnalante sia venuto a conoscenza nell'ambito del proprio contesto lavorativo e che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o della Società; tra queste rientrano anche le segnalazioni di condotte illecite rilevanti ai sensi del Decreto 231 o violazioni del Modello 231.

In conformità a quanto previsto dal Decreto *Whistleblowing* (nonché dal Testo Unico della Finanza), la Società ha istituito diversi canali che consentono l'effettuazione di segnalazioni garantendo la riservatezza del segnalante e della persona coinvolta nonché del contenuto della segnalazione e della relativa documentazione.

I soggetti individuati per la gestione delle segnalazioni sono specificamente formati in materia di *whistleblowing* e autorizzati ai sensi del Regolamento UE n. 2016/679 (GDPR).

I segnalanti non possono subire alcuna ritorsione e, a tal proposito, il Decreto *Whistleblowing* dispone la previsione di sanzioni pecuniarie e disciplinari a carico di chi realizza atti ritorsivi nonché misure di sostegno per i segnalanti e la possibilità per quest'ultimi di comunicare all'ANAC le ritorsioni che ritengono di aver subito in ragione di una segnalazione.

A tal riguardo, la Società adotta tutte le misure necessarie per garantire che sia assicurato il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante in ragione di una segnalazione.

Si precisa che ai sensi del Decreto *Whistleblowing*, le segnalazioni possono essere effettuate anche da soggetti esterni alla Società (indicati nel Decreto *Whistleblowing*) e le tutele riservate al segnalante vengono estese anche a soggetti collegati (indicati nel Decreto *Whistleblowing*).

Per tutto quanto concerne la tematica in oggetto nonché per ogni maggiore dettaglio sui canali di segnalazione, si rimanda espressamente al “**Regolamento interno in materia di Whistleblowing**”, che deve essere considerato a tutti gli effetti parte integrante del Modello.

4.5.3. Flussi informativi da parte delle funzioni di controllo

Si aggiunge che la Società ha costituito un comitato delle funzioni di controllo aziendale coordinato dal Presidente del CdA, che si riunisce semestralmente per confrontarsi sugli esiti delle verifiche effettuate. L'OdV partecipa a tale comitato ed è inoltre destinatario dei verbali trimestrali delle funzioni di controllo.

4.6 Raccolta e conservazione delle informazioni

Ogni informazione raccolta e ogni *report* ricevuto o preparato dall'Organismo di Vigilanza sono conservati per 5 anni (o, nei casi di conservazione di documenti inerenti a una segnalazione ai sensi del Decreto *Whistleblowing*, per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni) in un apposito archivio tenuto dall'OdV in formato cartaceo o elettronico.

4.7 Verifiche sull'adeguatezza del Modello

Oltre all'attività di vigilanza che l'OdV svolge continuamente sull'effettività del Modello (e che si concreta nella verifica della coerenza tra i comportamenti dei Destinatari ed il Modello stesso), lo stesso può effettuare specifiche verifiche (ad esempio, con modalità “a campione”) sull'effettiva capacità del Modello di prevenire i Reati, eventualmente avvalendosi del supporto di soggetti terzi con adeguate caratteristiche di professionalità e indipendenza.

Inoltre, viene svolta una *review* di tutte le segnalazioni eventualmente ricevute nel corso dell'anno, delle azioni intraprese dall'OdV e delle verifiche a campione degli eventi considerati rischiosi.

Per le verifiche l'OdV si avvale, di norma, del supporto di altre funzioni interne che, di volta in volta, si rendano a tal fine necessarie.

Le verifiche e il relativo esito sono inseriti nel *report* periodico agli Organi Sociali nei quali, in caso di emersione di criticità, l'OdV esporrà i miglioramenti che suggerisce di attuare.

CAPITOLO 5 – FORMAZIONE E DIFFUSIONE DEL MODELLO

5.1 Formazione e informazione degli Organi Sociali e dei Dipendenti

Ai fini dell'efficacia del presente Modello, è obiettivo della Società garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute nei confronti dei Destinatari. Il livello di formazione ed informazione è attuato con un differente grado di approfondimento in relazione al diverso livello di coinvolgimento nelle Attività Sensibili.

Dovranno essere svolte attività di formazione periodica a favore degli Organi Sociali e dei Dipendenti sui contenuti del Modello e del D.Lgs. 231/2001.

- La comunicazione iniziale

L'adozione del presente Modello è comunicata a tutti i Dipendenti e collaboratori presenti in azienda al momento della sua adozione, così come lo sono eventuali successivi aggiornamenti significativi.

I nuovi assunti, invece, sono informati dell'adozione da parte della Società del Modello al momento dell'avvio dell'attività lavorativa presso la Società.

La Società, in particolare, deve garantire che ciascun nuovo assunto:

- riceva, al momento dell'instaurazione del rapporto, copia aggiornata del Modello 231 della Società;
- sottoscriva una dichiarazione di ricezione e di impegno al rispetto dello stesso.

- La formazione

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D. Lgs. 231/2001 è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei rispettivi destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno gli stessi funzioni di rappresentanza della Società.

Con riferimento ai nuovi assunti, la Società garantisce che questi ricevano, nell'ambito dell'attività formativa che viene svolta nelle prime giornate lavorative, una formazione di base anche in merito alla normativa di cui al Decreto 231.

La mancata partecipazione all'attività di formazione senza giustificazione costituisce una violazione dei principi contenuti nel presente Modello e, pertanto, potrà essere oggetto di sanzione ai sensi di quanto indicato nel seguente Capitolo.

L'attività di formazione, volta a diffondere la conoscenza del Modello, è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della società.

Tutti i programmi di formazione avranno un contenuto minimo comune consistente nell'illustrazione dei principi del D.Lgs. 231/01, degli elementi costitutivi il Modello, delle singole fattispecie di Reati e dei comportamenti considerati sensibili in relazione al compimento dei reati sopra citati.

All'interno dei piani di formazione previsti dalla Società, è inoltre inserita anche la formazione in materia di *whistleblowing*.

La partecipazione ai programmi di formazione sopra descritti è obbligatoria e all'OdV deve essere fornita costante informativa al riguardo.

5.2 Selezione ed informazione dei Consulenti, dei Fornitori e dei *Partner*

Fatto salvo quanto sopra previsto in relazione ai contratti di *outsourcing* infragruppo, relativamente ai Consulenti, ai Fornitori e ai *Partner*, sono istituiti appositi sistemi in grado di orientare la selezione dei medesimi secondo criteri che tengano in debito conto i principi di prevenzione ed integrità di cui al presente Modello, principi di cui gli stessi verranno adeguatamente informati.

In occasione dell'instaurarsi di un nuovo rapporto con Consulenti, *Partner* e Fornitori la Società:

- a) informerà la controparte in merito al proprio impegno a svolgere la propria attività aziendale in modo lecito e nel pieno rispetto dei principi previsti dal D.Lgs. 231/2001 e dell'adozione del Modello;
- b) chiederà alla controparte di tenere, a sua volta, condotte conformi ai principi previsti dal D.Lgs. 231/2001.

CAPITOLO 6 – SISTEMA DISCIPLINARE

6.1 principi generali

La definizione di un sistema disciplinare e di sanzioni (che devono essere commisurate alla violazione e dotate di potere deterrente) applicabili in caso di violazione delle regole di cui al presente Modello costituisce, ai sensi dell'art. 6, comma 1, D. Lgs. 231/2001, un requisito essenziale del Modello.

L'applicazione del suddetto sistema sanzionatorio presuppone la mera violazione delle disposizioni del Modello; esso, pertanto, troverà applicazione indipendentemente dall'instaurazione, dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'Autorità Giudiziaria nel caso in cui il comportamento da censurare integri anche uno dei Reati.

In virtù di quanto previsto dal Decreto *Whistleblowing* e con riferimento a qualunque destinatario del Modello, si precisa che, tra le condotte passibili di sanzione, devono essere considerate anche le violazioni previste da detto decreto¹.

6.2 Misure nei confronti dei Dipendenti

I comportamenti tenuti dai Dipendenti della Società in violazione delle singole regole comportamentali dedotte nel presente Modello sono definiti come illeciti disciplinari.

Con riferimento alle sanzioni irrogabili nei riguardi dei Dipendenti, le stesse sono irrogate e attuate nel rispetto delle procedure previste dall'articolo 7 della Legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) ed eventuali normative speciali applicabili.

A. Dipendenti che non rivestono la qualifica di dirigenti

Le sanzioni applicabili ai Dipendenti, conformemente alle previsioni di cui al CCNL applicato dalla Società, sono le seguenti:

- 1) richiamo verbale;
- 2) ammonizione scritta;
- 3) multa (nei limiti stabiliti dal CCNL applicabile e da eventuali accordi sindacali tempo per tempo vigenti);
- 4) sospensione dal lavoro e dal trattamento economico (nei limiti stabiliti dal CCNL applicabile e da eventuali accordi sindacali aziendali tempo per tempo vigenti);
- 5) licenziamento (nei casi previsti dalla legge nonché in quelli previsti dal CCNL applicabile e da eventuali accordi sindacali aziendali tempo per tempo vigenti).

¹ Si precisa che il Decreto *Whistleblowing* elenca (all'art. 21) determinate condotte per le quali l'ANAC può irrogare, a seguito di un procedimento di accertamento, sanzioni amministrative pecuniarie.

Restano ferme – e si intendono qui richiamate – tutte le disposizioni, previste dalla legge e dal CCNL applicato, relative alle procedure e agli obblighi da osservare nell'applicazione delle sanzioni.

Per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, agli organi sociali e funzioni aziendali competenti.

Fermi restando gli obblighi per la Società, scaturenti dallo Statuto dei Lavoratori e dal CCNL applicabile, i comportamenti sanzionabili che costituiscono violazione del presente del Modello sono i seguenti:

- a) adozione, nell'espletamento delle Attività Sensibili/Strumentali, di comportamenti palesemente in violazione delle prescrizioni del presente Modello, tali da determinare la concreta applicazione a carico della Società di sanzioni previste dal D. Lgs. 231/2001;
- b) violazione di procedure interne previste dal presente Modello o adozione, nell'espletamento delle Attività Sensibili/Strumentali, di comportamenti non conformi alle prescrizioni del Modello.

Le sanzioni sopra elencate possono essere applicate – in base alla gravità del comportamento – anche in caso di violazioni del Decreto *Whistleblowing*.

B. Dipendenti che rivestono la qualifica di dirigenti

In caso di violazione, da parte di dirigenti, del presente Modello o di adozione, nell'espletamento delle Attività Sensibili, di un comportamento non conforme alle prescrizioni dello stesso (ivi comprese la violazione, in qualsivoglia modo, delle misure a tutela del segnalante, nonché l'ipotesi di effettuazione con dolo o colpa grave di segnalazioni che si rivelino infondate ovvero di altre violazioni del Decreto *Whistleblowing*), la Società provvede ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto normativamente previsto e in conformità con quanto previsto dal CCNL applicabile.

Più in particolare, in relazione alla gravità del comportamento commesso, potranno essere irrogate le seguenti sanzioni:

- 1) richiamo verbale da parte dell'Amministratore Delegato, per le ipotesi in cui il dirigente non si sia attenuto scrupolosamente alle indicazioni contenute nel presente Modello;
- 2) richiamo scritto, per le ipotesi di maggior gravità rispetto a quelle di cui al punto precedente (quali, a titolo esemplificativo ma non esaustivo, la mancata partecipazione – senza giustificazione – alle attività formative, il mancato rispetto dei flussi informativi indicati nel presente Modello, ecc.) con comunicazione da parte dell'Amministratore Delegato;
- 3) licenziamento, per le ipotesi di gravità tale da non suggerire la prosecuzione del rapporto, con decisione assunta dal Consiglio di Amministrazione o da soggetto dallo stesso delegato.

* * *

Le sanzioni e l'eventuale richiesta di risarcimento dei danni verranno commisurate al livello di responsabilità ed autonomia, all'eventuale esistenza di precedenti disciplinari a carico, all'intenzionalità

del comportamento nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui la Società può ragionevolmente ritenersi esposta – ai sensi e per gli effetti del Decreto 231 – a seguito della condotta censurata.

L'adesione ai principi e alle regole contenute nel Modello costituisce elemento di fondamentale rilievo nella valutazione professionale della risorsa e ha riflessi diretti sul percorso di carriera e retributivo; in particolare, l'aderenza ai principi e alle regole del Modello costituisce uno dei requisiti su cui vengono basati eventuali programmi di retribuzione variabile/premiale/MBO.

6.3 Misure nei confronti degli Amministratori

In caso di violazione del Modello (ivi comprese le violazioni previste dal Decreto *Whistleblowing*), da parte di uno o più membri del Consiglio di Amministrazione, viene informato il Collegio Sindacale e l'intero CdA, che prende gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea dei soci al fine di adottare le misure più idonee previste dalla legge e/o la revoca di deleghe eventualmente conferite all'amministratore.

Si coglie l'occasione per specificare che, nel caso in cui la Società venisse individuata quale ente incolpato nell'ambito di un procedimento ex Decreto 231 e in tale procedimento il legale rappresentante della Società fosse direttamente coinvolto in qualità di indagato per il reato presupposto dell'illecito amministrativo ascritto all'ente, la nomina del difensore dell'ente non verrebbe effettuata da detto legale rappresentante, bensì da altro/i soggetto/i, munito/i degli appositi poteri.

6.4 Misure nei confronti dei Sindaci

In caso di violazione del presente Modello (ivi comprese le violazioni previste dal Decreto *Whistleblowing*) da parte di uno o più Sindaci, viene informato l'intero Collegio Sindacale e il Consiglio di Amministrazione, il quale prenderà gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'Assemblea dei Soci al fine di adottare le misure più idonee previste dalla legge. Nell'ipotesi di nomina di un Collegio Sindacale, in caso di violazione del presente Modello da parte di uno o più sindaci, l'OdV informa l'intero Collegio Sindacale e il Consiglio di Amministrazione, i quali prenderanno gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'Assemblea dei Soci al fine di adottare le misure più idonee previste dalla legge.

6.5 Misure nei confronti dei Consulenti, dei Fornitori e dei Partner

Ogni violazione delle regole di cui al presente Modello (ivi comprese le violazioni previste dal Decreto *Whistleblowing*), applicabili ai Consulenti, ai Fornitori o ai *Partner* od ogni commissione dei Reati previsti dal Modello è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti.



Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla Società, come nel caso di applicazione alla stessa da parte del giudice delle misure previste dal Decreto 231.

6.6 Misure nei confronti dei componenti dell'OdV

In caso di violazione del presente Modello (ivi comprese le violazioni previste dal Decreto *Whistleblowing*), da parte di un membro dell'OdV, verrà informato immediatamente il Consiglio di Amministrazione perché assuma gli opportuni provvedimenti.



PARTI SPECIALI



**PARTE SPECIALE – I – Reati nei rapporti con la Pubblica Amministrazione e Induzione
a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria**

CAPITOLO I.1 - LE FATTISPECIE DI REATO

MALVERSAZIONE DI EROGAZIONI PUBBLICHE (ART. 316-BIS C.P.)

Tale ipotesi di reati si configura nei confronti di chiunque, avendo ottenuto dallo Stato, da altro ente pubblico o dall'Unione Europea contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non li destina a tali attività.

Per l'integrazione del reato è sufficiente che anche solo una parte delle attribuzioni ricevute sia stata impiegata per scopi diversi da quelli previsti, non rilevando, in alcun modo, che l'attività programmata sia stata comunque svolta. Risultano altresì irrilevanti le finalità che l'autore del reato abbia voluto perseguire, poiché l'elemento soggettivo del reato medesimo è costituito dalla volontà di sottrarre risorse destinate ad uno scopo prefissato.

Tipico esempio è rappresentato dall'ottenimento di un finanziamento pubblico erogato in vista dell'assunzione presso la società di personale appartenente a categorie privilegiate successivamente disattesa.

INDEBITA PERCEZIONE DI EROGAZIONI PUBBLICHE (ART. 316-TER C.P.)

Tale ipotesi di reato si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere ovvero mediante l'omissione di informazioni dovute - si ottengano, senza averne diritto, contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominati, concessi o erogati dallo Stato, da altri enti pubblici o dalla Unione Europea.

È prevista un'aggravante speciale nei casi in cui il fatto offenda gli interessi finanziari dell'Unione Europea e il danno o il profitto siano superiori a euro 100.000.

In questo caso, contrariamente a quanto visto in merito al reato precedente, a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie di cui all'art. 640-*bis* c.p. (truffa aggravata per il conseguimento di erogazioni pubbliche), nel senso che si configura solo nei casi in cui la condotta non integri gli estremi del reato di cui a quest'ultima disposizione.

TRUFFA IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (ART. 640, COMMA 2, N. 1 C.P.)

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici e raggiri (intendendosi compresa in tale definizione anche l'eventuale omissione di informazioni che, se conosciute, avrebbero certamente determinato in senso negativo la volontà dello Stato, di altro ente pubblico o dell'Unione Europea) tali da indurre in errore e da arrecare un danno (di tipo patrimoniale) a tali enti.

Si pensi, in particolare, alla trasmissione all'amministrazione finanziaria di documentazione contenente false informazioni al fine di ottenere un rimborso fiscale non dovuto; ovvero, più in generale, all'invio ad

enti previdenziali o amministrazioni locali di comunicazioni contenenti dati falsi in vista di un qualsiasi vantaggio o agevolazione per la Società.

Si pensi, ancora, alla falsa prospettazione dolosa di determinati vantaggi a seguito della sottoscrizione di uno strumento finanziario che già *ex ante* non possiede tali caratteristiche vantaggiose.

TRUFFA AGGRAVATA PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE (ART. 640-BIS C.P.)

Il reato in oggetto si perfeziona allorquando i fatti di cui al precedente art. 640 c.p. riguardano l'ottenimento di contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni concesse dallo Stato, da altri enti pubblici o dall'Unione Europea.

Si pensi ad esempio alle ipotesi di indebito ottenimento di un finanziamento pubblico finalizzato al sostegno delle attività imprenditoriali in determinati settori (come, ad esempio, nel settore energetico), mediante la produzione di falsa documentazione attestante la sussistenza dei requisiti per l'ottenimento del finanziamento.

FRODE INFORMATICA (ART. 640-TER C.P.)

Si configura il reato di frode informatica quando, al fine di procurare a sé o ad altri un ingiusto profitto, venga alterato in qualsiasi modo il funzionamento di un sistema informatico, o si intervenga, senza diritto, su dati, informazioni o programmi contenuti in un sistema informatico.

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 P.A.

Per ciò che concerne i reati di cui agli artt. 316-*bis*, 316-*ter* e 640-*bis* c.p., si precisa che i contributi e le sovvenzioni sono attribuzioni pecuniarie a fondo perduto che possono avere carattere periodico o *una tantum*, in misura fissa o determinata in base a parametri variabili, natura vincolata 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.

CONCUSSIONE (ART. 317 C.P.)

L'art. 317 c.p., come modificato dalla Legge 6 novembre 2012, n. 190 e dalla Legge 27 maggio 2015, n. 69, punisce il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Nella formulazione codicistica antecedente alla modifica apportata dalla Legge 27 maggio 2015, n. 69, la fattispecie in esame prevedeva quale soggetto attivo solo il pubblico ufficiale. Il legislatore con tale ultima modifica ha riesteso la soggettività attiva del reato anche all'incaricato di pubblico servizio.

La concussione, al pari della corruzione, prevede una condotta bilaterale, ovverosia da parte del concussore e del concusso.

Tuttavia, a differenza della corruzione, solo il concussore è assoggettato a pena, in quanto il concusso è la vittima del reato: pertanto, per la natura privatistica dell'attività svolta dalla Società, i suoi Esponenti non potrebbero commettere il reato in proprio in quanto sprovvisti della necessaria qualifica pubblicistica; i medesimi potrebbero tutt'al più concorrere in un reato di concussione commesso da un pubblico ufficiale o da un incaricato di pubblico servizio ai sensi dell'art. 110 c.p. o rispondere della diversa ipotesi delittuosa (qualora la condotta del Pubblico Ufficiale o dell'incaricato di pubblico servizio si sostanzi in un'induzione indebita a dare o promettere denaro o altra utilità) prevista e punita dall'art. 319-*quater* c.p.

Inoltre, è astrattamente possibile che un Esponente della Società rivesta, al di fuori dell'attività lavorativa, una pubblica funzione o svolga un pubblico servizio: si pensi all'amministratore della Società che svolga l'incarico di componente di una giunta comunale. In tale ipotesi, questi, nello svolgimento del proprio ufficio o servizio, dovrà astenersi dal tenere comportamenti che, in violazione dei propri doveri d'ufficio e/o con abuso delle proprie funzioni, siano idonei a recare un vantaggio alla Società.

INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ (ART. 319-QUATER C.P.)

La presente fattispecie di reato è stata introdotta dalla Legge 190/2012, scorporando l'induzione alla corruzione rispetto alla concussione.

Tale ipotesi di reato si configura qualora il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induca taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Sono previste pene diverse per il pubblico ufficiale o incaricato di pubblico servizio che induce il privato a dare o promettere utilità e per il privato cittadino che asseconda tale richiesta.

È prevista un'aggravante speciale nei casi in cui il fatto offenda gli interessi finanziari dell'Unione Europea e il danno o il profitto siano superiori a euro 100.000.

Il legislatore del 2012 ha esteso la punibilità anche al privato che subisce l'attività induttiva, a cui è riservato un regime sanzionatorio più mite rispetto a quello previsto per il pubblico funzionario.

L'elemento comune a tutte le varie fattispecie del reato di corruzione consiste nell'accordo fra un pubblico agente (Pubblico Ufficiale o un Incaricato di Pubblico Servizio) e un soggetto privato. L'accordo corruttivo presuppone che le controparti agiscano in posizione paritaria fra di loro e non ha rilevanza il fatto che l'iniziativa provenga dall'una o dall'altra parte, diversamente da quanto avviene nei reati di concussione e di induzione indebita a dare o promettere utilità, che invece richiedono che il soggetto rivestente la qualifica pubblica paventando l'abuso dei propri poteri, faccia valere la propria posizione di superiorità, alla quale corrisponde nel privato una situazione di soggezione. Peraltro, può risultare difficile distinguere nella pratica quando ricorra una fattispecie di corruzione piuttosto che un reato di

induzione indebita; la distinzione rileva innanzitutto per la determinazione della pena con la quale è punito il soggetto privato, che è più lieve nel reato di induzione indebita.

Nel fatto della corruzione si ravvisano due distinti reati: l'uno commesso dal soggetto corrotto, rivestente la qualifica pubblica (c.d. corruzione passiva), l'altro commesso dal corruttore (c.d. corruzione attiva), che, in forza della disposizione di cui all'art. 321 c.p., è punito con le stesse pene previste per il corrotto. Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale.

CORRUZIONE PER L'ESERCIZIO DELLA FUNZIONE (ARTT. 318 E 320 C.P.)

L'ipotesi di reato di cui all'art. 318 c.p. si configura nel caso in cui un pubblico ufficiale, per compiere un atto di propria competenza riceve, per sé o per un terzo, in denaro o altra utilità, una retribuzione che non gli è dovuta o ne accetta la promessa.

Il legislatore, con la Legge n. 190 del 2012, ha eliminato ogni riferimento a un atto di ufficio già compiuto o da compiere.

La norma punisce sia la compravendita di singoli atti di ufficio, precedentemente riconducibili alla fattispecie di corruzione impropria, sia la c.d. corruzione per asservimento, ossia la messa a libro paga del pubblico agente, svincolata dal riferimento a uno specifico atto. In quest'ultima ipotesi il pubblico amministratore non si limita a fare mercimonio di un singolo atto d'ufficio, ma concede al privato la sua generale disponibilità in vista del conseguimento di una serie indeterminata di risultati vantaggiosi.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da tre a otto anni (la pena, che precedentemente era da uno a sei anni, è stata recentemente aumentata dalla Legge 9 gennaio 2019, n. 3, recante «*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*»).

Ai sensi dell'art. 320 c.p. le disposizioni di cui all'art. 318 c.p. si applicano anche alla persona incaricata di un pubblico servizio, qualora rivesta la qualità di pubblico impiegato: in tali casi, tuttavia, le pene previste dal legislatore sono ridotte fino ad un terzo rispetto alle fattispecie delittuose che vedono coinvolto un pubblico ufficiale.

CORRUZIONE PER UN ATTO CONTRARIO AI DOVERI DI UFFICIO, CIRCOSTANZE AGGRAVANTI E AMBITO APPLICATIVO (ARTT. 319, 319-BIS, 320 E 321 C.P.)

L'ipotesi di reato di cui all'art. 319 c.p. si configura nel caso in cui il pubblico ufficiale, per compiere un atto contrario ai suoi doveri di ufficio o per omettere o ritardare un atto del suo ufficio riceve, per sé o per un terzo, in denaro o altra utilità, una retribuzione che non gli è dovuta o ne accetta la promessa (si pensi ad esempio ad ipotesi corruttive nei confronti dei funzionari pubblici mezzo di Consulenti per impedire la comminazione di sanzioni pecuniarie).

Ai fini della configurabilità di tale reato in relazione al compimento di un atto contrario ai doveri di ufficio vanno considerati sia gli atti illegittimi o illeciti (vietati, cioè, da norme imperative o contrastanti con norme

dettate per la loro validità ed efficacia) sia quegli atti che, pur formalmente regolari, siano stati posti in essere dal pubblico ufficiale violando il dovere d'imparzialità o asservendo la sua funzione ad interessi privati o comunque estranei a quelli proprio della Pubblica Amministrazione.

Per questa fattispecie di reato la pena può essere aumentata ai sensi dell'art. 319-*bis* c.p. qualora l'atto contrario ai doveri di ufficio abbia ad oggetto il conferimento di pubblici impieghi, stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene, nonché il pagamento o rimborso di tributi.

Ai sensi dell'art. 320 c.p., le disposizioni dell'art. 319 c.p. si applicano anche all'incaricato di un pubblico servizio: in tali casi, tuttavia, le pene previste dal legislatore sono ridotte fino ad un terzo rispetto alle fattispecie delittuose che vedono coinvolto un pubblico ufficiale.

Ai sensi dell'art. 321 c.p. le pene previste dagli artt. 318 e 319 c.p. si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il danaro o altra utilità.

Si sottolinea infine che le ipotesi di reato di cui agli artt. 318 e 319 c.p. si differenziano dalla concussione in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

CORRUZIONE IN ATTI GIUDIZIARI (ART. 319-TER C.P.)

Tale ipotesi di reato si configura nel caso in cui, per favorire o danneggiare una parte in un procedimento giudiziario, si corrompa un pubblico ufficiale, e dunque un magistrato, un cancelliere o altro funzionario dell'autorità giudiziaria (si pensi ad esempio al caso in cui un Esponente della Società faccia "pressioni" su un Pubblico Ministero per ottenere una richiesta di archiviazione di un procedimento penale).

È importante sottolineare come il reato possa configurarsi a carico della Società indipendentemente dal fatto che la stessa sia parte del procedimento.

ISTIGAZIONE ALLA CORRUZIONE (ART. 322 C.P.)

Tale ipotesi di reato si configura nel caso in cui venga offerto o promesso danaro o altra utilità ad un pubblico ufficiale o incaricato di pubblico servizio (per indurlo a compiere, omettere o ritardare un atto di sua competenza o compiere un atto contrario ai suoi doveri di ufficio) e tale offerta o promessa non venga accettata.

PECULATO, CONCUSSIONE, INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ, CORRUZIONE E ISTIGAZIONE ALLA CORRUZIONE 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 C.P.)

Sulla base del richiamo all'art. 322-*bis* operato dall'art. 25 del Decreto, le fattispecie di reato previste dagli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si configurano anche nel caso in cui il danaro o altra utilità siano dati, offerti o promessi, anche a seguito di induzione a farlo:

- a) a membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;
- b) a 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;
- c) a 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;
- d) a membri e ad addetti di enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;
- e) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;
- f) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale;
- g) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di organizzazioni pubbliche internazionali;
- h) ai membri delle assemblee parlamentari internazionali o di un'organizzazione internazionale o sovranazionale e ai giudici e funzionari delle corti internazionali;
- i) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di Stati non appartenenti all'Unione europea, quando il fatto offende gli interessi finanziari dell'Unione.

Le disposizioni degli articoli 319-*quater*, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità sono dati, offerti o promessi:

- a) alle persone indicate nel primo comma del presente articolo;
- b) 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.

TRAFFICO DI INFLUENZE ILLECITE (ART. 346-BIS C.P.)

La norma in parola prevede la punizione di chiunque, all'infuori dei casi di concorso nei reati di cui agli artt. 318, 319 e 319-*ter* c.p. e nei reati di corruzione di cui all'art. 322-*bis* c.p., sfruttando o vantando relazioni con un pubblico ufficiale o con un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'art. 322-*bis* c.p., indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso il pubblico ufficiale o l'incaricato di un pubblico servizio o

uno degli altri soggetti di cui all'art. 322-*bis* c.p. ovvero per remunerarlo, in relazione all'esercizio delle sue funzioni o dei suoi poteri.

Parimenti, è punito chi indebitamente dà o promette denaro o altra utilità.

La pena è aumentata se il soggetto che indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità riveste la qualifica di pubblico ufficiale o di incaricato di un pubblico servizio.

Le pene sono altresì aumentate se i fatti sono commessi in relazione all'esercizio di attività giudiziarie o per remunerare il pubblico ufficiale o l'incaricato di un pubblico servizio o uno degli altri soggetti di cui all'art. 322-*bis* c.p., in relazione al compimento di un atto contrario ai doveri d'ufficio o all'omissione o al ritardo di un atto del suo ufficio.

È prevista la diminuzione della pena nel caso i fatti siano di particolare tenuità.

INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 377-BIS C.P.)

La Legge 3 agosto 2009, n. 116 ha introdotto un ulteriore art. 25-*decies* per il reato di "induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" come previsto all'art. 377-*bis* c.p.

Ai sensi di tale ultimo articolo, salvo che il fatto costituisca più grave reato, è punito 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 alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere.

I reati sopra considerati trovano come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione (ricomprendendo in tale definizione anche la Pubblica Amministrazione di Stati esteri).

Si indicano pertanto nel capitolo seguente alcuni criteri generali per la definizione di "Pubblica Amministrazione", "Pubblici Ufficiali" e "Incaricati di Pubblico Servizio".

CAPITOLO I.2 - CRITERI PER LA DEFINIZIONE DI P.A. E DI SOGGETTI INCARICATI DI UN PUBBLICO SERVIZIO.

Obiettivo del presente capitolo è quello di indicare dei criteri generali e fornire un elenco esemplificativo dai soggetti di cui all'art. 5, comma 1, lett. a) e b), D.Lgs. 231/2001. Sono, inoltre, riportate anche delle indicazioni in merito alle fattispecie di reato che si possono compiere in relazione alle diverse categorie di soggetti coinvolti.

I.2.1 Enti della pubblica amministrazione

Agli effetti della legge penale, viene comunemente considerato come "Ente della pubblica amministrazione" qualsiasi persona giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi.

Sebbene non esista nel codice penale una definizione di pubblica amministrazione, in base a quanto stabilito nella Relazione Ministeriale al codice stesso ed in relazione ai reati in esso previsti, sono ritenuti appartenere alla pubblica amministrazione quegli enti che svolgano "tutte le attività dello Stato e degli altri enti pubblici".

Nel tentativo di formulare una preliminare classificazione di soggetti giuridici appartenenti a tale categoria è possibile richiamare, da ultimo, l'art. 1, comma 2, D.Lgs. 165/2001 in tema di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, il quale definisce come amministrazioni pubbliche tutte le amministrazioni dello Stato.

A titolo esemplificativo, si possono indicare quali soggetti della pubblica amministrazione, i seguenti enti o categorie di enti:

A titolo esemplificativo, si possono indicare quali soggetti della Pubblica Amministrazione i seguenti Enti o categorie di Enti:

- Enti ed Amministrazioni dello Stato ad ordinamento autonomo (quali, ad esempio, Ministeri, Camera e
- Senato, Agenzia delle Entrate, Magistratura ordinaria e amministrativa);
- Regioni, Province e Comuni;
- Società municipalizzate;
- Partiti politici ed associazioni loro collegate;
- Autorità di Vigilanza (quali ad esempio Banca d'Italia, Consob, AGCM);
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, ISTAT, ENASARCO; ARPA);
- ASL o ATS;

- Enti e Monopoli di Stato;
- Soggetti di diritto privato che esercitano un pubblico servizio (ad esempio, Cassa Depositi e Prestiti, Ferrovie dello Stato);
- Fondazioni di previdenza ed assistenza.

Anche i soggetti di diritto privato concessionari di pubblici servizi e le società partecipate a maggioranza da un ente pubblico sono considerate, dalla più recente giurisprudenza, alla stessa stregua di enti pubblici.

Ferma restando la natura puramente esemplificativa degli enti pubblici sopra elencati, si evidenzia come non tutte le persone fisiche che agiscono nella sfera e in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie criminose ex D.Lgs. 231/2001.

In particolare, le figure che assumono rilevanza a tal fine sono soltanto quelle dei "Pubblici Ufficiali" e degli "Incaricati di Pubblico Servizio".

1.2.2 Pubblici Ufficiali

Ai sensi dell'art. 357, primo comma, c.p., è considerato pubblico ufficiale "*agli effetti della legge penale*" colui il quale esercita "*una pubblica funzione legislativa, giudiziaria o amministrativa*".

Il secondo comma si preoccupa poi di definire la nozione di "pubblica funzione amministrativa". Non si è compiuta invece un'analoga attività definitoria per precisare la nozione di "funzione legislativa" e "funzione giudiziaria" in quanto la individuazione dei soggetti che rispettivamente le esercitano non ha di solito dato luogo a particolari problemi o difficoltà.

Pertanto, il secondo comma dell'articolo in esame precisa che, agli effetti della legge penale "*è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi*".

Tale ultima definizione normativa individua, innanzitutto, la delimitazione "esterna" della funzione amministrativa. Tale delimitazione è attuata mediante il ricorso a un criterio formale che fa riferimento alla natura della disciplina, per cui è definita pubblica la funzione amministrativa disciplinata da "norme di diritto pubblico", ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Inoltre, il secondo comma dell'art. 357 c.p. traduce in termini normativi alcuni dei principali criteri di massima individuati dalla giurisprudenza e dalla dottrina per differenziare la nozione di "pubblica funzione" da quella di "servizio pubblico". Vengono quindi pacificamente definite come "funzioni pubbliche" quelle attività amministrative che rispettivamente ed alternativamente costituiscono esercizio di: (a) poteri deliberativi; (b) poteri autoritativi; (c) poteri certificativi. Alla luce dei principi sopra enunciati, si può affermare che la categoria di soggetti più problematica è certamente quella che ricopre una "pubblica funzione amministrativa".

A titolo meramente esemplificativo si possono menzionare i seguenti soggetti, nei quali la giurisprudenza ha individuato la qualifica di Pubblico Ufficiale: ufficiale giudiziario, consulente tecnico del giudice, curatore fallimentare, esattore o dirigente di aziende municipalizzate anche se in forma di S.p.A., assistente universitario, portalettere, consigliere comunale, geometra tecnico comunale, insegnante delle scuole pubbliche, ufficiale sanitario, notaio, dipendente dell'INPS, medico convenzionato con l'ASL.

Si segnala, altresì, come la Corte di cassazione abbia spiegato che, ai fini della determinazione della qualifica di "pubblico ufficiale" sia sempre necessario valutare le "specifiche mansioni svolte" dal soggetto².

1.2.3 Incaricati di un pubblico servizio

La definizione della categoria di "soggetti incaricati di un pubblico servizio" si rinviene all'art. 358 c.p. il quale recita che *"sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale"*.

Il legislatore puntualizza la nozione di "pubblico servizio" attraverso due ordini di criteri, uno positivo ed uno negativo. Il "servizio", affinché possa definirsi pubblico, deve essere disciplinato – del pari alla "pubblica funzione" - da norme di diritto pubblico, ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

Esempi di incaricati di pubblico servizio sono: i dipendenti delle autorità di vigilanza che non concorrono a formare la volontà dell'autorità e che non hanno poteri autoritativi, i dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati, gli impiegati degli uffici pubblici, ecc.

Il legislatore ha, inoltre, precisato che non può mai costituire "servizio pubblico" lo svolgimento di "semplici mansioni di ordine" né la "prestazione di opera meramente materiale". Con riferimento alle attività che vengono svolte da soggetti privati in base ad un rapporto concessorio con un soggetto pubblico, si ritiene che ai fini della definizione come pubblico servizio dell'intera attività svolta nell'ambito di tale rapporto concessorio non è sufficiente l'esistenza di un atto autoritativo di investitura soggettiva del pubblico servizio, ma è necessario accertare se le singole attività che vengono in questione siano a loro volta soggette a una disciplina di tipo pubblicistico.

La giurisprudenza ha individuato la categoria degli incaricati di un pubblico servizio, ponendo l'accento sul carattere della strumentalità ed accessorietà delle attività rispetto a quella pubblica in senso stretto.

Essa ha quindi indicato una serie di "indici rivelatori" del carattere pubblicistico dell'ente, per i quali è emblematica la casistica in tema di società per azioni a partecipazione pubblica. In particolare, si fa riferimento ai seguenti indici:

² Laddove queste siano *"funzioni prettamente pubblicistiche"*, tale qualifica può dirsi integrata (Cass. Pen., Sez. V, 28 giugno 2017, n. 31676, fattispecie in cui la Suprema Corte ha ritenuto qualificabile come pubblico ufficiale il *project manager* di una società partecipata da un ente pubblico).



- (a) la sottoposizione ad un'attività di controllo e di indirizzo a fini sociali, nonché ad un potere di nomina e revoca degli amministratori da parte dello Stato o di altri enti pubblici;
- (b) la presenza di una convenzione e/o concessione con la pubblica amministrazione;
- (c) l'apporto finanziario da parte dello Stato;
- (d) l'immanenza dell'interesse pubblico in seno all'attività economica.

Sulla base di quanto sopra riportato, l'elemento discriminante per indicare se un soggetto rivesta o meno la qualifica di "incaricato di un pubblico servizio" è rappresentato, non dalla natura giuridica assunta o detenuta dall'ente, ma dalle funzioni affidate al soggetto le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale.

CAPITOLO I.3 – LE ATTIVITÀ SENSIBILI NEI RAPPORTI CON LA P.A.

I.3.1 Attività Sensibili nei rapporti con la P.A.

Le Attività Sensibili nell'ambito dei Reati nei rapporti con la Pubblica Amministrazione e di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci che la Società ha individuato al proprio interno sono le seguenti:

- 1. Gestione dei rapporti con la Pubblica Amministrazione (di natura amministrativa o commerciale e compresi i rapporti con l'Amministrazione Finanziaria)**
- 2. Predisposizione delle comunicazioni alle Autorità di Vigilanza e gestione dei rapporti con le stesse**
- 3. Gestione dei rapporti con l'Autorità Giudiziaria (gestione di procedimenti in cui la Società è parte attiva/passiva) e partecipazione di esponenti aziendali a processi penali**
- 4. Gestione dei procedimenti volti all'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari e loro impiego**

I.3.2 Attività Strumentali alla commissione di reati di tipo corruttivo

Alcune attività che non comportano rapporti diretti con la P.A. possono tuttavia essere strumentali alla commissione della tipologia di reati di tipo corruttivo ("**Attività Strumentali**").

Ciò può accadere:

1. quando l'attività costituisce strumento di creazione di disponibilità occulte, da utilizzare per la corruzione di pubblici ufficiali;
2. quando l'attività costituisce il mezzo per corrispondere, direttamente o per interposta persona, ai funzionari pubblici, in forma occulta o indiretta, denaro o altra utilità in cambio di interessamenti indebiti.

Le Attività Strumentali che la Società ha individuato al proprio interno sono le seguenti:

- 1. Selezione di Fornitori, Consulenti e *Partner* e gestione dei relativi rapporti**
- 2. Gestione degli omaggi, spese di rappresentanza, sponsorizzazioni e beneficenze**
- 3. Gestione dei flussi finanziari**
- 4. Selezione, assunzione e gestione del personale (compresa la gestione dei rimborsi spese)**
- 5. Gestione dei Sistemi informatici e del patrimonio informativo aziendale (*rimando*)**

CAPITOLO I.4 - PRINCIPI GENERALI DI COMPORTAMENTO

I.4.1 Il sistema in linea generale

Obiettivo della presente Parte Speciale è che tutti i Destinatari adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire il verificarsi dei Reati in essa considerati.

Tutte le Attività Sensibili e le Attività Strumentali devono essere svolte conformandosi alle leggi vigenti, ai valori e alle politiche delle Società nonché alle regole contenute nel presente Modello.

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

La Società deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, *policy*, ecc.) improntati a principi generali di:

- a) conoscibilità all'interno della Società;
- b) chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri;
- c) chiara descrizione delle linee di riporto.

Le procedure interne adottate dalla Società devono essere caratterizzate dai seguenti elementi:

- a) massima separazione possibile, all'interno di ciascun processo, tra il soggetto che lo inizia (impulso decisionale), il soggetto che lo esegue e conclude, e il soggetto che lo controlla;
- b) traccia scritta di ciascun passaggio rilevante del processo;
- c) adeguato livello di formalizzazione;
- d) attenzione ad evitare che i sistemi premianti dei soggetti con poteri di spesa o facoltà decisionali a rilevanza esterna siano basati su target di performance sostanzialmente irraggiungibili.

I.4.2 Il sistema di deleghe e procure

In linea di principio, il sistema di deleghe e procure deve essere caratterizzato da elementi di "sicurezza" ai fini della prevenzione dei reati cd. presupposto (rintracciabilità ed evidenziabilità delle Attività Sensibili) e, nel contempo, consentire comunque la gestione efficiente dell'attività aziendale.

Si intende per "delega" l'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative. Si intende per "procura" il negozio giuridico unilaterale con cui la società attribuisce dei poteri di rappresentanza nei confronti dei terzi.

I requisiti essenziali del sistema di deleghe, ai fini di una efficace prevenzione dei Reati sono i seguenti:

- a) tutti coloro che intrattengono per conto della Società rapporti con la P.A. devono essere dotati di delega formale in tal senso (ovvero ricevere chiara indicazione di tale attribuzione, all'interno di documenti, politiche o regolamenti aziendali);
- b) le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e a una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;
- c) ciascuna delega deve definire in modo specifico e inequivoco i poteri del delegato e il soggetto (organo o individuo) cui il delegato riporta gerarchicamente;
- d) i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
- e) il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli.

I requisiti essenziali del sistema di attribuzione delle procure, ai fini di una efficace prevenzione dei Reati, sono i seguenti:

- a) le procure descrivono i poteri di gestione conferiti e, ove necessario, sono accompagnate da apposita comunicazione aziendale che fissi: l'estensione di poteri di rappresentanza ed i limiti di spesa numerici; ovvero i limiti assuntivi per categorie di rischio, richiamando comunque il rispetto dei vincoli posti dai processi di approvazione del *budget* e degli eventuali *extrabudget*, dai processi di monitoraggio delle Attività Sensibili da parte di funzioni diverse;
- b) la procura può essere conferita a persone fisiche espressamente individuate nella procura stessa, oppure a persone giuridiche che agiranno a mezzo di propri procuratori investiti, nell'ambito della stessa, di analoghi poteri;
- c) le procure speciali devono dettagliatamente stabilire l'ambito di operatività e i poteri del procuratore;
- d) un aggiornamento tempestivo delle procure, stabilendo i casi in cui le procure devono essere attribuite, modificate e revocate (assunzione o estensione di nuove responsabilità e poteri, trasferimento a diverse mansioni incompatibili con quelle per cui era stata conferita, dimissioni, licenziamento, revoca, ecc.).

L'OdV verifica periodicamente, con il supporto degli Esponenti della Società competenti, il sistema di deleghe e procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative (tali sono quei documenti interni all'azienda con cui vengono conferite le deleghe), raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie.

I.4.3 Principi generali di comportamento

I seguenti principi di carattere generale si applicano ai Destinatari del Modello sia direttamente sia in forza di apposite clausole contrattuali.

È fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di Reato rientranti tra quelle sopra considerate (artt. 24, 25 e 25-*decies* D.Lgs. 231/2001).

Inoltre:

- i rapporti con la Pubblica Amministrazione devono essere tenuti solamente dai soggetti formalmente delegati o muniti di procura siano essi dipendenti o collaboratori;
- i soggetti delegati devono operare nel rispetto dei poteri di rappresentanza, delle deleghe e delle procure loro conferite;
- i rapporti con la Pubblica Amministrazione devono essere improntati alla massima trasparenza, collaborazione, disponibilità e nel pieno rispetto del suo ruolo istituzionale e delle previsioni di legge esistenti in materia, delle norme comportamentali richiamate nel Codice Etico, nonché della presente Parte Speciale, dando puntuale e sollecita esecuzione alle sue prescrizioni ed agli adempimenti richiesti;
- è consigliato gestire i rapporti con i rappresentanti della Pubblica Amministrazione in presenza di almeno un altro soggetto;
- le informazioni che possono essere raccolte durante lo svolgimento della propria attività, qualunque sia il ruolo ricoperto, dovranno sempre intendersi come “riservate e confidenziali”. Tali informazioni non dovranno quindi essere comunicate a terzi (inclusi quindi soggetti legati direttamente o indirettamente alla Pubblica Amministrazione) al fine di concedere una qualsiasi potenziale forma di beneficio;
- gli adempimenti nei confronti della Pubblica Amministrazione devono essere effettuati con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere evitando di porre in essere condotte ingannevoli tali da indurre in errore i Funzionari Pubblici o gli Incaricati di Pubblico Servizio; i documenti devono essere elaborati in modo puntuale e in un linguaggio chiaro, oggettivo ed esaustivo;
- astenersi dalla partecipazione a eventuali associazioni di categoria, laddove risulti che le attività di *lobbying* svolte dall'ente associativo siano svolte in maniera non trasparente o comunque illecita;
- ciascuna funzione aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta nell'ambito della (propria) attività disciplinata nella presente sede, ivi inclusa quella trasmessa alla Pubblica Amministrazione in via telematica o elettronica. Tra questa, a mero titolo esemplificativo
 - o licenze, autorizzazioni e simili connesse all'attività di Compagnia Privata od ottenute ad altri fini nonché gli accordi con le controparti contrattuali soggetti pubblici / incaricati di pubblico servizio;

- atti, verbali, bilanci, dichiarazioni et similia relativi alla gestione degli affari legali, fiscali e societari oppure alla gestione amministrativa, previdenziale e assistenziale del personale;
 - verbali relativi a visite ispettive, procedure istruttorie e simili;
 - atti del contenzioso in materia civile, penale, amministrativa, tributaria, ecc.;
- la corresponsione dei corrispettivi maturati per effetto delle prestazioni rese alla Pubblica Amministrazione e/o ai soggetti ad essa assimilati deve avvenire in rigorosa osservanza dei contratti sottoscritti ed in stretta aderenza al loro effettivo svolgimento;
- qualunque conflitto di interessi o mancata conformità alle disposizioni aziendali interne dovesse sorgere nell'ambito dei rapporti con la Pubblica Amministrazione e/o con soggetti ad essa assimilati deve essere formalmente comunicati all'Organismo di Vigilanza, da parte dei diretti interessati.

Nei casi in cui dovessero verificarsi eventi straordinari ossia criticità non risolvibili nell'ambito della ordinaria gestione dei rapporti con la Pubblica Amministrazione, il personale deve immediatamente segnalare la situazione al proprio diretto superiore per le azioni del caso; il personale non può dare seguito e deve immediatamente segnalare per le azioni del caso al proprio responsabile qualunque tentativo di corruzione o concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente a conoscenza.

Nell'ambito dei suddetti comportamenti è fatto divieto in particolare di:

- a) promettere o accordare vantaggi di qualsiasi natura (denaro, regali, posti di lavoro, concessione di consulenze ecc.) in favore di rappresentanti della P.A. italiana o straniera, o a loro familiari, rivolti ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale o che possa comunque influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società;
- b) effettuare prestazioni in favore dei Consulenti, Fornitori e *Partner* che non trovino adeguata giustificazione nel contesto del rapporto contrattuale con gli stessi instaurato, nonché riconoscere compensi in favore dei medesimi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti nel settore;
- c) esibire documenti/dati falsi o alterati, sottrarre o omettere informazioni dovute al fine di orientare indebitamente a proprio favore le decisioni della Pubblica Amministrazione;
- d) presentare false dichiarazioni ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati o rendicontare in modo non veritiero l'attività per la quale sono già state effettuate delle erogazioni pubbliche;
- e) utilizzare contributi, sovvenzioni, finanziamenti, mutui agevolati o altre forme di erogazioni dello stesso tipo, comunque denominate, ottenute dallo Stato o da una Pubblica Amministrazione italiana o europea per scopi diversi da quelli a cui i medesimi sono destinati;

- f) indurre con violenza o minaccia, o, alternatively, con offerta di denaro o altra utilità, a rendere dichiarazioni o a rendere dichiarazioni mendaci, la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale;
- g) alterare il funzionamento di un sistema informatico o telematico, ovvero intervenire senza diritto su dati, informazioni o programmi utilizzati per lo scambio di dati con la Pubblica Amministrazione;
- h) adottare comportamenti contrari alle leggi e al Codice Etico in sede di: incontri formali e informali, anche a mezzo di professionisti esterni e soggetti terzi, per indurre giudici o arbitri (compresi gli ausiliari e i periti d'ufficio) a favorire indebitamente gli interessi della Società; decisione del contenzioso, anche a mezzo di professionisti esterni, per influenzare indebitamente le decisioni dell'organo giudicante o le posizioni della Pubblica Amministrazione quando questa sia controparte del contenzioso.

CAPITOLO I.5 - PRINCIPI SPECIFICI DI COMPORTAMENTO

Ai fini dell'attuazione delle regole elencate al precedente Capitolo, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali qui di seguito descritti per le singole Attività Sensibili. Tali principi potranno trovare attuazione anche per mezzo dell'adozione di specifiche procedure aziendali.

In relazione alle **Attività Sensibili** la Società adotta i seguenti principi procedurali.

1. Gestione dei rapporti con la Pubblica Amministrazione (di natura amministrativa o commerciale e compresi i rapporti con l'Amministrazione Finanziaria)

1. Ai Destinatari che materialmente intrattengono rapporti con la P.A. per conto della Società deve essere formalmente conferito potere in tal senso (con apposita delega ovvero nel relativo contratto per Fornitori, Consulenti o *Partner*). Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta che rispetti tutti i criteri elencati al precedente capitolo. In particolare, sono previsti diversi livelli autorizzativi in base ai quali:
 - tutti i soggetti che intervengono nel processo devono essere individuati e autorizzati;
 - gli atti che impegnano contrattualmente la Società devono essere sottoscritti da soggetti provvisti di delega;
 - sono definiti diversi profili di utenza per l'accesso a procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite;
2. È prevista la segregazione dei compiti nell'ambito della gestione dei rapporti con la Pubblica Amministrazione e/o con soggetti ad essa assimilati per la richiesta di autorizzazioni e/o esecuzione di adempimenti nel rispetto dei livelli autorizzativi definiti in base al sistema delle deleghe in essere;
3. Sono previste attività di controllo connesse alla gestione delle richieste di autorizzazione o esecuzione di adempimenti nei confronti della Pubblica Amministrazione e/o con soggetti ad essa assimilati. Le attività prevedono tra l'altro:
 - il monitoraggio del piano delle scadenze degli adempimenti (es. verso Enti Previdenziali);
 - la verifica della correttezza e completezza della documentazione da fornire alla Pubblica Amministrazione e/o a soggetti ad essa assimilati sia per l'esecuzione di adempimenti (es. verso Enti Previdenziali), sia per la richiesta di autorizzazioni;
 - la valutazione delle condizioni contrattuali nonché il rispetto dei livelli autorizzativi e la coerenza con le politiche aziendali;
 - la verifica della documentazione predisposta dalla Società per l'accesso a bandi di gara pubblici, in termini di veridicità e congruità sostanziale; l'attività è effettuata dal

responsabile della struttura aziendale competente in virtù dell'oggetto del contratto o da soggetti a ciò delegati, sulla base del sistema dei poteri e delle deleghe interni;

- l'autorizzazione circa la documentazione da inviare alla Pubblica Amministrazione e/o a soggetti ad essa assimilati;
 - l'applicazione di regole per la comunicazione, da parte dei dipendenti della SIM, della presenza e/o della possibile insorgenza di conflitti di interesse nei rapporti con l'Amministrazione Finanziaria o altra P.A. con le quali si viene in contatto in ragione dell'assolvimento delle attività lavorative.
4. La Società garantisce la tracciabilità dei processi sia a livello di sistema informativo sia in termini documentali:
- le strutture provvedono all'archiviazione della documentazione cartacea relativa alle attività poste in essere;
 - ciascuna struttura è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta, anche in via telematica o elettronica.
5. Alle verifiche e alle ispezioni condotte dalla Pubblica Amministrazione presso le sedi e le proprietà della Società (ad esempio, Banca d'Italia, Agenzia delle Entrate, Guardia di Finanza, ecc.) devono partecipare almeno due soggetti a ciò espressamente delegati. Di tutto il procedimento relativo all'ispezione devono essere redatti e conservati appositi verbali che diano atto dei rilievi eventualmente emersi.
6. In caso di partecipazione a gare pubbliche,
7. L'OdV deve essere prontamente informato sull'inizio di ogni attività di verifica e ispezione e aggiornato sugli esiti della stessa, mediante apposite comunicazioni inviate a cura del responsabile dell'ambito interessato.

2. Predisposizione delle comunicazioni alle Autorità di Vigilanza e gestione dei rapporti con le stesse

- La Società garantisce il rispetto della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nonché di quanto disposto e regolamentato dalle Autorità di Vigilanza (a titolo esemplificativo e non esaustivo: regolamenti Consob, provvedimenti di Banca d'Italia, provvedimenti dell'Autorità Garante in materia di Privacy, ecc.);
- la Società invia alle Autorità di Vigilanza le segnalazioni previste dalla legge e dai regolamenti o richieste ad altro titolo in modo tempestivo, completo e accurato, trasmettendo a tal fine tutti i dati e i documenti previsti o richiesti;
- nei rapporti con le suddette Autorità, è prevista la massima collaborazione e trasparenza, nonché la veridicità, la correttezza e la completezza di tutti i dati, le informazioni e i documenti comunicati e trasmessi dalla SIM.

- Sono previsti diversi livelli autorizzativi in base ai quali:
 - tutti i soggetti che intervengono nel processo devono essere individuati e autorizzati;
 - gli atti che impegnano contrattualmente la Società devono essere sottoscritti da soggetti provvisti di delega;
 - sono definiti diversi profili di utenza per l'accesso a procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite.
- È prevista la segregazione dei compiti nell'ambito della gestione dei rapporti con le Autorità di Vigilanza nel rispetto del sistema di deleghe aziendale;
- Sono previste attività di controllo connesse alla gestione dei rapporti con Autorità di Vigilanza. Le attività prevedono tra l'altro:
 - la verifica della completezza, correttezza e accuratezza dei dati o delle comunicazioni da trasmettere all'Autorità competente;
 - i controlli di carattere giuridico sulla conformità alla normativa di riferimento della segnalazione/comunicazione richiesta;
 - i controlli automatici di sistema, con riferimento alle segnalazioni periodiche;
 - il monitoraggio periodico sulle scadenze per l'invio di dati / comunicazioni obbligatorie alle Autorità;
 - la formalizzazione di verbali /note informative all'esito delle attività di ispezioni e/o evasione richieste da parte delle Autorità competenti;
 - l'applicazione di regole volte a disciplinare la comunicazione, da parte dei dipendenti della Società,
 - della presenza e/o della possibile insorgenza di conflitti di interesse nei rapporti con le Autorità con le quali si viene in contatto in ragione dell'assolvimento delle attività lavorative.
- La Società garantisce la tracciabilità dei processi sia a livello di sistema informativo sia in termini documentali:
 - è fatto obbligo a tutte le strutture della Società, a vario titolo coinvolte nella predisposizione e trasmissione di comunicazioni ed adempimenti alle Autorità di Vigilanza, di archiviare e conservare la documentazione di competenza prodotta nell'ambito della gestione dei rapporti con le Autorità, ivi inclusa quella trasmessa alle Autorità anche attraverso supporto elettronico. Tale documentazione deve essere resa disponibile a richiesta anche alle funzioni di controllo interne;

- ogni comunicazione nei confronti delle Autorità avente ad oggetto notizie e/o informazioni rilevanti sull'operatività della Società è documentata/registrata in via informatica ed archiviata presso la Struttura di competenza;
- fatte salve le situazioni in cui non sia previsto l'immediato rilascio di un verbale da parte dell'Autorità, il personale della struttura interessata che ha presenziato alla visita ispettiva presenza anche alla stesura da parte del funzionario pubblico del verbale di accertamento ed eventuale prescrizione, riservandosi le eventuali controdeduzioni, firmando, per presa visione il verbale, comprensivo degli allegati, prodotto dal funzionario stesso;
- a ogni visita ispettiva da parte di funzionari rappresentanti delle Autorità di Vigilanza, è compito del soggetto interessato (cosiddetto "Preposto") redigere il "Verbale interno di ispezione", ossia un documento riepilogativo delle attività espletate durante la visita ispettiva con eventuali osservazioni e della documentazione fornita, oltre a quella eventualmente non consegnata ai funzionari dell'Autorità di Vigilanza poiché non disponibile;
- il "Preposto" è tenuto, inoltre, alla conservazione di tale documento; qualora l'esito dell'ispezione preveda l'invio di ulteriore documentazione, il "Preposto" ne garantisce la trasmissione all'Autorità richiedente;
- il "Preposto" provvede ad aggiornare l'OdV sulla visita ispettiva avvenuta tramite l'invio del "Verbale interno di ispezione" all'apposito indirizzo di posta elettronica e provvede a comunicare all'OdV qualsiasi eccezione comportamentale o qualsiasi evento inusuale, indicando le ragioni delle difformità e dando atto del processo autorizzativo seguito.

3. Gestione dei rapporti con l'Autorità Giudiziaria (gestione di procedimenti in cui la Società è parte attiva/passiva) e partecipazione di esponenti aziendali a processi penali

1. La Società definisce i ruoli e le responsabilità dei soggetti incaricati di gestire il singolo contenzioso e le posizioni precontenziose. In particolare, le attività di controllo connesse alla gestione dei contenziosi prevedono tra l'altro:
 - l'applicazione di regole volte a disciplinare i criteri di valutazione e l'*iter* autorizzativo degli accordi transattivi;
 - la formalizzazione dell'affidamento dell'incarico ai consulenti legali, autorizzate nel rispetto dei poteri definiti;
 - l'applicazione di regole volte a disciplinare l'attività di condivisione ed autorizzazione degli atti difensivi redatti da consulenti legali incaricati;
 - il sistematico monitoraggio delle cause in corso;
 - la verifica della completezza e accuratezza dei dati o delle comunicazioni da trasmettere all'Autorità;

2. La Società garantisce la tracciabilità delle attività mediante l'archiviazione degli atti giudiziari.
3. È previsto un flusso informativo verso i vertici aziendali in merito alla situazione delle cause in corso.
4. È delegata all'Amministratore Delegato la facoltà di conferire l'incarico di gestire le attività giudiziarie e non giudiziarie a legali esterni, qualora ritenuto necessario, fermo restando l'obbligo di astensione nel caso lo stesso e la Società siano coinvolte di un medesimo procedimento penale;
5. In relazione all'attività sensibile in oggetto, gli amministratori, i dirigenti e i dipendenti agiscono nei limiti dei poteri e delle deleghe conferiti.
6. Il coinvolgimento di Consulenti per la gestione di controversie deve avvenire solo previa verifica della professionalità e dell'onorabilità dei medesimi.
7. L'Organismo di Vigilanza deve essere periodicamente aggiornato in occasione di eventi di rilievo, quali udienze importanti alle quali partecipino Esponenti della Società.

Si rinvia inoltre a quanto espressamente di seguito previsto in materia di selezione dei Consulenti.

4. Gestione dei procedimenti volti all'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari e loro impiego

1. La Società individua, prima dell'inizio del procedimento, i ruoli e le responsabilità delle funzioni interne ed esterne in merito al processo di gestione dell'accesso a contributi e sovvenzioni pubblici.
2. La Società assicura il monitoraggio costante – attraverso figure appositamente nominate all'inizio del processo – dell'avanzamento del progetto per il quale sono stati richiesti/ottenuti contributi pubblici e sull'eventuale relativa attività di *reporting* alla P.A., con evidenza e gestione delle eventuali anomalie.
3. La Società assicura l'effettuazione di controlli sull'effettivo impiego dei fondi erogati dagli organismi pubblici, in relazione agli obiettivi dichiarati dalla Società nella documentazione di richiesta.
4. Deve essere presentato un resoconto finale all'OdV circa l'impiego delle somme ricevute da un ente pubblico per lo scopo per cui erano state richieste.

In relazione alle **Attività Strumentali** la Società adotta i seguenti principi procedurali.

1. Selezione di Fornitori, Consulenti e Partner e gestione dei relativi rapporti

1. L'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente ai soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno.

2. Tutto il processo di acquisto è gestito nel rispetto della segregazione dei compiti e nel rispetto di specifici livelli autorizzativi.
3. I Consulenti, i Fornitori e i *Partner* devono essere scelti con metodi trasparenti (ad esempio, utilizzando apposite *vendor-list* contenenti l'indicazione delle controparti di fiducia cui si è legati da rapporti consolidati o una procedura formalizzata di *beauty contest*), sulla base di una opportuna valutazione sia in termini economici sia qualitativi delle proposte contrattuali di più parti (salvo deroghe espressamente autorizzate e motivate dalla peculiarità della prestazione ricercata – che non permetta di ottenere più proposte contrattuali – e/o dalla caratteristica di *intuitu personae* della medesima).
4. Le regole per la scelta del fornitore devono rispettare anche quanto previsto dal Codice Etico, al fine di prevenire il rischio che la sua scelta ricada su familiari o soggetti legati/vicini ad amministratori, direttori generali, dirigenti preposti alla formulazione dei documenti contabili societari, sindaci o liquidatori, nonché a soggetti sottoposti a quest'ultimi di un'altra società od ente, a fini corruttivi;
5. Nell'ambito dell'attività in oggetto è necessario motivare e tracciare la scelta del Fornitore, Consulente o *Partner* (che deve possedere gli effettivi requisiti tecnici/professionali/organizzativi e la potenzialità di erogazione della prestazione richiesta) assicurando l'archiviazione della relativa documentazione.
6. In relazione ai Consulenti, Fornitori e *Partner* principali e/o esposti a maggior rischio di commissione dei reati alla luce della tipologia dell'attività espletata, la Società effettua una *due diligence* rafforzata (anche avvalendosi di società specializzate) volta a scongiurare il rischio di instaurare rapporti con imprese legate alla criminalità organizzata.
7. Sia in fase di primo incarico sia periodicamente, ai Consulenti, Fornitori e *Partner* viene richiesta la presentazione di documentazione (eventualmente anche un'autocertificazione) comprovante il possesso dei necessari requisiti abilitativi e autorizzativi, con l'obbligo di comunicare senza ritardo l'eventuale venir meno di uno di detti requisiti (ad esempio, condanna per qualche reato o sanzione disciplinare dell'Ordine professionale di appartenenza).
8. I contratti con Consulenti, Fornitori e *Partner* devono essere definiti per iscritto in tutti i loro termini e condizioni.
9. In relazione alle attività esternalizzate, la Società verifica regolarmente il permanere delle condizioni di idoneità degli outsourcer a garantire il soddisfacimento delle condizioni imposte dalla normativa di riferimento e più in generale prese in considerazione in fase di selezione degli stessi.
10. I contratti con Consulenti, Fornitori e *Partner* devono prevedere un'apposita clausola (“**Clausola 231**”) con cui i medesimi affermino: (i) di essere a conoscenza della normativa di cui al D.Lgs. 231/2001, del Modello e delle sue implicazioni per la Società, (ii) di non essere

mai stati implicati in procedimenti giudiziari relativi ai Reati nello stesso contemplati e (iii) di impegnarsi al rispetto delle disposizioni del Modello ai medesimi applicabili.

11. I contratti con Consulenti, Fornitori e *Partner* devono prevedere le conseguenze della violazione da parte degli stessi degli obblighi assunti previsti al punto che precede (ad esempio, risoluzione del rapporto).
12. La Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta dal Consulente, Fornitore o *Partner*, anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione delle procedure acquisitive di beni e servizi.
13. La Società verifica, prima dell'effettuazione di pagamenti verso Consulenti, Fornitori e *Partner*, l'effettiva corrispondenza tra quanto previsto in fattura e quanto previsto nel contratto nonché l'effettiva esecuzione della prestazione secondo quanto contrattualmente pattuito.

2. Gestione degli omaggi, spese di rappresentanza, sponsorizzazioni e beneficenze

1. Tutte le erogazioni di fondi (destinate a omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni) devono essere approvate dai soggetti cui il sistema interno di poteri e deleghe riconosce tale facoltà.
2. È vietata ogni forma di omaggio o liberalità a terzi eccedente le normali pratiche commerciali o di cortesia o comunque rivolta ad acquisire indebitamente trattamenti di favore nella conduzione di qualsiasi attività della Società. **In particolare, è vietata qualsiasi forma di omaggio a rappresentanti della P.A. o a loro familiari che possa anche solo ragionevolmente apparire come idonea ad influenzarne l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società.** Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore.
3. Sono definiti i ruoli, le responsabilità, le modalità operative e i principi comportamentali cui attenersi nella gestione di qualsiasi distribuzione gratuita di beni e servizi a clienti, fornitori, dipendenti e soggetti terzi in generale;
4. la distribuzione degli omaggi deve rientrare nell'ambito dei rapporti di cortesia. Gli omaggi devono essere offerti esclusivamente in occasione di particolari ricorrenze (ad es.: festività natalizie) e devono essere tali da non influenzare la volontà del beneficiario e tali da non poter essere interpretati da un osservatore esterno imparziale come finalizzati ad acquisire vantaggi in modo improprio;
5. qualsiasi omaggio deve essere documentato e autorizzato, nonché conforme ai principi stabiliti nel presente Modello e nel Codice Etico;
6. in relazione alle spese di rappresentanza, è prevista la preventiva autorizzazione motivata da parte del Responsabile della struttura interessata alla spesa.
7. La Società garantisce la registrazione di ogni regalia eventualmente resa.

8. È vietato offrire o dare denaro, regali, ospitalità o altri oggetti di valore, direttamente o tramite altri, a funzionari, dipendenti o rappresentanti di qualsiasi Cliente, o di qualsiasi altra organizzazione, se ciò potrebbe ragionevolmente dare l'impressione di influenzare il rapporto tra tali soggetti e la Società.
9. Non sono consentiti omaggi in denaro contante o equivalenti in contanti (quali, ad esempio, buoni benzina o buoni spesa).
10. Il processo di gestione delle spese di rappresentanza, delle donazioni e degli omaggi, nonché delle sponsorizzazioni deve essere puntualmente tracciato, al fine di garantirne la trasparenza e la verificabilità. Tutta la documentazione inerente a tali attività deve essere adeguatamente conservata e archiviata a cura delle Funzioni coinvolte. In aggiunta, i regali offerti devono essere documentati in modo adeguato.

3. Gestione dei flussi finanziari

1. Tutti i flussi finanziari in entrata e in uscita devono essere adeguatamente identificabili e tracciabili, nonché correttamente e regolarmente registrati in appositi libri e registri contabili.
2. Tutti i flussi finanziari in entrata e in uscita devono essere supportati da specifica documentazione giustificatrice, che riporti chiaramente e fedelmente le transazioni a cui fa riferimento.
3. È previsto un sistema di monitoraggio e di *reporting* periodico dell'andamento dei flussi di cassa della Società.
4. La Società garantisce il principio di segregazione dei ruoli tra i soggetti che autorizzano, coloro che eseguono e coloro che controllano i flussi finanziari in entrata e in uscita nel rispetto dei limiti di spesa coerenti con le responsabilità organizzative e con le competenze gestionali.
5. La Società individua preventivamente gli Esponenti aziendali a cui sono conferiti i poteri di spesa attraverso apposite procure ovvero delibere del Consiglio di Amministrazione, al fine di garantire la chiara individuazione a posteriori del soggetto avente i poteri di spesa per ogni transazione finanziaria effettuata.
6. Sono stabiliti adeguati limiti all'autonomo impiego delle risorse finanziarie, attraverso la definizione di limiti di spesa coerenti con le responsabilità organizzative e con le competenze gestionali.
7. Sono sempre tracciabili le movimentazioni finanziarie effettuate dalla Società, i soggetti che le hanno predisposte e autorizzate e le motivazioni sottostanti le entrate e le uscite di denaro.
8. Tutte le operazioni che comportano l'impiego di risorse economiche o finanziarie sono documentate e registrate in conformità ai principi di correttezza professionale e contabile.
9. La documentazione inerente alle movimentazioni finanziarie deve essere adeguatamente conservata e archiviata.

10. Il pagamento delle fatture può avvenire solo previa autorizzazione dell'unità aziendale richiedente il bene servizio che attesti l'avvenuta consegna del bene / regolare esecuzione della prestazione, nonché previo controllo amministrativo contabile delle fatture stesse rispetto ai contratti / ordini di acquisto / lettere di conferimento.
11. Sono previsti sistemi di controllo e di autorizzazione degli utilizzi di risorse finanziarie che eccedono i limiti determinati in sede di definizione del *budget*.
12. La Società effettua controlli dei flussi finanziari aziendali in entrata ed uscita; tali controlli devono tener conto degli istituti di credito utilizzati (sede delle banche coinvolte nelle operazioni) e di eventuali schermi societari e strutture fiduciarie utilizzate per eventuali operazioni straordinarie, nonché della sede legale della società controparte e del luogo di destinazione o provenienza del denaro in uscita o in entrata (ad esempio, paradisi fiscali, Paesi rientranti nelle *black-list* internazionali, ecc.).
13. È fatto divieto di trasferimento di denaro contante o di titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) in Euro o in valuta estera, effettuato a qualsiasi titolo quando il valore dell'operazione è pari o superiore a quello di legge. Il trasferimento può tuttavia essere eseguito per il tramite di banche, istituti di moneta elettronica e Poste Italiane S.p.A.

4. Selezione, assunzione e gestione del personale (compresa la gestione dei rimborsi spese)

- La Società in relazione alle attività in oggetto garantisce la segregazione dei compiti in base ai livelli autorizzativi definiti dal sistema di deleghe e dalla normativa aziendale.
- Il processo di selezione e assunzione del personale deve avvenire secondo criteri di trasparenza basati sui seguenti parametri:
 - individuazione dei soggetti competenti a gestire le assunzioni;
 - strutturazione del processo di selezione e assunzione lungo più fasi, con coinvolgimento di più funzioni/soggetti;
 - applicazione di criteri oggettivi – basati sulla parità di trattamento e sulla valorizzazione del merito e della professionalità – nella scelta del candidato più idoneo all'assunzione e nell'individuazione del relativo inquadramento e trattamento;
 - verifica dell'assenza di elementi ostativi all'instaurazione del rapporto di lavoro e della professionalità adeguata rispetto all'incarico o alle mansioni da assegnare;
 - esclusione di qualsiasi interferenza da parte di soggetti terzi nel processo di assunzione del personale dipendente.
- L'attività di gestione amministrativa del personale è supportata da un sistema gestionale, il cui utilizzo consente la tracciabilità di ogni fase del processo.

- Eventuali avanzamenti interni di carriera e riconoscimenti di premi (ivi compresa l'eventuale previsione, nel trattamento retributivo, di una componente variabile legata al raggiungimento di specifici obiettivi) devono essere assegnati secondo criteri oggettivi, basati sulla parità di trattamento e sulla valorizzazione del merito e della professionalità.
- Al neoassunto viene consegnata copia del Modello e del Codice Etico e viene chiesto di firmare una dichiarazione di presa visione e impegno al rispetto di tali documenti.
- In particolare, sono presenti attività di controllo che prevedono tra l'altro
 - un sistematico monitoraggio della rilevazione presenze al fine di individuare eventuali anomalie;
 - l'applicazione di regole volte a disciplinare le modalità di selezione del personale;
 - il monitoraggio e la valutazione annuale della prestazione professionale del personale di Compagnia Privata, ovvero del contributo fornito da ogni dipendente allo svolgimento della mission aziendale e al raggiungimento degli obiettivi fissati dall'azienda;
 - l'applicazione di regole volte a disciplinare le politiche di remunerazione e di incentivazione;
 - l'applicazione di regole volte a disciplinare l'iter autorizzativo delle richieste di ferie / straordinari /permessi;
 - l'applicazione di regole volte a disciplinare: le richieste di rimborso delle spese di trasferta / missione dei dipendenti; le modalità di autorizzazione a sistema da parte del responsabile della funzione competente delle note spese, a seguito della verifica dei relativi giustificativi.
- Le spese effettuate da Esponenti aziendali per conto della Società devono essere caratterizzate da attinenza all'attività di business.
- Le spese sostenute da Esponenti della Società per conto di questa possono essere rimborsate solo previa presentazione di idonee pezze giustificative.

6. Gestione dei Sistemi informatici e del patrimonio informativo aziendale (*rimando*)

Relativamente ai presidi adottati dalla SIM al fine di prevenire il potenziale rischio di commissione o tentata commissione di Reati previsti dalla presente Parte Speciale mediante l'impiego di sistemi informatici, si rinvia a quanto indicato al riguardo nella Parte Speciale VII dedicata ai delitti informatici.

* * *

Per ogni aspetto di maggiore dettaglio riferibile – anche indirettamente – alle Attività Sensibili sopra indicate e, in generale, alla prevenzione del rischio di commissione di Reati Presupposto astrattamente rilevanti in relazione alla presente Parte Speciale, si rimanda anche espressamente – *inter alia* – al contenuto dei seguenti documenti normativi interni:



- *policy* di gestione delle risorse umane;
- *policy* di remunerazione e incentivazione;
- *policy* delle funzioni esternalizzate;
- *policy* di gestione dei conflitti di interesse;
- *Policy* delle funzioni esternalizzate e in *Cloud*.

CAPITOLO I.6 – FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

Con riferimento alla presente Parte Speciale, ogni funzione coinvolta deve comunicare per quanto di competenza e con periodicità definita quanto previsto nella seguente tabella (si precisa che i flussi in oggetto, all'occorrenza, possono eventualmente essere forniti in occasione di incontri *de visu* con l'OdV):

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
<i>Compliance</i>	Descrizione delle attività rilevanti intercorse con la Pubblica Amministrazione e Autorità di Vigilanza.	Annuale
<i>Compliance</i>	Segnalazione di eventuali criticità o conflitti di interesse riscontrati nei rapporti con la Pubblica Amministrazione.	Ad evento
<i>Compliance</i>	Elenco e copia delle deleghe e procure rilasciate a Esponenti Aziendali e/o Consulenti al fine di intrattenere rapporti con la Pubblica Amministrazione.	Annuale
<i>Compliance</i>	Elenco dei principali contenziosi giudiziali e stragiudiziali in corso e breve descrizione dello stato di ciascuno di essi.	Annuale
<i>Compliance</i>	Elenco delle ispezioni ricevute e/o in corso, specificando: i) Pubblica Amministrazione/Autorità di Vigilanza procedente; ii) soggetti partecipanti e iii) periodo di svolgimento; iv) esito. Trasmissione dei verbali d'ispezione che diano evidenza di criticità.	Ad evento
<i>Compliance</i>	Segnalazione di criticità riscontrate nella gestione di eventuali erogazioni pubbliche.	Ad evento
<i>Compliance</i>	Informativa in merito all'erogazione di omaggi o donazioni e all'effettuazione di sponsorizzazioni, con indicazione dei soggetti coinvolti.	Annuale
<i>Compliance</i>	Elenco del personale assunto nel periodo di riferimento, con indicazione: i) dell'inquadramento e delle mansioni; ii) delle procedure seguite per la selezione; iii) dei controlli svolti sulla sussistenza dei requisiti per l'assunzione.	Annuale



PARTE SPECIALE – II – Reati Societari (ivi inclusi i Reati di corruzione tra privati)

CAPITOLO II.1 - LE FATTISPECIE DI REATO

II.1.1 Le ipotesi di falsità

FALSE COMUNICAZIONI SOCIALI (ART. 2621 C.C.)

FATTI DI LIEVE ENTITÀ (ART. 2621-BIS C.C.)

L'ipotesi di reato di cui all'art. 2621 c.c. si configura nel caso in cui nell'intento di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, vengano esposti, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero, ovvero vengano omessi fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione.

Ai sensi dell'art. 2621-bis c.c., inoltre, qualora i fatti richiamati al precedente art. 2621 c.c. costituiscano fatti di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta, troveranno applicazione pene in misura ridotta rispetto a quelle previste ai sensi dell'art. 2621 c.c. sopra indicato. Le predette pene troveranno applicazione altresì allorquando i fatti di cui all'articolo 2621 c.c. riguardino società che non superano i limiti indicati dal secondo comma dell'articolo 1 del Regio Decreto 16 marzo 1942, n. 267. In tale caso, il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale.

FALSE O OMESSE DICHIARAZIONI PER IL RILASCIO DEL CERTIFICATO PRELIMINARE (ART. 54 D.LGS. 19/2023)

La norma punisce chiunque, al fine di far apparire adempiute le condizioni per il rilascio del certificato preliminare di cui all'articolo 29 del D.Lgs. 19/2023 (ovverosia, il certificato attraverso il quale l'autorità preposta – per quanto riguarda lo Stato italiano, il notaio – verifica e attesta il rispetto dei requisiti di legalità per la realizzazione dell'operazione transfrontaliera), forma documenti in tutto o in parte falsi, altera documenti veri, rende dichiarazioni false oppure omette informazioni rilevanti.

II.1.2 La tutela del capitale sociale

INDEBITA RESTITUZIONE DEI CONFERIMENTI (ART. 2626 C.C.)

Il reato in questione, come quello previsto dal successivo art. 2627 c.c., riguarda la tutela dell'integrità del capitale sociale e si compie quando gli amministratori, in assenza di legittime ipotesi di riduzione del capitale sociale, provvedono a restituire, anche per equivalente, i conferimenti effettuati dai soci ovvero liberano i soci dall'obbligo di eseguirli. Il reato in esame assume rilievo solo quando, per effetto degli atti compiuti dagli amministratori, si intacca il capitale sociale e non i fondi o le riserve. Per questi ultimi, eventualmente, sarà applicabile il reato contemplato dal successivo art. 2627 c.c.

La restituzione dei conferimenti può essere palese (quando gli amministratori restituiscono beni ai soci senza incasso di alcun corrispettivo o rilasciano dichiarazioni dirette a liberare i soci dai loro obblighi di versamento) ovvero, più probabilmente, simulata (quando per realizzare il loro scopo gli amministratori utilizzano stratagemmi o artifici quali, per esempio, la distribuzione di utili fittizi con somme prelevate dal

capitale sociale e non dalle riserve, oppure la compensazione del credito vantato dalla società con crediti inesistenti vantati da uno o più soci).

Soggetti attivi del reato possono essere solo gli amministratori. 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 della condotta illecita degli amministratori.

ILLEGALE RIPARTIZIONE DEGLI UTILI E DELLE RISERVE (ART. 2627 C.C.)

Tale ipotesi di reato consiste nella ripartizione di utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, ovvero nella ripartizione di riserve (anche non costituite con utili) che non possono per legge essere distribuite.

Si fa presente che la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Soggetti attivi del reato sono gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della ripartizione degli utili o delle riserve, 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 della condotta illecita degli amministratori.

ILLECITE OPERAZIONI SULLE AZIONI O QUOTE SOCIALI O DELLA SOCIETÀ CONTROLLANTE (ART. 2628 C.C.)

Tale ipotesi di reato consiste nel procedere – fuori dai casi consentiti dalla legge – all'acquisto o alla sottoscrizione di azioni o quote emesse dalla società (o dalla società controllante) che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

La norma è diretta alla tutela dell'effettività e integrità del capitale sociale e non può prescindere dall'analisi di cui all'art. 2357 c.c. il quale prevede che la società per azioni non può acquistare azioni proprie, nemmeno tramite società fiduciaria o interposta persona, se non nei limiti degli utili distribuibili o delle riserve disponibili risultanti dall'ultimo bilancio regolarmente approvato. La norma prevede che le azioni devono essere interamente liberate e che, inoltre, non possono essere acquistate azioni eccedenti la decima parte del capitale sociale, tenuto conto anche delle azioni possedute dalle società controllate.

Tra le fattispecie tramite le quali può essere realizzato l'illecito vanno annoverate non solo le ipotesi di semplice acquisto ma anche quelle di trasferimento della proprietà delle azioni, per esempio, mediante permuta o contratti di riporto, o anche quelle di trasferimento senza corrispettivo, quale la donazione.

Soggetti attivi del reato sono gli amministratori. Inoltre, è configurabile una responsabilità a titolo di concorso degli amministratori della controllante con quelli della controllata, nell'ipotesi in cui le operazioni illecite sulle azioni della controllante medesima siano effettuate da questi ultimi su istigazione dei primi.

OPERAZIONI IN PREGIUDIZIO DEI CREDITORI (ART. 2629 C.C.)

Tale ipotesi di reato consiste nell'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o di fusioni con altra società o di scissioni, tali da cagionare danno ai creditori.

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

Il reato è punibile a querela di parte.

Soggetti attivi del reato sono, anche in questo caso, gli amministratori.

FORMAZIONE FITTIZIA DEL CAPITALE (ART. 2632 C.C.)

Tale ipotesi di reato è integrata dalle seguenti condotte:

- a) formazione o aumento in modo fittizio del capitale sociale, anche in parte, mediante attribuzione di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale;
- b) sottoscrizione reciproca di azioni o quote;
- c) sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

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

INDEBITA RIPARTIZIONE DEI BENI SOCIALI DA PARTE DI LIQUIDATORI (ART. 2633 C.C.)

Tale ipotesi di reato consiste nel procedere, da parte di liquidatori con la ripartizione dei beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, con danno cagionato ai creditori. I liquidatori sono puniti a querela della persona offesa. Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

B.1.3 La tutela del corretto funzionamento della società

IMPEDITO CONTROLLO (ART. 2625 C.C.)

Tale ipotesi di reato consiste nell'impedire od ostacolare, mediante occultamento di documenti o con altri idonei artifici, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali.

L'illecito può essere commesso esclusivamente dagli amministratori.

ILLECITA INFLUENZA SULL'ASSEMBLEA (ART. 2636 C.C.)

Tale ipotesi di reato consiste nel determinare la maggioranza in assemblea con atti simulati o fraudolenti, allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Tra gli interventi che sono suscettibili di integrare il reato in questione, si possono annoverare ad esempio l'ammissione al voto di soggetti non aventi diritto (perché, ad esempio, in conflitto di interessi con la delibera in votazione) o la minaccia o l'esercizio della violenza per ottenere dai soci l'adesione alla delibera o la loro astensione.

Il reato è costruito come un reato comune, che può essere commesso da “chiunque” ponga in essere la condotta criminosa.

II.1.4 La tutela penale contro le frodi

AGGIOTAGGIO (ART. 2637 C.C.)

Tale ipotesi di reato consiste nel diffondere notizie false ovvero nel realizzare operazioni simulate o altri artifici, concretamente idonei a provocare 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, ovvero nell'incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o gruppi bancari.

Anche questo è un reato comune, che può essere commesso da “chiunque” ponga in essere la condotta criminosa.

II.1.5 La corruzione tra privati (art. 2635 c.c.)

La Legge 6 novembre 2012, n. 190 recante “*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*” ha introdotto nel nostro ordinamento giuridico e, precisamente, all'art. 2635 c.c. il reato di “*corruzione tra privati*”, riscrivendo la precedente fattispecie di reato societario concernente l’*“infedeltà a seguito di dazione o promessa di utilità”*.

A differenza della precedente fattispecie di reato, l'attuale art. 2635 c.c. è stato inserito - limitatamente alla condotta corruttiva attiva - nel novero dei Reati Presupposto ex D.Lgs. 231/2001 (attuale art. 25-ter co. 1, lettera s-bis), prevedendo, quindi, l'estensione della responsabilità amministrativa degli enti anche al reato di “*corruzione tra privati*”.

L'Articolo in parola è poi stato oggetto di ulteriori modifiche, l'ultima delle quali intervenuta con D.Lgs. 15 marzo 2017, n. 38. A seguito di detta modifica, l'art. 2635 c.c. recita come segue:

“Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità per compiere o omettere un atto, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da uno a tre anni. Si applica la stessa pena se il fatto è commesso da chi nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo.

Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma.

Chi, anche per interposta persona, offre, promette o dà denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste.

Le pene stabilite nei commi precedenti sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi

dell'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.

Fermo quanto previsto dall'articolo 2641, la misura della confisca per valore equivalente non può essere inferiore al valore delle utilità date, promesse e offerte”.

La fattispecie si configura come reato a concorso necessario, per cui è essenziale che siano poste in essere due condotte corruttive:

- a. la condotta corruttiva attiva di colui che dà offre o promette denaro o altra utilità ai soggetti di cui all'art. 2635 co. 1;
- b. la condotta corruttiva passiva di colui che – avendo ricevuto o essendo destinatario di una promessa di denaro o altra utilità, per sé o per altri – compia od ometta atti, in violazione dei propri obblighi d'ufficio o di fedeltà.

Si noti che la condotta corruttiva passiva può essere compiuta solo dai soggetti specificamente elencati nel comma primo dell'art. 2635 c.c. e che, quindi, possono essere corrotti solo coloro che ricoprono i seguenti ruoli in società (o enti privati):

- gli amministratori;
- i direttori generali;
- i dirigenti preposti alla redazione dei documenti contabili societari;
- i sindaci;
- i liquidatori;
- altri soggetti che esercitano attività direttive nella società
- soggetti sottoposti alla direzione o alla vigilanza dei predetti soggetti qualificati.

L'eliminazione del riferimento al “documento alla società” – prima della modifica di cui al D.lgs. 15 marzo 2017, n. 38 presupposto necessario della configurabilità del reato – comporta un'anticipazione del momento consumativo e pone l'accento non più sul danno subito dall'ente in seguito alla condotta delittuosa dell'agente, ma sulla violazione da parte di quest'ultimo degli obblighi di ufficio o di fedeltà.

La Legge 9 gennaio 2019, n. 3, recante «*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*», ha eliminato dalla fattispecie la previsione della procedibilità a querela della persona offesa. Il presente reato è dunque procedibile d'ufficio.

II.1.6 Istigazione alla corruzione tra privati (art. 2635-bis c.c.)

Il sopra citato D.Lgs. 15 marzo 2017, n. 38 ha, altresì, introdotto nell'ordinamento una nuova fattispecie di reato, denominata “Istigazione alla corruzione tra privati”, prevista e punita dall'art. 2635 *bis* c.c., che recita come segue:

“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 od ometta un atto in violazione degli obblighi inerenti al proprio ufficio 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.

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”.

Le fattispecie in esame sono state, inoltre, inserite nel catalogo dei reati presupposto della responsabilità amministrativa degli enti, all’art. 25-ter, lett. s bis del Decreto 231.

In particolare, ai fini dell’applicazione della responsabilità amministrativa degli enti ex Decreto 231 – come per la fattispecie di corruzione tra privati ex art. 2635 c.c. – rileva la sola condotta cosiddetta “attiva”, in virtù del richiamo che l’art. 25-ter, lett. s bis, del Decreto 231 fa al primo comma dell’art. 2635-bis c.c. (*“Chiunque offre o promette [...]”*).

La Legge 9 gennaio 2019, n. 3, recante «*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*», ha eliminato dalla fattispecie la previsione della procedibilità a querela della persona offesa. Il presente reato è dunque procedibile d’ufficio.

CAPITOLO II.2.1 – LE ATTIVITÀ SENSIBILI NELL’AMBITO DEI REATI SOCIETARI

Le Attività Sensibili nell’ambito dei Reati in oggetto che la Società ha individuato al proprio interno sono le seguenti:

- 1. Formazione e tenuta della contabilità, del bilancio d’esercizio, delle relazioni e di altre comunicazioni societarie previste dalla legge**
- 2. Predisposizione delle comunicazioni alle Autorità di Vigilanza e gestione dei rapporti con le stesse**
- 3. Gestione delle operazioni societarie, delle attività assembleari e dei rapporti tra soci e tra organi sociali**
- 4. Gestione delle operazioni con Parti Correlate.**
- 5. Gestione e divulgazione delle informazioni e delle comunicazioni verso l’esterno**

CAPITOLO II.2.2 – LE ATTIVITÀ SENSIBILI E STRUMENTALI NELL’AMBITO DEI REATI DI CORRUZIONE TRA PRIVATI

Le Attività Sensibili nell’ambito dei reati di corruzione tra privati che la Società ha individuato al proprio interno sono le seguenti:

- 1. Gestione dei rapporti con gli istituti bancari, assicurativi e finanziari**
- 2. Gestione delle controversie e conclusione di accordi transattivi**

In relazione ai reati di corruzione tra privati, le Attività Strumentali che la Società ha individuato al proprio interno sono le seguenti:

- 1. Selezione di Fornitori, Consulenti e *Partner* e gestione dei relativi rapporti**
- 2. Gestione degli omaggi, spese di rappresentanza, sponsorizzazioni e beneficenze**
- 3. Gestione dei flussi finanziari**
- 4. Selezione, assunzione e gestione del personale (compresi i rimborsi spese)**

CAPITOLO II.3 - PRINCIPI GENERALI DI COMPORTAMENTO

Obiettivo della presente Parte Speciale, al fine di prevenire la commissione dei Reati in oggetto, è che tutti i Destinatari del Modello si attengano – nei limiti delle rispettive competenze – a regole di condotta conformi a quanto quivi prescritto.

II.3.1 Il sistema in linea generale

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello e, in particolare, a quelle indicate ai successivi paragrafi, i Destinatari devono in generale conoscere e rispettare:

1. le vigenti prassi aziendali, la documentazione e le disposizioni inerenti alla struttura gerarchico-funzionale aziendale ed organizzativa ed il sistema di controllo della gestione, che si intendono qui interamente richiamate;
2. le norme inerenti al sistema amministrativo, contabile e finanziario attualmente esistenti;
3. la normativa italiana applicabile.

I Destinatari, inoltre, sono tenuti ad operare sulla base delle *best practice* cui Compagnia Privata si ispira nell'esercizio delle proprie funzioni e sul fondamento che qualsiasi condotta attiva od omissiva posta in essere in violazione diretta od indiretta dei principi normativi e delle regole procedurali interne che attengono alla formazione della documentazione contabile ed alla rappresentazione esterna, così come all'esercizio delle attività di controllo e di vigilanza è da considerare come commessa in danno della Società stessa.

CAPITOLO II.3.1 - PRINCIPI GENERALI DI COMPORTAMENTO

La presente Parte Speciale prevede l'espresso divieto a carico dei Destinatari di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-ter, D.Lgs. 231/2001) e che, sebbene non costituiscano di per sé un'ipotesi di reato, possano esserne il presupposto (ad es. mancato controllo).

La presente Parte Speciale prevede, conseguentemente, l'espresso obbligo di:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle prassi aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
2. tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di Reato rientranti tra quelle sopra considerate, possano potenzialmente diveltarlo;
3. osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
4. assicurare il regolare funzionamento della Società e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare nel rispetto delle leggi vigenti. In ordine a tale punto, è fatto divieto di:
 - tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante
 - l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione svolte dalle Autorità di Vigilanza (quali, a titolo esemplificativo, Banca d'Italia, Consob, Covip, ecc.), dal Collegio Sindacale, della società di revisione o dei soci;
 - porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
5. astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false o non corrette, idonee a provocare 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.

Per quanto riguarda gli strumenti finanziari quotati o per i quali è stata presentata una richiesta di ammissione alle negoziazioni o in un mercato regolamentato, si rinvia a quanto previsto nella Parte Speciale relativa ai reati ed illeciti amministrativi riconducibili ad abusi di mercato.

Nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di:

- a) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà sulla situazione economica, patrimoniale e finanziaria della Società;
- b) omettere di effettuare, con la dovuta chiarezza, completezza e tempestività, nei confronti delle Autorità in questione, (i) tutte le comunicazioni, periodiche e non, previste dalla legge e dalla ulteriore normativa di settore, nonché (ii) la trasmissione dei dati e documenti previsti dalle norme in vigore e/o specificamente richiesti dalle predette Autorità;
- c) esporre in tali comunicazioni e nella documentazione trasmessa fatti non rispondenti al vero oppure occultare fatti concernenti la situazione economica, patrimoniale o finanziaria della Società;
- d) porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle Autorità pubbliche di Vigilanza, anche in sede di ispezione (espressa opposizione, rifiuti pretestuosi, comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti);
- e) restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- f) ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- g) acquistare o sottoscrivere quote o azioni della Società o di società controllate fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;
- h) effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- i) procedere a formazione e/o aumenti fittizi del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale;
- j) porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che, in altro modo, ostacolino lo svolgimento dell'attività di controllo attribuite ai soci;
- k) determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- l) pubblicare o divulgare notizie false, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento o ingannatorio suscettibili di determinare riflessi su strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di

ammissione alle negoziazioni in un mercato regolamentato e idonei ad alterarne sensibilmente il prezzo;

- m) promettere o accordare – anche per mezzo dell'intermediazione di terzi – vantaggi di qualsiasi natura (denaro, regali, posti di lavoro, concessione di consulenze ecc.) in favore di terzi aventi rapporti d'affari con la Società, rivolti ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale o che possano comunque ragionevolmente influenzare l'indipendenza di giudizio del terzo o indurre il medesimo ad assicurare un qualsiasi vantaggio per la Società;
- n) effettuare prestazioni in favore dei Consulenti, Fornitori e Partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale con gli stessi instaurato, nonché riconoscere compensi in favore dei medesimi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti nel settore.

CAPITOLO II.4.1 - PRINCIPI SPECIFICI DI COMPORTAMENTO IN RELAZIONE AI REATI SOCIETARI

Ai fini dell'attuazione delle regole elencate al precedente Capitolo, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali qui di seguito descritti per le singole Attività Sensibili. Tali principi potranno trovare attuazione anche per mezzo dell'adozione di specifiche procedure aziendali.

1. Formazione e tenuta della contabilità, del bilancio d'esercizio, delle relazioni o di altre comunicazioni societarie previste dalla legge

1. La Società garantisce:

- (i) che il bilancio sia predisposto sulla base dei principi generali di redazione e criteri di valutazione conformi ai principi contabili applicabili;
- (ii) la tracciatura dei flussi e l'identificazione dei soggetti che alimentano la trasmissione dei dati contabili e finanziari necessari alla predisposizione del bilancio d'esercizio;
- (iii) la massima tracciabilità dei suddetti processi, onde permettere l'individuazione di eventuali errori/scostamenti;
- (iv) il rispetto del principio di segregazione dei ruoli, distribuendo i compiti inerenti all'amministrazione e alla contabilità tra più soggetti (ad esempio, distinzione tra soggetti che autorizzano un processo, soggetti che lo eseguono e soggetti che lo controllano);
- (v) la trasmissione della bozza di bilancio agli amministratori con ragionevole anticipo rispetto alla riunione del Consiglio di Amministrazione chiamato a deliberare sull'approvazione dello stesso;
- (vi) l'approntamento di adeguate difese fisiche e/o informatiche a protezione dei luoghi in cui sono custodite le scritture contabili in modo da impedire eventuali atti di distruzione e/o occultamento.

2. La Direzione Amministrazione, nel rispetto delle norme civilistiche e fiscali vigenti, assicura il coordinamento e il controllo degli adempimenti contabili relativi alla gestione economica, patrimoniale e finanziaria della Società, al fine di garantire la corretta formazione del bilancio d'esercizio.

3. La documentazione di supporto dell'attività in oggetto è archiviata in modo da consentire una facile consultazione sia da parte degli organi interni preposti al controllo sia da parte di enti ed istituzioni esterne adeguatamente autorizzate.

4. Compagnia Privata verifica che la Società di Revisione incaricata della revisione legale soddisfi i requisiti di indipendenza stabiliti dalla normativa vigente.

5. Il sistema informatico utilizzato garantisce la tracciabilità delle informazioni contabili e l'identificazione delle Funzioni aziendali che alimentano il sistema stesso; per ciascuna registrazione contabile, inoltre, è conservata un'adeguata documentazione di supporto.
6. Sono previste riunioni periodiche tra la Società di Revisione, il Comitato per il Controllo Interno e il Collegio Sindacale, aventi ad oggetto la valutazione dell'adeguatezza dei principi contabili utilizzati e la loro omogeneità ai fini della redazione del bilancio, nonché la valutazione dei risultati esposti nella relazione di certificazione e nelle lettere di suggerimenti della Società di Revisione.
7. Tra le attività di controllo previste in relazione all'attività in oggetto – rinviando ovviamente nel dettaglio alle procedure applicabili – sono comprese:
 - l'applicazione di regole volte a disciplinare il processo di produzione dei dati per la contabilità e dei *report* gestionali;
 - la verifica di correttezza e completezza delle informazioni relative alle registrazioni contabili;
 - la verifica di correttezza e completezza delle informazioni necessarie alla redazione dei documenti di bilancio;
 - l'applicazione di regole volte a disciplinare l'esecuzione degli adempimenti per il deposito del Bilancio a seguito della approvazione;
 - la verifica con cadenza periodica dei saldi di contabilità generale.

2. Predisposizione delle comunicazioni alle Autorità di Vigilanza e gestione dei rapporti con le stesse

Trattasi dei rapporti con le Autorità di Vigilanza in merito agli adempimenti previsti in tema di comunicazioni dei dati societari.

Per maggiori dettagli si rinvia ai presidi indicati al paragrafo precedente e nella sezione della Parte Speciale I relativa ai Reati contro la P.A.

3. Gestione delle operazioni societarie, delle attività assembleari e dei rapporti tra soci e tra organi sociali

1. Tutte le operazioni straordinarie nonché i conferimenti, la distribuzione di utili o riserve, la sottoscrizione od acquisto di azioni, le operazioni sul capitale sociale, fusioni e scissioni, il riparto dei beni in sede di liquidazione, avvengono nel rispetto della normativa e delle *best practice* previste in materia di *corporate governance*.
2. Ai fini della corretta realizzazione di tali operazioni straordinarie sul capitale e della corretta conduzione delle attività assembleari la Società assicura:
 - (i) l'identificazione, in via preliminare, di tutti gli adempimenti e le scadenze previste dalle disposizioni di legge applicabili nonché dei relativi responsabili;

- (ii) il monitoraggio continuo di tutte le attività di volta in volta poste in essere da parte del personale coinvolto nell'esecuzione della specifica operazione.

3. La Società garantisce:

- (i) l'identificazione della persona (o delle persone) preposta/e alla trasmissione della documentazione rilevante ai fini di ogni riunione del Consiglio di Amministrazione e dell'assemblea dei soci;
- (ii) la tempestiva trasmissione ai soci di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea dei soci e di ogni altro documento che i soci richiedano ai sensi dell'art. 2476 comma 2 c.c.;
- (iii) in generale, la massima collaborazione tra organo amministrativo e organo di controllo.

4. A tal fine:

- (i) le Strutture e gli Organi della SIM, a qualsiasi titolo coinvolti nella gestione dei rapporti con il Collegio Sindacale e la Società di Revisione, sono tenute alla massima diligenza, professionalità, trasparenza, collaborazione, disponibilità e al pieno rispetto del ruolo istituzionale degli stessi, dando puntuale e sollecita esecuzione alle prescrizioni ed agli eventuali adempimenti richiesti nel presente protocollo, in conformità alle disposizioni di legge esistenti in materia nonché alle eventuali previsioni del Codice Etico;
- (ii) devono essere puntualmente trasmesse le comunicazioni periodiche al Collegio Sindacale e alla Società di Revisione, e tempestivamente riscontrate le richieste/istanze pervenute dagli stessi;
- (iii) i membri del Consiglio di Amministrazione e i dipendenti che, a qualunque titolo, siano coinvolti in una richiesta di produzione di documenti o di informazioni da parte del Collegio Sindacale nonché della Società di Revisione pongono in essere comportamenti improntati alla massima correttezza e trasparenza e non ostacolano in alcun modo le attività di controllo e/o di revisione;
- (iv) i dati ed i documenti devono essere resi disponibili in modo puntuale ed in un linguaggio chiaro, oggettivo ed esaustivo in modo da fornire informazioni accurate, complete, fedeli e veritiere;
- (v) ciascuna Struttura aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione formalmente prodotta e/o consegnata ai membri del Collegio Sindacale e ai Revisori, nell'ambito della propria attività, ivi inclusa quella trasmessa in via elettronica.

4. Gestione delle operazioni societarie, delle attività assembleari e dei rapporti tra soci e tra organi sociali

- Tutte le operazioni straordinarie nonché i conferimenti, la distribuzione di utili o riserve, la sottoscrizione od acquisto di azioni, le operazioni sul capitale sociale, fusioni e scissioni, il riparto dei beni in sede di liquidazione, avvengono nel rispetto della normativa e delle best practice previste in materia di corporate governance.
- Le attività di valutazione tecnico-economica delle operazioni straordinarie effettuate sono tracciabili; In particolare, è garantito quanto segue:
 - (i) le attività di predisposizione e verifica della documentazione a supporto degli Organi Sociali per la delibera delle operazioni straordinarie sono adeguatamente segregate;
 - (ii) l'attività di gestione dei conferimenti, degli utili e delle riserve e le operazioni sulle partecipazioni e sul capitale sono effettuate nel rispetto della normativa civilistica di riferimento;
 - (iii) è prevista la conservazione e l'archiviazione dei verbali delle assemblee e della documentazione inerenti le operazioni societarie;
 - (iv) il personale designato dalla SIM in qualità di componente del Consiglio di Amministrazione è tenuto a comunicare – nelle forme e nei termini previsti dall'art. 2391 c.c. – l'interesse che, per conto della SIM ovvero per conto proprio o di terzi, abbia in una determinata operazione della società, astenendosi dall'effettuare l'operazione se si tratta di amministratore delegato.
- In caso di operazioni transfrontaliere, la Società cura che vengano debitamente rispettate le previsioni di cui all'art. 29 del D.Lgs. 19/2023 in relazione al certificato inerente ai requisiti di legalità per la realizzazione dell'operazione.

5. Gestione delle operazioni con Parti Correlate

1. Le operazioni con Parti Correlate sono regolarmente poste in essere a condizioni di mercato e comunque sulla base di valutazione di convenienza economica e sempre nel rispetto della normativa vigente, dando adeguata motivazione delle ragioni e della convenienza per la conclusione delle stesse.
2. L'operatività con Soggetti Collegati prevede uno specifico *iter* procedurale (istruttorio, deliberativo e di monitoraggio) volto a garantire l'imparzialità e la correttezza sostanziale e procedurale di tali operazioni; la relativa documentazione è archiviata.

6. Gestione e divulgazione delle informazioni e delle comunicazioni verso l'esterno

- Al personale interno è richiesto di
 - (i) astenersi dal rilasciare, a qualsivoglia organo di informazione (quotidiani, periodici, radio e televisione) nonché a qualsiasi soggetto comunque collegato ad organi di informazione, in qualunque sede, luogo od occasione, commenti o dichiarazioni di qualunque genere o tipo in qualunque modo connessi con l'attività lavorativa o con



Compagnia Privata o con la Clientela; e ciò indipendentemente dallo scopo, dai toni, e da qualsivoglia altra considerazione circa opportunità o eventuali valenze positive o negative delle dichiarazioni o dei commenti;

- (ii) rilasciare solo ed esclusivamente quelle interviste e dichiarazioni espressamente autorizzate dalla Società con le modalità, i toni, le espressioni e le forme parimenti autorizzati;
- (iii) non partecipare a qualsiasi tipo di programma, televisivo o radiofonico in qualità di Esponenti delle Società, se non appositamente e preventivamente autorizzati dai componenti dell'alta direzione all'uopo delegati.

CAPITOLO II.4.2 - PRINCIPI SPECIFICI DI COMPORTAMENTO IN RELAZIONE ALLE FATTISPECIE DI CORRUZIONE TRA PRIVATI

Ai fini dell'attuazione delle regole elencate al precedente Capitolo, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali qui di seguito descritti per le singole Attività Sensibili e Strumentali. Tali principi potranno trovare attuazione anche per mezzo dell'adozione di specifiche procedure aziendali.

1. Gestione dei rapporti con gli istituti bancari, assicurativi e finanziari

- La Società prevede un sistema autorizzativo e organizzativo che:
 - (i) definisce i ruoli e le responsabilità dei soggetti coinvolti nei rapporti con gli istituti di credito e finanziari nonché con le compagnie assicurative;
 - (ii) assicura la tracciabilità dei contatti e delle interlocuzioni di maggiore rilevanza con tali controparti.

2. Gestione delle controversie e conclusione di accordi transattivi

1. La Società definisce i ruoli e le responsabilità dei soggetti incaricati di gestire i contenziosi e le posizioni precontenziose.
2. Il processo che conduce ad un accordo transattivo deve essere sempre adeguatamente tracciato e gli accordi transattivi devono essere debitamente formalizzati, sottoscritti in coerenza con il sistema autorizzativo in essere e correttamente archiviati.
3. Il coinvolgimento di Consulenti per la gestione di controversie deve avvenire solo previa verifica della professionalità e dell'onorabilità dei medesimi.
4. L'Organismo di Vigilanza deve essere periodicamente aggiornato in occasione di eventi di rilievo, quali udienze importanti alle quali partecipino Esponenti della Società.

Si rinvia inoltre a quanto espressamente di seguito previsto in materia di selezione dei Consulenti.

In relazione alle **Attività Strumentali** la Società adotta i seguenti principi procedurali.

5. Selezione di Fornitori, Consulenti e *Partner* e gestione dei relativi rapporti

- L'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente ai soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno.
- Tutto il processo di acquisto è gestito nel rispetto della segregazione dei compiti e nel rispetto di specifici livelli autorizzativi.
- I Consulenti, i Fornitori e i *Partner* devono essere scelti con metodi trasparenti (ad esempio, utilizzando apposite *vendor-list* contenenti l'indicazione delle controparti di fiducia cui si è legati da rapporti consolidati o una procedura formalizzata di *beauty contest*), sulla base di

una opportuna valutazione sia in termini economici sia qualitativi delle proposte contrattuali di più parti (salvo deroghe espressamente autorizzate e motivate dalla peculiarità della prestazione ricercata – che non permetta di ottenere più proposte contrattuali – e/o dalla caratteristica di *intuitu personae* della medesima).

- Le regole per la scelta del fornitore devono rispettare anche quanto previsto dal Codice Etico, al fine di prevenire il rischio che la sua scelta ricada su familiari o soggetti legati/vicini ad amministratori, direttori generali, dirigenti preposti alla formulazione dei documenti contabili societari, sindaci o liquidatori, nonché a soggetti sottoposti a quest'ultimi di un'altra società od ente, a fini corruttivi;
- Nell'ambito dell'attività in oggetto è necessario motivare e tracciare la scelta del fornitore / professionista (che deve possedere gli effettivi requisiti tecnici/professionali/organizzativi e la potenzialità di erogazione della prestazione richiesta) assicurando l'archiviazione della relativa documentazione.
- In relazione ai Consulenti, Fornitori e *Partner* principali e/o esposti a maggior rischio di commissione dei reati alla luce della tipologia dell'attività espletata, la Società effettua una *due diligence* rafforzata (anche avvalendosi di società specializzate) volta a scongiurare il rischio di instaurare rapporti con imprese legate alla criminalità organizzata.
- Sia in fase di primo incarico sia periodicamente, ai Consulenti, Fornitori e *Partner* viene richiesta la presentazione di documentazione (eventualmente anche un'autocertificazione) comprovante il possesso dei necessari requisiti abilitativi e autorizzativi, con l'obbligo di comunicare senza ritardo l'eventuale venir meno di uno di detti requisiti (ad esempio, condanna per qualche reato o sanzione disciplinare dell'Ordine professionale di appartenenza).
- I Consulenti, Fornitori e *Partner* devono garantire e su richiesta poter documentare anche con riferimento ai subappaltatori da loro incaricati:
 - in relazione all'utilizzo di marchi o segni distintivi e alla commercializzazione di beni o servizi – il rispetto della disciplina in tema di protezione dei titoli di proprietà industriale e del diritto d'autore e, comunque, la legittima provenienza dei beni forniti;
 - in relazione ai lavoratori impiegati, il rispetto della disciplina in tema di immigrazione e la regolarità retributiva, contributiva, previdenziale, assicurativa e fiscale.
- I contratti con Consulenti, Fornitori e *Partner* devono essere definiti per iscritto in tutti i loro termini e condizioni.
- In relazione alle attività esternalizzate, la Società verifica regolarmente il permanere delle condizioni di idoneità degli outsourcer a garantire il soddisfacimento delle condizioni imposte dalla normativa di riferimento e più in generale prese in considerazione in fase di selezione degli stessi.

- I contratti con Consulenti, Fornitori e *Partner* devono prevedere un'apposita dichiarazione con cui i medesimi affermino: (i) di essere a conoscenza della normativa di cui al D.Lgs. 231/2001, del Modello e delle sue implicazioni per la Società, (ii) di non essere mai stati implicati in procedimenti giudiziari relativi ai Reati nello stesso contemplati e (iii) di impegnarsi al rispetto delle disposizioni del Modello ai medesimi applicabili.
- I contratti con Consulenti, Fornitori e *Partner* devono prevedere le conseguenze della violazione da parte degli stessi degli obblighi assunti previsti al punto che precede (ad esempio, risoluzione del rapporto).
- La Struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta dal Consulente, Fornitore o *Partner*, anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione delle procedure acquisitive di beni e servizi.
- La Società verifica, prima dell'effettuazione di pagamenti verso Consulenti, Fornitori e *Partner*, l'effettiva corrispondenza tra quanto previsto in fattura e quanto previsto nel contratto nonché l'effettiva esecuzione della prestazione secondo quanto contrattualmente pattuito.

6. Gestione degli omaggi, spese di rappresentanza, sponsorizzazioni e beneficenze

- Tutte le erogazioni di fondi (destinate a omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni) devono essere approvate dai soggetti cui il sistema interno di poteri e deleghe riconosce tale facoltà.
- È vietata ogni forma di omaggio o liberalità a terzi eccedente le normali pratiche commerciali o di cortesia o comunque rivolta ad acquisire indebitamente trattamenti di favore nella conduzione di qualsiasi attività della Società. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore.
- Sono definiti i ruoli, le responsabilità, le modalità operative e i principi comportamentali cui attenersi nella gestione di qualsiasi distribuzione gratuita di beni e servizi a clienti, fornitori, dipendenti e soggetti terzi in generale;
- la distribuzione degli omaggi deve rientrare nell'ambito dei rapporti di cortesia. Gli omaggi devono essere offerti esclusivamente in occasione di particolari ricorrenze (ad es.: festività natalizie) e devono essere tali da non influenzare la volontà del beneficiario e tali da non poter essere interpretati da un osservatore esterno imparziale come finalizzati ad acquisire vantaggi in modo improprio;
- qualsiasi omaggio deve essere documentato e autorizzato, nonché conforme ai principi stabiliti nel presente Modello e nel Codice Etico adottato dalla SIM;
- in relazione alle spese di rappresentanza, è prevista la preventiva autorizzazione motivata da parte del Responsabile della struttura interessata alla spesa.

- La Società garantisce la registrazione di ogni regalia eventualmente resa.
- È vietato offrire o dare denaro, regali, ospitalità o altri oggetti di valore, direttamente o tramite altri, a funzionari, dipendenti o rappresentanti di qualsiasi Cliente, o di qualsiasi altra organizzazione, se ciò potrebbe ragionevolmente dare l'impressione di influenzare il rapporto tra tali soggetti e la Società.
- Non sono consentiti omaggi in denaro contante o equivalenti in contanti (come, ad esempio, buoni).
- Gli omaggi consentiti, salvo il rispetto di quanto sopra, non potranno essere in ogni caso superiori a Euro 150.
- Il processo di gestione delle spese di rappresentanza, delle donazioni e degli omaggi, nonché delle sponsorizzazioni deve essere puntualmente tracciato, al fine di garantirne la trasparenza e la verificabilità. Tutta la documentazione inerente a tali attività deve essere adeguatamente conservata e archiviata a cura delle Funzioni coinvolte. In aggiunta, i regali offerti devono essere documentati in modo adeguato.

7. Gestione dei flussi finanziari

- Tutti i flussi finanziari in entrata e in uscita devono essere adeguatamente identificabili e tracciabili, nonché correttamente e regolarmente registrati in appositi libri e registri contabili.
- Tutti i flussi finanziari in entrata e in uscita devono essere supportati da specifica documentazione giustificatrice, che riporti chiaramente e fedelmente le transazioni a cui fa riferimento.
- È previsto un sistema di monitoraggio e di *reporting* periodico dell'andamento dei flussi di cassa della Società.
- La Società garantisce il principio di segregazione dei ruoli tra i soggetti che autorizzano, coloro che eseguono e coloro che controllano i flussi finanziari in entrata e in uscita nel rispetto dei limiti di spesa coerenti con le responsabilità organizzative e con le competenze gestionali.
- La Società individua preventivamente gli Esponenti aziendali a cui sono conferiti i poteri di spesa attraverso apposite procure ovvero delibere del Consiglio di Amministrazione, al fine di garantire la chiara individuazione a posteriori del soggetto avente i poteri di spesa per ogni transazione finanziaria effettuata.
- Sono stabiliti adeguati limiti all'autonomo impiego delle risorse finanziarie, attraverso la definizione di limiti di spesa coerenti con le responsabilità organizzative e con le competenze gestionali.
- Sono sempre tracciabili le movimentazioni finanziarie effettuate dalla Società, i soggetti che le hanno predisposte e autorizzate e le motivazioni sottostanti le entrate e le uscite di denaro.

- Tutte le operazioni che comportano l'impiego di risorse economiche o finanziarie sono documentate e registrate in conformità ai principi di correttezza professionale e contabile.
- La documentazione inerente alle movimentazioni finanziarie deve essere adeguatamente conservata e archiviata.
- Il pagamento delle fatture può avvenire solo previa autorizzazione dell'unità aziendale richiedente il bene servizio che attesti l'avvenuta consegna del bene / regolare esecuzione della prestazione, nonché previo controllo amministrativo contabile delle fatture stesse rispetto ai contratti / ordini di acquisto / lettere di conferimento.
- Sono previsti sistemi di controllo e di autorizzazione degli utilizzi di risorse finanziarie che eccedono i limiti determinati in sede di definizione del *budget*.
- La Società effettua controlli dei flussi finanziari aziendali in entrata ed uscita; tali controlli devono tener conto degli istituti di credito utilizzati (sede delle banche coinvolte nelle operazioni) e di eventuali schermi societari e strutture fiduciarie utilizzate per eventuali operazioni straordinarie, nonché della sede legale della società controparte e del luogo di destinazione o provenienza del denaro in uscita o in entrata (ad esempio, paradisi fiscali, Paesi rientranti nelle *black-list* internazionali, ecc.).
- È fatto divieto di trasferimento di denaro contante o di titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) in Euro o in valuta estera, effettuato a qualsiasi titolo quando il valore dell'operazione è pari o superiore a Euro 1.000. Il trasferimento può tuttavia essere eseguito per il tramite di banche, istituti di moneta elettronica e Poste Italiane S.p.A.

8. Selezione, assunzione e gestione del personale (compresa la gestione dei rimborsi spese)

- La Società in relazione alle attività in oggetto garantisce la segregazione dei compiti in base ai livelli autorizzativi definiti dal sistema di deleghe e dalla normativa aziendale.
- Il processo di selezione e assunzione del personale deve avvenire secondo criteri di trasparenza basati sui seguenti parametri:
 - individuazione dei soggetti competenti a gestire le assunzioni;
 - strutturazione del processo di selezione e assunzione lungo più fasi, con coinvolgimento di più funzioni/soggetti;
 - applicazione di criteri oggettivi – basati sulla parità di trattamento e sulla valorizzazione del merito e della professionalità – nella scelta del candidato più idoneo all'assunzione e nell'individuazione del relativo inquadramento e trattamento;
 - verifica dell'assenza di elementi ostativi all'instaurazione del rapporto di lavoro e della professionalità adeguata rispetto all'incarico o alle mansioni da assegnare;
 - esclusione di qualsiasi interferenza da parte di soggetti terzi nel processo di assunzione del personale dipendente.

- L'attività di gestione amministrativa del personale è supportata da un sistema gestionale, il cui utilizzo consente la tracciabilità di ogni fase del processo.
- Eventuali avanzamenti interni di carriera e riconoscimenti di premi (ivi compresa l'eventuale previsione, nel trattamento retributivo, di una componente variabile legata al raggiungimento di specifici obiettivi) devono essere assegnati secondo criteri oggettivi, basati sulla parità di trattamento e sulla valorizzazione del merito e della professionalità.
- Al neoassunto viene consegnata copia del Modello e del Codice Etico e viene chiesto di firmare una dichiarazione di presa visione e impegno al rispetto di tali documenti.
- In particolare, sono presenti attività di controllo che prevedono tra l'altro
 - un monitoraggio della rilevazione presenze al fine di individuare eventuali anomalie;
 - l'applicazione di regole volte a disciplinare le modalità di selezione del personale;
 - il monitoraggio e la valutazione annuale della prestazione professionale del personale di Compagnia Privata, ovvero del contributo fornito da ogni dipendente allo svolgimento della mission aziendale e al raggiungimento degli obiettivi fissati dall'azienda;
 - l'applicazione di regole volte a disciplinare le politiche di remunerazione e di incentivazione;
 - l'applicazione di regole volte a disciplinare l'iter autorizzativo delle richieste di ferie / straordinari / permessi;
 - l'applicazione di regole volte a disciplinare: le richieste di rimborso delle spese di trasferta / missione dei dipendenti; le modalità di autorizzazione a sistema da parte del responsabile della funzione competente delle note spese, a seguito della verifica dei relativi giustificativi.
- Le spese effettuate da Esponenti aziendali per conto della Società devono essere caratterizzate da attinenza all'attività di *business*.
- Le spese sostenute da Esponenti della Società per conto di questa possono essere rimborsate solo previa presentazione di idonee pezze giustificative.

* * *

Per ogni aspetto di maggiore dettaglio riferibile – anche indirettamente – alle Attività Sensibili sopra indicate e, in generale, alla prevenzione del rischio di commissione di Reati Presupposto astrattamente rilevanti in relazione alla presente Parte Speciale, si rimanda anche espressamente al contenuto – *inter alia* – dei seguenti documenti normativi interni:

- *policy* di gestione delle risorse umane;
- *policy* di remunerazione e incentivazione;



- *policy* delle funzioni esternalizzate;
- *policy* di gestione dei conflitti di interesse;
- *Policy* delle funzioni esternalizzate e in *Cloud*.

CAPITOLO II.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

Con riferimento alla presente Parte Speciale, ogni funzione coinvolta deve comunicare per quanto di competenza e con periodicità definita quanto previsto nella seguente tabella (si precisa che i flussi in oggetto, all'occorrenza, possono eventualmente essere forniti in occasione di incontri *de visu* con l'OdV):

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
<i>Amministrazione</i>	Segnalazione di (i) criticità riscontrate nell'ambito del processo di approvazione del bilancio e (ii) eventuali operazioni effettuate sul capitale.	Ad evento
<i>Amministrazione</i>	Informativa in merito a eventuali anomalie nei rapporti con istituti di credito e compagnie assicurative e in merito a qualsivoglia controversia dovesse sorgere nell'ambito dei rapporti con gli stessi. Informativa in merito a eventuali sinistri.	Ad evento

Si rinvia, quanto alle Attività Strumentali, ai flussi informativi previsti nella **Parte Speciale I.**



PARTE SPECIALE – III – Reati e illeciti amministrativi riconducibili ad abusi di mercato

CAPITOLO III.1 - LE FATTISPECIE DI REATO

Si descrivono di seguito le singole fattispecie di reato e di illecito amministrativo per le quali l'art. 25-*sexies*, D.Lgs. 231/2001 e l'art. 187-*quinquies* D.Lgs. n. 58/98 (di seguito, "TUF") prevedono la responsabilità della Società nei casi in cui tali reati e illeciti amministrativi siano stati compiuti nell'interesse o a vantaggio della società stessa. I reati e gli illeciti amministrativi di cui alla presente Parte Speciale si riferiscono a strumenti finanziari 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. La relativa disciplina è stata innovata con il Regolamento (UE) n. 596/2014 del Parlamento Europeo e del Consiglio del 16 aprile 2014 (cosiddetto "**Regolamento MAR**"), relativo agli abusi di mercato, al quale – a seguito della novella legislativa intervenuta con il D.Lgs. 10 agosto 2018, n. 107 – vengono ora effettuati diversi rimandi da parte del TUF.

III.1.1 La definizione di "informazione privilegiata"

Attorno al concetto di informazione privilegiata ruotano l'intera disciplina relativa all'*insider trading* e quella concernente l'informazione societaria disciplinata nel Titolo III, Capo I, artt. 114 e seguenti del TUF e nel Regolamento Emittenti n. 11971/1999.

Secondo quanto previsto dall'art. 180, lett. b-*ter*, TUF, si intendono di carattere privilegiato le informazioni che presentano le seguenti caratteristiche:

- a. sono di carattere preciso e pertanto:
 - i. devono essere inerenti a un complesso di circostanze o eventi esistenti o verificatisi o a circostanze o eventi che ragionevolmente possa prevedersi che verranno ad esistenza o che si verificheranno (il riferimento è ai casi in cui la notizia è in via di formazione e riguarda eventi non ancora verificatisi, si pensi al caso caratterizzato dalla notizia che una società quotata stia per lanciare un'OPA, oppure il caso riguardante un piano strategico di riposizionamento produttivo della società emittente i titoli); e
 - ii. devono essere sufficientemente specifiche (ossia esplicite e dettagliate), in modo che chi le impiega sia posto in condizione di ritenere che dall'uso delle stesse potranno effettivamente realizzarsi quegli effetti sul prezzo degli strumenti finanziari;
- b. non sono ancora state rese pubbliche;
- c. riguardano, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, e sono relative alla situazione economica patrimoniale ("corporate information") ovvero a vicende organizzative dell'emittente ("market information");
- d. sono "*price sensitive*", ossia sono tali che, se rese pubbliche, sarebbero presumibilmente utilizzate da un investitore ragionevole come uno degli elementi su cui fondare le proprie decisioni di investimento.

Inoltre, il legislatore dell'Unione Europea – con il Regolamento MAR – ha precisato ulteriormente il concetto in esame, specificando, all'art. 7, che *“nel caso di un processo prolungato che è inteso a concretizzare, o che determina una particolare circostanza o un particolare evento, tale futura circostanza o futuro evento, nonché le tappe intermedie di detto processo che sono collegate alla concretizzazione o alla determinazione della circostanza o dell'evento futuri possono essere considerate come informazioni aventi carattere preciso”* e che, di conseguenza, *“una tappa intermedia in un processo prolungato è considerata un'informazione privilegiata”*.

Con riferimento alla definizione in oggetto si elencano qui di seguito, a mero titolo esemplificativo e non esaustivo, alcune circostanze in cui la Società potrebbe trovarsi a dover gestire Informazioni Privilegiate appartenenti ad altre società:

- distribuzione di prodotti assicurativi a prevalente contenuto finanziario;
- dati revisionali e obiettivi quantitativi concernenti l'andamento della gestione;
- comunicazioni relative a operazioni di fusione/scissione e a nuove iniziative di particolare rilievo ovvero a trattative e/o accordi in merito all'acquisizione e/o cessione di *asset* significativi;
- attività di finanza straordinaria, quali, a titolo esemplificativo, fusioni, scissioni, incorporazioni, scorpori;
- mutamento nel controllo o nei patti parasociali di controllo;
- cambiamenti nell'organo di amministrazione e controllo;
- modifica del revisore o qualsiasi informazione collegata alla sua attività;
- operazioni sul capitale o emissione di obbligazioni o warrant per acquistare/sottoscrivere azioni;
- aumento o diminuzione del capitale sociale;
- acquisto o cessione di partecipazioni o altri *asset* o attività rilevanti;
- ristrutturazione o riorganizzazione che abbiano un effetto sul bilancio;
- decisioni relative ai programmi di acquisto di azioni proprie o operazioni aventi ad oggetto altri strumenti finanziari quotati;
- modifiche dei diritti relativi a determinate categorie di azioni quotate;
- istanze di fallimento ovvero ordinanze del tribunale relative a procedure concorsuali;
- significative controversie legali;
- revoca o cancellazione di linee di credito;
- liquidazione volontaria o altre cause di liquidazione;
- rilevante cambiamento nel valore degli *asset*;
- insolvenza dei principali debitori;

- riduzione del valore delle proprietà immobiliari;
- introduzione di processi o prodotti innovativi;
- decremento o incremento nel valore degli strumenti finanziari in portafoglio;
- aggiudicazione di gare per l'acquisto di asset rilevanti;
- ordini rilevanti ricevuti da clienti, loro cancellazione o rilevanti modifiche;
- ritiro o ingresso in rilevanti settori di business;
- rilevanti modifiche nella politica degli investimenti;
- informazioni relative al pagamento dei dividendi;
- analisi relative a strumenti finanziari o emittenti in particolare se contenenti raccomandazioni di investimento;
- rapporti delle agenzie di *rating*, ricerche da parte di banche d'affari, raccomandazioni o suggerimenti concernenti gli strumenti finanziari;
- decisioni riguardanti le modifiche delle regole di *governance* degli indici di mercato, con particolare riguardo alla loro composizione;
- decisioni delle autorità della concorrenza e del mercato relative alle società quotate non ancora pubblicate.

III.1.2 I reati di abuso di mercato

ABUSO O COMUNICAZIONE ILLECITA DI INFORMAZIONI PRIVILEGIATE. RACCOMANDAZIONE O INDUZIONE DI ALTRI ALLA COMMISSIONE DI ABUSO DI INFORMAZIONI PRIVILEGIATE (ART. 184 TUF)

La fattispecie punisce chiunque, essendo in possesso di informazioni privilegiate per essere membro di organi amministrativi, di direzione o di controllo di una società emittente, oppure per essere socio, ovvero per averle apprese nell'esercizio di un'attività lavorativa, di una professione o di una funzione privata o pubblica, o di un ufficio:

- a. acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni privilegiate acquisite nelle modalità sopra descritte (c.d. "*insider trading*");
- b. comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio cui si è preposti (a prescindere dalla circostanza che i terzi destinatari utilizzino effettivamente l'informazione comunicata per compiere operazioni) (c.d. "*tipping*");
- c. raccomanda o induce altri, sulla base delle informazioni privilegiate delle quali è in possesso, a compiere taluna delle operazioni indicate nella lettera a) (c.d. "*tuyautage*").

La fattispecie punisce, inoltre, i soggetti che, entrando in possesso di informazioni privilegiate a causa della preparazione o della realizzazione di attività delittuose, compiono taluna delle azioni di cui sopra

(è l'ipotesi, ad esempio, del pirata informatico che a seguito dell'accesso abusivo al sistema informatizzato di una società riesce ad entrare in possesso di informazioni riservate "*price sensitive*").

Inoltre, fuori dai casi di concorso nel reato, la fattispecie punisce anche chiunque essendo in possesso di informazioni privilegiate per motivi diversi da quelli sopra indicati (cosiddetto "*insider* secondario") e conoscendo il carattere privilegiato di tali informazioni commette taluni dei fatti sopra indicati.

MANIPOLAZIONE DEL MERCATO (ART. 185 TUF)

La fattispecie punisce chiunque diffonde notizie false (c.d. manipolazione informativa) o pone in essere operazioni simulate o altri artifici (c.d. manipolazione operativa) concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

Si ha manipolazione informativa anche allorquando la creazione di un'indicazione fuorviante derivi dall'inosservanza degli obblighi di comunicazione da parte dell'emittente o di altri soggetti obbligati

III.1.3 Gli illeciti amministrativi ex art. 187-*quinquies* del TUF

ABUSO DI INFORMAZIONI PRIVILEGIATE E COMUNICAZIONE ILLECITA DI INFORMAZIONI PRIVILEGIATE (ART. 14 REGOLAMENTO MAR)

L'art. 14 del Regolamento MAR prevede che non sia consentito:

- a) abusare o tentare di abusare di informazioni privilegiate;
- b) raccomandare ad altri di abusare di informazioni privilegiate o indurre altri ad abusare di informazioni privilegiate; oppure
- c) comunicare in modo illecito informazioni privilegiate.

I comportamenti degli *insider* secondari sono puniti sia se sono commessi a titolo di dolo sia se sono commessi con colpa.

DIVIETO DI MANIPOLAZIONE DEL MERCATO (ART. 15 REGOLAMENTO MAR)

L'art. 15 del Regolamento MAR prevede che non sia consentito effettuare manipolazioni di mercato o tentare di effettuare manipolazioni di mercato.

Sulla scorta dell'interpretazione fornita da dottrina e giurisprudenza in merito alla disciplina previgente alla novella, si precisa che l'illecito amministrativo di manipolazione del mercato è teso ad ampliare le condotte rilevanti ai fini dell'applicabilità delle sanzioni amministrative rispetto a quelle penalmente sanzionate dalla corrispondente fattispecie delittuosa e punisce chiunque, tramite qualsiasi mezzo di informazione, compreso internet, diffonde informazioni, voci o notizie false o fuorvianti che forniscano o siano suscettibili di fornire indicazioni false ovvero fuorvianti in merito agli strumenti finanziari. A differenza di quanto previsto dalla corrispondente fattispecie di reato, pertanto, non è richiesto, ai fini della sanzionabilità delle condotte, che le notizie false, le operazioni simulate o gli altri artifici siano "concretamente idonee" ad alterare i prezzi.

Ricalcando la disciplina di cui al D.Lgs. 231/2001, prevede l'art. 187-*quinquies* del TUF che l'ente sia punito – con una sanzione amministrativa pecuniaria che può arrivare al quindici per cento del fatturato (quando tale importo sia superiore a quindici milioni di euro e il fatturato sia determinabile ai sensi dell'articolo 195, comma 1-*bis* TUF³) – nel caso in cui sia commessa nel suo interesse o a suo vantaggio una violazione del divieto di cui all'articolo 14 o del divieto di cui all'articolo 15 del Regolamento MAR:

- a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria o funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;
- b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

Se, in seguito alla commissione degli illeciti, il prodotto o il profitto conseguito dall'ente è di rilevante entità, la sanzione è aumentata fino a dieci volte tale prodotto o profitto.

Si sottolinea che anche il semplice tentativo può rilevare ai fini dell'applicabilità della disciplina in oggetto, essendo questo – nei casi di specie – equiparato alla consumazione

³ Il quale prevede che, "ai fini dell'applicazione delle sanzioni amministrative pecuniarie previste dal presente titolo, per fatturato si intende il fatturato totale annuo della società o dell'ente, risultante dall'ultimo bilancio disponibile approvato dall'organo competente, così come definito dalle disposizioni attuative di cui all'articolo 196-bis".

CAPITOLO III.2 – LE ATTIVITÀ SENSIBILI IN RELAZIONE AI REATI DI ABUSO DI MERCATO

Le Attività Sensibili che la Società ha individuato al proprio interno in relazione ai Reati in oggetto sono le seguenti:

- 1. Gestione delle informazioni privilegiate**
- 2. Gestione dell'operatività sui mercati**

CAPITOLO III.3 – PRINCIPI GENERALI DI COMPORTAMENTO

Obiettivo della presente Parte Speciale, al fine di prevenire la commissione dei Reati nella stessa considerati, è che tutti i Destinatari del Modello si attengano al rispetto di tutte le procedure e ai principi che siano direttamente o indirettamente funzionali alla prevenzione di condotte idonee a integrare i reati tributari sopra richiamati.

I Destinatari dovranno attenersi ai seguenti principi di condotta:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le Attività Sensibili individuate nella presente Parte Speciale;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato o di illecito amministrativo rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- adoperarsi affinché le comunicazioni all'esterno siano veritiere e corrette;
- astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false o non corrette, idonee a provocare una sensibile alterazione del prezzo di strumenti finanziari quotati o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato.

CAPITOLO III.4 – PRINCIPI SPECIFICI DI COMPORTAMENTO

Ai fini dell'attuazione delle regole elencate al precedente Capitolo, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali qui di seguito descritti per le singole Attività Sensibili. Tali principi potranno trovare attuazione anche per mezzo dell'adozione di specifiche procedure di Gruppo.

1. Gestione delle informazioni privilegiate

1. La Società assicura il rispetto del divieto di:

- a) utilizzare o comunicare informazioni privilegiate relative a strumenti finanziari o emittenti strumenti finanziari, quotati, comunque ottenute (*i.e.* in qualsiasi modo e per qualsiasi via), anche al di fuori della propria attività lavorativa;
- b) partecipare a gruppi di discussione o *chat-room* su internet aventi ad oggetto strumenti finanziari o emittenti strumenti finanziari, quotati e nei quali vi sia uno scambio di informazioni concernenti strumenti finanziari quotati, o società quotate in genere o strumenti finanziari emessi da tali soggetti, a meno che si tratti di incontri istituzionali per i quali è già stata compiuta una verifica di legittimità da parte delle funzioni competenti e/o non vi sia scambio di informazioni il cui carattere non privilegiato sia evidente;
- c) sollecitare l'ottenimento di informazioni privilegiate su strumenti finanziari o emittenti strumenti finanziari quotati;
- d) comunicare qualsiasi informazione all'interno della Società, degli eventuali comitati, degli organi sociali di tipo collegiale senza il puntuale e metodico rispetto della normativa vigente in materia di informazioni privilegiate;
- e) lasciare documentazione contenente informazioni privilegiate in luoghi in cui potrebbe facilmente essere letta da persone che non sono autorizzate a conoscere tali informazioni secondo quanto previsto dalla normativa vigente;
- f) effettuare comunicazioni all'esterno nel mancato rispetto delle procedure e/o prassi aziendali in materia e senza il preventivo coordinamento con le funzioni preposte a tale compito;
- g) rivelare a terzi informazioni privilegiate (in qualunque modo siano state ottenute) relative a strumenti finanziari o emittenti strumenti finanziari, quotati o non quotati, se non nei casi in cui tale rivelazione sia richiesta da leggi, da altre disposizioni regolamentari o da specifici accordi contrattuali con cui le controparti si siano impegnate a utilizzare dette informazioni privilegiate esclusivamente per i fini per i quali dette informazioni sono trasmesse e a mantenere la riservatezza sulle stesse;

- h) comunicare o diffondere all'esterno analisi o valutazioni su uno strumento finanziario quotato (o indirettamente sul suo emittente) che possano influenzare i terzi, dopo aver preso precedentemente posizione su tale strumento finanziario, beneficiando di conseguenza dell'impatto della valutazione diffusa sul prezzo di detto strumento, senza avere allo stesso tempo comunicato al pubblico, in modo corretto ed efficace, l'esistenza di tale conflitto di interesse;
- i) diffondere informazioni di mercato false o fuorvianti tramite mezzi di comunicazione, compreso internet, o tramite qualsiasi altro mezzo;
- j) diffondere al pubblico valutazioni o una notizia su uno strumento finanziario o un emittente senza prima aver verificato l'attendibilità e il carattere non privilegiato dell'informazione;
- k) consigliare ai terzi operazioni di investimento sulla base delle informazioni privilegiate in loro possesso;
- l) discutere di informazioni privilegiate in presenza di estranei o, comunque, soggetti non autorizzati a conoscere tali informazioni sulla base della normativa vigente;
- m) discutere di informazioni privilegiate al telefono in luoghi pubblici ovvero in ufficio con la modalità "viva voce", onde evitare che informazioni privilegiate possano essere ascoltate da estranei o comunque da soggetti non autorizzati a conoscere tali informazioni secondo quanto previsto dalla normativa vigente.

2. Gestione dell'operatività sui mercati

1. La Società assicura il rispetto del divieto di:

- a) impartire ordini per l'acquisto di uno strumento finanziario ed effettuare ulteriori acquisti e/o diffondere informazioni fuorvianti sullo strumento finanziario in modo da aumentarne il prezzo;
- b) impartire ordini in modo tale da evitare che i prezzi di mercato degli strumenti finanziari di interesse per la Società scendano al di sotto di un certo livello, principalmente per sottrarsi alle conseguenze negative derivanti dal connesso peggioramento del *rating* degli strumenti finanziari stessi;
- c) agire consultandosi con altri soggetti per acquisire una posizione dominante sull'offerta o sulla domanda di uno strumento finanziario che abbia l'effetto di fissare, direttamente o indirettamente, i prezzi di acquisto o di vendita o determinare altre condizioni commerciali non corrette;
- d) effettuare operazioni di compravendita di uno strumento finanziario nella consapevolezza di un conflitto di interessi (a meno che esso non venga esplicitato nelle

forme previste dalla normativa), allorquando tale operazione non sarebbe stata ragionevolmente effettuata in caso di assenza di conflitto di interessi;

- e) operare creando inusuali concentrazioni di operazioni in accordo con altri soggetti su un particolare strumento finanziario;
- f) effettuare operazioni che hanno la finalità di aggirare gli accorgimenti previsti dai meccanismi di negoziazione (ad esempio, con riferimento ai limiti quantitativi, ai parametri relativi al differenziale tra le proposte di acquisto e di vendita, ecc.);
- g) impartire ordini di compravendita o effettuare operazioni prima o dopo che la stessa società o soggetti ad essa collegati abbiano diffuso studi, ricerche o raccomandazioni di investimento errate o tendenziose o manifestamente influenzate da interessi rilevanti;
- h) acquistare partecipazioni di un emittente appartenente al c.d. “mercato sottile” realizzando poi operazioni volte a farne aumentare i prezzi così da consentire di ottenere performance superiori al *benchmark* di riferimento;
- i) aprire o impartire l'ordine di aprire una posizione lunga su uno strumento finanziario ed effettuare ulteriori acquisti e/o diffondere fuorvianti informazioni positive sullo strumento finanziario in modo da aumentarne il prezzo;
- j) prendere una posizione ribassata su uno strumento finanziario ed effettuare un'ulteriore attività di vendita e/o diffondere fuorvianti informazioni negative sullo strumento finanziario in modo da ridurne il prezzo;
- k) aprire o impartire l'ordine di aprire una posizione su un determinato strumento finanziario e chiuderla immediatamente dopo che la posizione stessa è stata resa nota al pubblico;
- l) realizzare un'inusuale operatività sugli strumenti finanziari di una società emittente prima dell'annuncio di informazioni privilegiate relative alla società, a meno che tale operatività non sia basata solo su analisi di mercato, su informazioni non privilegiate ovvero su altre notizie pubblicamente disponibili;
- m) realizzare operazioni che hanno la finalità di aumentare il prezzo di uno strumento finanziario nei giorni precedenti all'emissione di uno strumento finanziario derivato collegato o di uno strumento finanziario convertibile.

* * *

Per ogni aspetto di maggiore dettaglio riferibile – anche indirettamente – alle Attività Sensibili sopra indicate e, in generale, alla prevenzione del rischio di commissione di Reati Presupposto astrattamente rilevanti in relazione alla presente Parte Speciale, si rimanda anche espressamente al contenuto dei seguenti documenti normativi interni:



- *policy* delle funzioni esternalizzate;
- *policy* di gestione dei conflitti di interesse;
- *Policy* delle funzioni esternalizzate e in *Cloud*;
- *policy* di trasmissione degli ordini;
- *policy* in tema di prodotti finanziari complessi;
- procedure attività di gestione;
- procedura del servizio di consulenza.

**CAPITOLO III.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA**

Con riferimento alla presente Parte Speciale, ogni funzione coinvolta deve comunicare per quanto di competenza e con periodicità definita quanto previsto nella seguente tabella (si precisa che i flussi in oggetto, all'occorrenza, possono eventualmente essere forniti in occasione di incontri *de visu* con l'OdV):

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
<i>Compliance</i>	Criticità emerse nella gestione delle informazioni privilegiate.	Ad evento
<i>Compliance</i>	Informativa su eventuali operazioni sospette rilevate.	Semestrale (se presenti)



PARTE SPECIALE – IV – Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio, reati aventi finalità di terrorismo e trasferimento fraudolento di valori

CAPITOLO IV.1 - LE FATTISPECIE DI REATO

IV.1.1 Le fattispecie dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

RICETTAZIONE (ART. 648 C.P.)

Tale ipotesi di reato si configura nel caso in cui un soggetto, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta danaro o cose provenienti da un qualsiasi delitto o contravvenzione, o comunque si intromette nel farli acquistare, ricevere od occultare.

Per “acquisto” si intende l’effetto di un’attività negoziale, a titolo gratuito ed oneroso, mediante la quale l’agente conseguiva il possesso del bene.

Per “ricezione” si intende ogni forma di conseguimento del possesso del bene proveniente dal delitto, anche se solo temporaneamente.

Per “occultamento” si intende il nascondimento del bene proveniente da delitto dopo averlo ricevuto.

Perché sussista il reato non è necessario che il denaro o i beni debbano provenire direttamente o immediatamente da un qualsiasi reato, ma è sufficiente anche una provenienza mediata, a condizione che l’agente sia consapevole di tale provenienza. Ricorre pertanto il delitto in esame non solo in relazione al prodotto o al profitto del reato, ma anche al denaro o alle cose che costituiscono il prezzo del reato, cioè alle cose acquistate col denaro di provenienza delittuosa oppure al denaro conseguito dall’alienazione di cose della medesima provenienza (si pensi al caso in cui la Società, al fine di ottenere un prezzo vantaggioso, acquisti beni da un soggetto che, parallelamente alla fornitura di tali beni, notoriamente svolga attività illecite quali lo spaccio di stupefacenti o faccia parte di un’associazione di tipo mafioso e utilizzi i profitti derivanti da tali attività illecite per investirli nell’attività lecita).

RICICLAGGIO (ART. 648-BIS C.P.)

Tale ipotesi di reato si configura nel caso in cui un soggetto sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto o contravvenzione, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l’identificazione della loro provenienza da reato.

Per “sostituzione” si intende la condotta consistente nel rimpiazzare il denaro, i beni o le altre utilità di provenienza illecita con valori diversi.

Per “trasferimento” si intende la condotta consistente nel ripulire il denaro, i beni o le altre utilità mediante il compimento di atti negoziali.

Per la realizzazione di tale reato, dunque, è richiesto un *quid pluris* rispetto al reato di ricettazione, ovvero il compimento di atti o fatti diretti alla sostituzione del denaro.

La pena è della reclusione da due a sei anni e della multa da euro 2.500 a euro 12.500 quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l’arresto superiore nel massimo a un anno o nel minimo a sei mesi.

La pena è aumentata quando il fatto è commesso nell'esercizio dell'attività professionale; è invece diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. In tal caso si applica l'ultimo comma dell'articolo 648 c.p.

IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA (ART. 648-TER C.P.)

Tale ipotesi di reato si configura nel caso di impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto o contravvenzione.

La punibilità per tale reato è prevista solo per coloro i quali non siano già compartecipi del reato principale ovvero non siano imputabili a titolo di ricettazione o riciclaggio.

Il termine "impiegare" è normalmente sinonimo di "utilizzo per qualsiasi scopo": tuttavia, considerato che il fine ultimo perseguito dal legislatore consiste nell'impedire il turbamento del sistema economico e dell'equilibrio concorrenziale attraverso l'utilizzo di capitali illeciti reperibili a costi inferiori rispetto a quelli leciti, si ritiene che per "impiegare" debba intendersi in realtà "investire". Pertanto, dovrebbe ritenersi rilevante un utilizzo a fini di profitto.

Premesso che presupposto comune di tutte e tre le fattispecie incriminatrici di cui agli artt. 648, 648 *bis* e 648 *ter* c.p. è quello costituito dalla provenienza da reato del denaro o di qualsiasi altra utilità di cui l'agente sia venuto a disporre, si precisa che tali fattispecie si distinguono sotto il profilo soggettivo, per il fatto che la prima di esse richiede, oltre alla consapevolezza della su indicata provenienza, necessaria anche per le altre, solo una generica finalità di profitto, mentre la seconda o 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 o finanziarie.

La pena è aumentata quando il fatto è commesso nell'esercizio dell'attività professionale.

AUTORICICLAGGIO (ART. 648-TER.1 C.P.)

L'art. 648-*ter*.1 c.p. prevede la sanzione della reclusione da due a otto anni e la multa da Euro 5.000,00 a Euro 25.000,00 per chi *"avendo commesso o concorso a commettere un delitto, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa"* e una specifica pena *"quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi"*.

Il secondo comma prevede la pena della reclusione da uno a quattro anni e della multa da euro 2.500 a euro 12.500 quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi.

Il terzo comma dell'art. 648-ter.1 c.p. prevede, inoltre, un'altra circostanza attenuante se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni.

Tale fattispecie, pertanto, prevede e punisce una condotta tale per cui l'autore, dopo aver commesso o concorso a commettere un reato, cerca di *"ostacolare concretamente l'identificazione della provenienza delittuosa"* del provento ricavato dal primo reato attraverso il suo riutilizzo *"in attività economiche, finanziarie, imprenditoriali o speculative"*.

Costituiscono circostanze aggravanti:

- l'aver commesso tale reato con le condizioni o le finalità di cui all'art. 416-bis.1 c.p., concernente "Circostanze aggravanti e attenuanti per reati connessi ad attività mafiose" ovvero al fine di agevolare l'attività delle associazioni di tipo mafioso: in tal caso troveranno, in ogni caso, applicazione le pene previste dal primo comma dell'art. 648-ter.1 c.p.;
- l'aver commesso tale reato nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale.

Costituisce invece una circostanza attenuante – che comporta la diminuzione della pena fino alla metà – il fatto che il reo *"si sia efficacemente adoperato per evitare che le condotte siano 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"* (art. 648-ter.1, comma 6, c.p.).

Non è invece punibile, ai sensi del comma 4 dell'art. 648-ter.1 c.p., l'autore del Reato di Autoriciclaggio allorquando il denaro, i beni o le altre utilità vengano destinati *"alla mera utilizzazione o al godimento personale"*.

NORMATIVA DI PREVENZIONE DEI REATI DI RICICLAGGIO

La normativa italiana in tema di prevenzione dei Reati di Riciclaggio prevede norme tese ad ostacolare le pratiche di riciclaggio, vietando tra l'altro l'effettuazione di operazioni di trasferimento di importi rilevanti con strumenti anonimi ed assicurando la ricostruzione delle operazioni attraverso l'identificazione e l'adequata verifica della Clientela e la registrazione dei dati in appositi archivi.

La cornice legislativa antiriciclaggio è oggi rappresentata dal Decreto legislativo 21 novembre 2007, n. 231 (**"Decreto Antiriciclaggio"**) e dalle relative disposizioni di attuazione emanate dal Ministro dell'economia e delle finanze, dall'Unità di Informazione Finanziaria per l'Italia e da Banca d'Italia.

I principali obblighi, che scaturiscono dal Decreto Antiriciclaggio, sono i seguenti:

- obblighi di adeguata verifica del Cliente e del titolare effettivo;
- obbligo di astenersi dall'apertura del rapporto continuativo o dall'esecuzione dell'operazione qualora l'intermediario non sia in grado di rispettare gli obblighi di adeguata verifica;
- obblighi di conservazione;

- obblighi di segnalazione di tutte quelle operazioni ritenute “sospette”;
- obblighi in capo agli organi di controllo.

Inoltre, i Titoli III e IV prevedono obblighi in capo agli organi di controllo, nonché ulteriori obblighi di carattere residuale.

1. Gli obblighi di **adeguata verifica della Clientela** consistono nelle seguenti attività:

- identificare il Cliente e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente;
- identificare il titolare effettivo e verificarne l'identità attraverso l'adozione di misure proporzionate al rischio;
- ottenere informazioni sullo scopo e sulla natura prevista del rapporto continuativo o della prestazione professionale;
- svolgere un controllo costante nel corso del rapporto continuativo o della prestazione professionale, verificare ed aggiornare i dati e le informazioni acquisite.

In tale ambito rientra anche l'obbligo della Clientela di fornire, sotto la propria responsabilità, tutte le informazioni necessarie ed aggiornate per consentire agli intermediari di adempiere agli obblighi di adeguata verifica.

Compagni Privata è tenuta ad assolvere l'obbligo di adeguata verifica della Clientela nei seguenti casi:

- quando si instaura un rapporto continuativo;
- quando si eseguono operazioni occasionali, disposte dai clienti, che comportino la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 Euro, indipendentemente dal fatto che siano effettuate con una operazione unica o con più operazioni che appaiono tra di loro collegate per realizzare un'operazione frazionata;
- quando vi è sospetto di riciclaggio o di finanziamento del terrorismo, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile;
- quando vi sono dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti ai fini dell'identificazione di un Cliente.

È inoltre previsto che, per quanto riguarda le operazioni o i rapporti continuativi con persone politicamente esposte, residenti in Italia o in un altro Stato comunitario o in un Paese terzo (“PEP”), inclusi i Politici Locali Italiani (PIL), i Destinatari debbano:

- stabilire adeguate procedure basate sul rischio per determinare se il Cliente sia una persona politicamente esposta;
- adottare ogni misura adeguata a stabilire l'origine del patrimonio e dei fondi impiegati nel rapporto continuativo o nell'operazione;

- assicurare un controllo continuo e rafforzato del rapporto continuativo. Infine, al ricorrere di determinati presupposti, trovano applicazione obblighi rafforzati.

Tra i casi in cui si dovrà porre in essere procedure d'identificazione e di verifica dell'identità dei clienti particolarmente rigorose figurano, tra l'altro, (i) l'ipotesi in cui il Cliente non sia fisicamente (ii) la sussistenza di un sospetto di riciclaggio o finanziamento del terrorismo o (iii) l'insorgenza di dubbi sulla veridicità o adeguatezza dei dati ottenuti.

2. obblighi di astensione - i soggetti obbligati che si trovano nell'impossibilità oggettiva di effettuare l'adeguata verifica della Clientela devono astenersi dall'instaurare, eseguire o proseguire il rapporto, la prestazione professionale e le operazioni e valutano se effettuare una segnalazione di operazione sospetta alla UIF. L'obbligo di astensione vale anche in relazione alle prestazioni di cui siano, direttamente o indirettamente, parte società fiduciarie, trust, società anonime o controllate aventi sede in Paesi terzi ad alto rischio.

3. Gli obblighi di registrazione hanno ad oggetto alcuni dei dati e delle informazioni acquisiti nel corso delle attività di adeguata verifica.

I soggetti obbligati registrano e conservano per un periodo di cinque anni, le seguenti informazioni:

- a) con riferimento ai rapporti continuativi ed alla prestazione professionale: la data di instaurazione, i dati identificativi del Cliente e del titolare effettivo, unitamente alle generalità dei delegati a operare per conto del titolare del rapporto e il codice del rapporto ove previsto;
- b) con riferimento a tutte le operazioni di importo pari o superiore a 15.000 Euro, indipendentemente dal fatto che si tratti di un'operazione unica o di più operazioni che appaiono tra di loro collegate per realizzare un'operazione frazionata: la data, la causale, l'importo, la tipologia dell'operazione, i mezzi di pagamento e i dati identificativi del soggetto che effettua l'operazione e del soggetto per conto del quale eventualmente opera.

4. Gli obblighi di conservazione riguardano le copie o i riferimenti dei documenti richiesti nel corso delle attività di adeguata verifica e permangono per un periodo di cinque anni dalla fine del rapporto continuativo o della prestazione professionale.

Per quanto riguarda le operazioni, i rapporti continuativi e le prestazioni professionali, i soggetti obbligati conservano, sempre per un periodo di cinque anni, le scritture e le registrazioni, consistenti nei documenti originali o nelle copie aventi analoga efficacia probatoria nei procedimenti giudiziari dall'esecuzione dell'operazione o dalla cessazione del rapporto continuativo.

5. Per ciò che attiene gli **obblighi di segnalazione di operazione sospetta**, è previsto che i destinatari della normativa siano tenuti ad inviare alla UIF, senza ritardo, un'apposita segnalazione quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo.

6. Obblighi in capo agli organi di controllo. Il Decreto Antiriciclaggio prevede in capo al Collegio Sindacale e, più in generale, a tutti i soggetti incaricati del controllo di gestione comunque

denominati presso i soggetti interessati, un obbligo di vigilare, ciascuno nell'ambito delle proprie attribuzioni e competenze, sull'osservanza delle norme contenute nel decreto stesso. In particolare, tali organi:

- a) comunicano, senza ritardo, alle Autorità di Vigilanza tutti gli atti o i fatti di cui vengono a conoscenza nell'esercizio dei propri compiti, che possano costituire una violazione delle disposizioni emanate ai sensi dell'art. 7, comma 2 (riguardanti le modalità di adempimento degli obblighi di adeguata verifica della Clientela, l'organizzazione, la registrazione, le procedure e i controlli interni volti a prevenire l'utilizzo degli intermediari finanziari sia per fini di riciclaggio che di finanziamento del terrorismo);
- b) comunicano, senza ritardo, al titolare dell'attività o al Legale Rappresentante o ad un suo delegato, le infrazioni alle disposizioni riguardanti l'obbligo di segnalazione delle operazioni sospette;
- c) comunicano, entro trenta giorni, al Ministero delle Finanze/alle Direzioni Provinciali dei Servizi vari competenti, le infrazioni al divieto di trasferimento di contante o titoli al portatore oltre i 2.000 Euro di cui vengano a conoscenza;
- d) comunicano, entro trenta giorni, all'Autorità di Vigilanza di settore le infrazioni alle disposizioni riguardanti gli obblighi di registrazione e di conservazione di cui hanno notizia.

Vi sono infine ulteriori **obblighi di natura residuale** gravanti in capo ai destinatari in forza delle disposizioni del Decreto Antiriciclaggio, tra cui: l'Obbligo di **formazione** dei dipendenti e collaboratori al fine della corretta applicazione delle disposizioni antiriciclaggio. Tali misure comprendono programmi di formazione finalizzati a riconoscere attività potenzialmente connesse al riciclaggio o al finanziamento del terrorismo.

IV.1.2 I delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori

FRODE INFORMATICA (ART. 640-TER C.P.)

Si configura il reato di frode informatica quando, procurando a sé o ad altri un ingiusto profitto con altrui danno, venga alterato in qualsiasi modo il funzionamento di un sistema informatico, o si intervenga, senza diritto, su dati, informazioni o programmi contenuti in un sistema informatico.

Il reato di frode informatica è richiamato dall'art. 25-*octies*.1 con riferimento alla sola ipotesi aggravata di cui al secondo comma dell'art. 640-*ter* c.p. (*"se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema"*).

TRASFERIMENTO FRAUDOLENTO DI VALORI (ART. 512-BIS C.P.)

Il reato punisce, salvo che il fatto costituisca più grave reato, chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648-*bis* e 648-*ter* c.p.

Il reato prevede altresì la punizione di chi, al fine di eludere le disposizioni in materia di documentazione antimafia, attribuisca fittiziamente ad altri la titolarità di imprese, quote societarie o azioni ovvero cariche sociali, qualora l'imprenditore o la società partecipi a procedure di aggiudicazione o di esecuzione di appalti o concessioni.

IV.1.3 I delitti con finalità di terrorismo

IL REATO DI FINANZIAMENTO DEL TERRORISMO

Il Reato di finanziamento del terrorismo è stato introdotto con il D.lgs. 109/2007, di recepimento della direttiva 2005/60/CE emanata dal Parlamento europeo e dal Consiglio in data 26 ottobre 2005.

Per finanziamento del terrorismo si intende: *“qualsiasi attività diretta, con qualsiasi mezzo, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi o di risorse economiche, in qualunque modo realizzati, destinati ad essere, in tutto o in parte, utilizzati al fine di compiere uno o più delitti con finalità di terrorismo o in ogni caso diretti a favorire il compimento di uno o più delitti con finalità di terrorismo previsti dal codice penale, e ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione dei delitti anzidetti”*.

La nuova normativa in tema di finanziamento del terrorismo adotta le medesime misure di prevenzione già vigenti contro i Reati di Riciclaggio ed introdotte con il Decreto Antiriciclaggio, prevedendo inoltre altre norme idonee per attuare il congelamento dei fondi e delle risorse economiche disposto dalle numerose risoluzioni del Consiglio di sicurezza delle Nazioni Unite che si sono succedute dal 1999 ad oggi, dal Regolamento CE n. 2580/2001 emanato dal Consiglio in data 27 dicembre 2001 e relativo a misure restrittive specifiche destinate a combattere il terrorismo, nonché dai Regolamenti comunitari emanati ai sensi degli artt. 60 e 301 del Trattato istitutivo della Comunità europea per il contrasto dell'attività dei Paesi che minacciano la pace e la sicurezza internazionale.

Il congelamento dei fondi e delle risorse economiche è disposto, con decreto, su proposta del Comitato di sicurezza finanziaria, dal Ministro dell'economia e delle finanze, di concerto con il Ministro degli affari esteri.

Ai sensi del D.lgs. 109/2007, per “congelamento di fondi” si intende il divieto di movimentazione, trasferimento, modifica, utilizzo o gestione dei fondi o di accesso ad essi, così da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consente l'uso dei fondi, compresa la gestione del portafoglio. Per “congelamento di risorse economiche” si intende, invece, il divieto di trasferimento, disposizione o, al fine di ottenere in qualsiasi modo fondi, beni o servizi, utilizzo delle risorse economiche, compresi, a titolo meramente esemplificativo, la vendita, la locazione, l'affitto o la costituzione di diritti reali di garanzia.

Si provvede qui di seguito a fornire una breve descrizione dei reati contemplati nella presente Parte Speciale, così come indicati all'art. 25-*quater* del Decreto 231 e ritenuti – ancorché astrattamente – applicabili alla Società.

ASSOCIAZIONI SOVERSIVE (ART. 270 C.P.)

Tale ipotesi di reato si configura nei confronti di chiunque nel territorio dello Stato promuova, costituisca, organizzi o diriga associazioni dirette a stabilire violentemente la dittatura di una classe sociale sulle altre, ovvero a sopprimere violentemente una classe sociale o, comunque, a sovvertire violentemente gli ordinamenti economici o sociali costituiti nello Stato ovvero, infine, aventi come scopo la soppressione violenta di ogni ordinamento politico e giuridico della società.

È punito, inoltre, chiunque partecipa alle suddette associazioni.

ASSOCIAZIONE CON FINALITÀ DI TERRORISMO ANCHE INTERNAZIONALE O DI EVERSIONE DELL'ORDINAMENTO DEMOCRATICO (ART. 270-BIS C.P.)

Tale ipotesi di reato si configura nei confronti di chiunque promuova, costituisca, organizzi, diriga o finanzi associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico.

Ai fini della legge penale, la finalità di terrorismo ricorre anche quando gli atti di violenza siano rivolti contro uno Stato estero, un'istituzione o un organismo internazionale.

ASSISTENZA AGLI ASSOCIATI (ART. 270-TER C.P.)

La norma in esame sanziona chiunque dia rifugio o fornisca vitto, ospitalità, mezzi di trasporto, strumenti di comunicazione a taluna delle persone che partecipano alle associazioni indicate nei precedenti articoli 270 e 270-bis.

La pena è aumentata se l'assistenza è prestata continuativamente.

Non è punibile chi commette il fatto in favore di un prossimo congiunto.

FINANZIAMENTO DI CONDOTTE CON FINALITÀ DI TERRORISMO (L. N. 153/2016, ART. 270-QUINQUIES.1 C.P.)

La norma punisce chiunque, al di fuori dei casi di cui agli articoli 270-bis e 270-quater.1 c.p., raccoglie, eroga o mette a disposizione beni o denaro, in qualunque modo realizzati, destinati a essere in tutto o in parte utilizzati per il compimento delle condotte con finalità di terrorismo, indipendentemente dall'effettivo utilizzo dei fondi per la commissione delle citate condotte. La norma punisce, altresì, chiunque deposita o custodisce i beni o il denaro sopra indicati.

SOTTRAZIONE DI BENI O DENARO SOTTOPOSTI A SEQUESTRO (ART. 270-QUINQUIES.2 C.P.)

La norma punisce chiunque sottrae, distrugge, disperde, sopprime o deteriora beni o denaro, sottoposti a sequestro per prevenire il finanziamento delle condotte con finalità di terrorismo di cui all'articolo 270-sexies.

CONDOTTE CON FINALITÀ DI TERRORISMO (ART. 270-SEXIES C.P.)

Sono considerate con finalità di terrorismo le condotte che, per la loro natura o contesto, possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere

o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale, nonché le altre condotte definite terroristiche o commesse con finalità di terrorismo da convenzioni o altre norme di diritto internazionale vincolanti per l'Italia.

COSPIRAZIONE POLITICA MEDIANTE ACCORDO E COSPIRAZIONE POLITICA MEDIANTE ASSOCIAZIONE (ARTT. 304 E 305 C.P.)

Questa norma punisce la condotta di chi si accordi al fine di commettere uno dei delitti di cui al precedente punto (art. 302 c.p.).

REATI DI TERRORISMO PREVISTI DALLE LEGGI SPECIALI

Tali fattispecie di reato consistono in tutta quella parte della legislazione italiana, emanata negli anni '70 e '80, volta a combattere il terrorismo.

REATI, POSTI IN ESSERE IN VIOLAZIONE DELL'ART. 2 DELLA CONVENZIONE DI NEW YORK DELL'8 DICEMBRE 1999

Ai sensi del citato articolo, commette un reato chiunque con qualsiasi mezzo, direttamente o indirettamente, illegalmente e intenzionalmente, fornisce o raccoglie fondi con l'intento di utilizzarli o sapendo che sono destinati ad essere utilizzati, integralmente o parzialmente, al fine di compiere:

- un atto che costituisce reato come definito in uno dei trattati elencati nell'allegato; ovvero
- qualsiasi altro atto diretto a causare la morte o gravi lesioni fisiche ad un civile, o a qualsiasi altra persona che non abbia parte attiva in situazioni di conflitto armato, quando la finalità di tale atto sia quella di intimidire una popolazione, od obbligare un governo o un'organizzazione internazionale a compiere o ad astenersi dal compiere qualcosa.

Perché un atto costituisca uno dei suddetti reati non è necessario che i fondi siano effettivamente utilizzati per compiere quanto descritto alle lettere (a) e (b).

Commette ugualmente reato chiunque tenti di commettere i reati sopra previsti.

Commette altresì un reato chiunque:

- prenda parte in qualità di complice al compimento di un reato di cui sopra;
- organizzi o diriga altre persone al fine di commettere un reato di cui sopra;
- contribuisca al compimento di uno o più reati di cui sopra con un gruppo di persone che agiscono con una finalità comune. Tale contributo deve essere intenzionale e deve essere compiuto al fine di facilitare l'attività o la finalità criminale del gruppo, laddove tale attività o finalità implicino la commissione del reato; o deve essere fornito con la piena consapevolezza che l'intento del gruppo è di compiere un reato.

Tra le condotte criminose integrative delle fattispecie di reato di terrorismo, quelle che potrebbero facilmente realizzarsi sono le condotte consistenti nel "finanziamento" (vedi art. 270-bis c.p.).

Al fine di poter affermare se sia o meno ravvisabile il rischio di commissione di tale tipologia di reati, occorre esaminare il profilo soggettivo richiesto dalla norma ai fini della configurabilità del reato.

Dal punto di vista dell'elemento soggettivo, i reati di terrorismo si configurano come reati dolosi. Quindi, perché si realizzi la fattispecie dolosa è necessario, dal punto di vista della rappresentazione psicologica dell'agente, che il medesimo abbia coscienza dell'evento antigiuridico e lo voglia realizzare attraverso una condotta a lui attribuibile. Pertanto, affinché si possano configurare le fattispecie di reato in esame, è necessario che l'agente abbia coscienza del carattere terroristico dell'attività e abbia l'intento di favorirla.

Ciò detto, perché si configuri una condotta criminosa integrativa del reato di terrorismo, è necessario che l'agente abbia coscienza del fatto che l'associazione alla quale concede il finanziamento si prefigga fini di terrorismo o di eversione e che abbia l'intento di favorirne l'attività. Peraltro, sarebbe altresì configurabile il perfezionamento della fattispecie criminosa anche qualora il soggetto agisse a titolo di dolo eventuale. In tal caso, l'agente dovrebbe prevedere ed accettare il rischio del verificarsi dell'evento, pur non volendolo direttamente. La previsione del rischio del verificarsi dell'evento e la determinazione volontaria nell'adottare la condotta criminosa devono desumersi da elementi univoci e obiettivi.

CAPITOLO IV.2 – LE ATTIVITÀ SENSIBILI

Le Attività Sensibili nell'ambito dei Reati in oggetto che la Società ha individuato al proprio interno sono le seguenti.

Riguardo alle attività svolte con la Clientela, un più elevato e potenziale rischio di riciclaggio potrebbe rilevarsi con riferimento ai rapporti con la Clientela e ad ipotesi di coinvolgimento/concorso in attività criminose della stessa; in particolare le attività identificate sono:

1. Instaurazione e gestione dei rapporti con la Clientela.
2. Esecuzione di operazioni disposte dalla Clientela.
3. Gestione degli adempimenti in materia di Antiriciclaggio.

Per quanto concerne i rischi legati alle attività condotte da Compagnia Privata come “società” per i reati di: **ricettazione**, si individuano le seguenti attività

1. Selezione di Fornitori, Consulenti e *Partner* e gestione dei relativi rapporti.

Per quanto concerne i rischi legati alle attività condotte da Compagnia Privata come “società” per i reati di: **terrorismo o eversione dell'ordine democratico e trasferimento fraudolento di valori**, si individuano le seguenti attività

1. Selezione, assunzione e gestione del personale (compresi i rimborsi spese).
2. Attività di investimento in Paesi a rischio terrorismo.

In relazione al **reato di autoriciclaggio**, le attività ritenute più specificamente a rischio risultano essere quelle in grado di generare proventi illeciti investibili vale a dire:

1. Formazione e tenuta della contabilità, del bilancio d'esercizio, delle relazioni o di altre comunicazioni societarie previste dalla legge.
2. Gestione degli adempimenti tributari e fiscali.
3. Gestione delle controversie e conclusione di accordi transattivi.
4. Gestione delle operazioni societarie ordinarie e straordinarie.
5. Gestione dei flussi finanziari.
6. Gestione omaggi, spese di rappresentanza, sponsorizzazioni e beneficenze.

CAPITOLO IV.3 - PRINCIPI GENERALI DI COMPORTAMENTO

IV.3.1 Il sistema in linea generale

Obiettivo della presente Parte Speciale, al fine di prevenire la commissione dei Reati oggetto della medesima, è che tutti i Destinatari del Modello si attengano al rispetto di tutte le procedure e ai principi che siano direttamente o indirettamente funzionali alla prevenzione degli stessi, come presidio fondamentale per il buon funzionamento, l'affidabilità e la reputazione della Società.

I Destinatari, anche in relazione al tipo di rapporto posto in essere con la Società, dovranno attenersi ai seguenti principi di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai Reati di Riciclaggio, Reati di terrorismo e di trasferimento fraudolento di valori;
2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di Reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di Consulenti, Fornitori, *Partner* e clienti anche stranieri;
4. non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura;
5. non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
6. effettuare un costante monitoraggio dei flussi finanziari aziendali;
7. astenersi dall'alterare in qualsiasi modo il funzionamento di sistemi informatici o telematici o intervenire sui contenuti di detti sistemi al fine di realizzare un trasferimento di denaro, di valore monetario o di valuta virtuale.

Per Compagnia Privata trovano, in particolare, applicazione i seguenti principi generali.

L'attività di prevenzione si basa sulla approfondita conoscenza della Clientela e delle controparti e sulla osservanza degli adempimenti previsti dalla normativa in tema di contrasto al riciclaggio dei proventi di attività criminosi ed al finanziamento del terrorismo.

Al fine di prevenire ed impedire il verificarsi dei reati di ricettazione, riciclaggio e impiego di denaro di provenienza illecita, individuati al precedente paragrafo, ai Destinatari coinvolti nello svolgimento delle Attività Sensibili individuate, Compagnia Privata richiede il rispetto dei seguenti principi generali di comportamento, in particolare, è fatto obbligo di:

- tenere un comportamento corretto, trasparente e di collaborazione, nel rispetto delle norme di legge, in tutte le attività inerenti l'operatività aziendale ed in particolare nell'ambito delle attività sensibili, mantenendosi aggiornati sull'evoluzione normativa in materia;
- ispirarsi a criteri di trasparenza nell'esercizio dell'attività aziendale e nella scelta di Fornitori, dei Consulenti e dei *Partner* commerciali e finanziari, prestando la massima attenzione alle notizie riguardanti i soggetti terzi;
- assicurare la tracciabilità delle fasi del processo decisionale relativo ai rapporti finanziari e societari con soggetti terzi;
- assicurare la tracciabilità dei controlli posti in essere, garantendo che la conservazione dei documenti sia di supporto e a sostegno di eventuali verifiche successive;
- informare prontamente l'OdV qualora sorga il ragionevole dubbio di trovarsi di fronte ad un'evenienza che possa ricondurre a situazioni connesse ai reati di cui sopra;
- informare tempestivamente il Responsabile della funzione Antiriciclaggio – nel rispetto delle disposizioni previste dalla regolamentazione interna – ogniqualvolta si sia a conoscenza, si sospetti o si abbiano motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo.

Inoltre, al fine di prevenire ed impedire il verificarsi dei delitti con finalità di terrorismo o di eversione dell'ordine democratico, i Destinatari coinvolti nello svolgimento delle Attività Sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta, in particolare è fatto obbligo di:

- astenersi dal fornire, direttamente o indirettamente, finanziamenti a favore di soggetti che perseguono, direttamente o in qualità di prestanome, finalità di terrorismo o eversione dell'ordine democratico;
- astenersi dal riconoscere compensi in favore di terzi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere.

La Società, a sua volta, al fine di prevenire il rischio di commissione dei Reati di Riciclaggio, dei Reati con finalità di Terrorismo e del Reato di Finanziamento del Terrorismo:

- adotta un sistema di individuazione e gestione del rischio di Riciclaggio e Finanziamento del Terrorismo conforme a quanto previsto dalle disposizioni normative tempo per tempo vigenti;
- adotta sistemi, anche informatici, di identificazione e valutazione del profilo di rischio della Clientela che consentano la corretta imputazione di ogni operazione di apertura e chiusura dei rapporti con i clienti;
- garantisce che il processo di registrazione, valutazione e archiviazione delle informazioni nonché conservazione della documentazione relativa alle attività di adeguata verifica della Clientela avvenga attraverso un'istruttoria con controlli periodici sulla corretta esecuzione dell'attività;

- adotta sistemi organizzativi, anche informatici, volti a consentire la rilevazione e segnalazione di operazioni ritenute anomale per tipologia, oggetto, frequenza o dimensioni;
- adotta specifiche procedure per la selezione e la gestione dei rapporti con Consulenti e Fornitori;
- adotta presidi idonei a prevenire il rischio di finanziamento del terrorismo;
- adotta presidi idonei a prevenire investimenti in “Paesi a rischio di terrorismo”;
- effettua un costante e regolare monitoraggio dei flussi finanziari aziendali, garantendone la tracciabilità e fornendo evidenza giustificativa di ciascuno di essi.

Al fine di prevenire ed impedire il verificarsi del reato di autoriciclaggio, i Destinatari coinvolti nello svolgimento delle Attività Sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta, in particolare è fatto divieto di:

- emettere fatture o altri documenti contabili relativi ad operazioni in tutto o in parte inesistenti;
- emettere fatture o altri documenti contabili per corrispettivi (o IVA) superiori agli importi reali;
- effettuare pagamenti a fronte dell'emissione di fatture relative ad attività non ricevute;
- occultare o distruggere tutti o parte dei documenti la cui tenuta è obbligatoria, in modo da rendere impossibile la ricostruzione di tutta la gestione economico/fiscale dell'anno.

Per l'attuazione di tali principi si rinvia al dettaglio delle procedure, di cui al successivo paragrafo.

Ai fini della presente Parte Speciale, si evidenzia che i reati in materia di riciclaggio di denaro o beni potrebbero essere potenzialmente commessi da parte della Società anche nell'ambito di operazioni societarie. Infatti, le operazioni societarie che comportano nuovi afflussi di capitale, sia di debito sia proprio, sono un possibile strumento di riciclaggio di denaro, qualora i soggetti finanziatori o soci, immettano nel patrimonio della Società denari di provenienza illecita, utilizzando quindi Compagnia Privata per ottenere successivamente denaro in modo lecito, grazie al rimborso del capitale di debito o la vendita delle azioni stesse.

CAPITOLO IV.4 – PRINCIPI SPECIFICI DI COMPORTAMENTO

Ai fini dell'attuazione delle regole elencate al precedente Capitolo, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali qui di seguito descritti per le singole Attività Sensibili. Tali principi potranno trovare attuazione anche per mezzo dell'adozione di specifiche procedure aziendali.

1. Instaurazione e gestione dei rapporti con la Clientela

- In relazione ai potenziali rischi di commissione reato sopra evidenziati, la Società ha implementato un sistema di presidi operativi e di controllo che prevede:
 - individuazione dei compiti e delle responsabilità;
 - definizione di differenti livelli decisionali e autorizzativi all'interno della struttura organizzativa;
 - segregazione dei compiti nell'ambito dell'attività di identificazione del Cliente e di adeguata verifica della Clientela;
 - attività di verifica nella gestione del processo di identificazione della Clientela;
- tali attività di verifica prevedono tra l'altro:
 - applicazione di regole volte a disciplinare il processo di adeguata verifica della Clientela finalizzate al corretto assolvimento dell'obbligo in materia (es. nel caso in cui non sia possibile rispettare gli obblighi di adeguata verifica, è vietato procedere all'instaurazione di rapporti ed eseguire operazioni di alcun genere ovvero è obbligatorio porre fine ai rapporti in essere);
 - applicazione di regole volte ad adottare misure rafforzate di adeguata verifica della Clientela e individuazione delle attività da porre in essere, nonché delle eventuali autorizzazioni necessarie, al fine di rispettare il corretto assolvimento dell'obbligo in materia;
 - verifica, all'atto dell'accensione del rapporto, della correttezza e della completezza dei dati censiti in anagrafica;
 - aggiornamento delle suddette informazioni in relazione alle motivazioni economiche sottostanti alle operazioni richieste o eseguite;
 - verifica dell'eventuale presenza del Cliente o del titolare effettivo nelle versioni aggiornate delle liste specifiche (*black-list*) e valutazione di ogni altra notizia o fatto, riguardante il Cliente, di cui la SIM venga a conoscenza, in occasione del censimento e, successivamente, su base periodica;
 - aggiornamento periodico della valutazione della Clientela tramite la verifica della coerenza tra il profilo assegnato al Cliente, la tipologia di operazione, la frequenza e le modalità di esecuzione, l'area geografica di riferimento (con particolare riguardo

all'operatività da/verso Paesi a rischio), il grado di rischio del prodotto, i fondi impiegati, l'orizzonte temporale dell'investimento, il comportamento tenuto dal Cliente al momento dell'esecuzione dell'operazione (se conosciuto);

- costante valutazione della natura e dello scopo dell'operazione eseguita dalla Clientela (ad es. analisi su transazioni rilevanti);
 - applicazione di regole volte a disciplinare le modalità ed i criteri di analisi e valutazione delle operazioni anomale e il processo di segnalazione delle operazioni sospette;
 - applicazione di regole volte a garantire la riservatezza delle informazioni trattate.
- È presente presenza di un sistema di controllo interno con il compito di monitorare e di presidiare la puntuale esecuzione delle seguenti attività:
 - acquisizione delle informazioni per l'identificazione e la profilatura della Clientela;
 - valutazione delle operazioni rilevate dalle procedure informatiche in uso;
 - rilevazione e valutazione degli altri indici di anomalia eventualmente presenti;
 - registrazione dei rapporti delle operazioni e conservazione della documentazione;
 - fruizione della sistematica formazione prevista per i dipendenti.
 - La Società garantisce la tracciabilità dei processi tramite l'archiviazione di tutta la documentazione a supporto delle attività svolte; al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate nonché l'adozione di una procedura informatica volta a costruire il profilo di rischio riciclaggio della Clientela.

2. Esecuzione di operazioni disposte dalla Clientela

In relazione all'esecuzione di operazioni disposte dalla Clientela, la Società:

- al compimento di operazioni oltre la soglia di legge, anche se frazionate:
 - procede all'identificazione della Clientela, e verifica l'eventuale presenza del nominativo nelle versioni aggiornate delle "*black-list*";
 - verifica, la sussistenza di eventuali titolari effettivi, acquisisce informazioni sullo scopo e sulla natura dell'operazione e, qualora il Cliente sia una società o un Ente, verifica la sussistenza dei poteri di rappresentanza e la struttura di proprietà e di controllo del Cliente;
 - procede alla profilatura della Clientela;
- pone in essere tutti i presidi previsti dalla normativa in materia di Antiriciclaggio, (attività di adeguata verifica della Clientela, registrazione e segnalazione di eventuali Operazioni Sospette);

- adotta adeguati presidi che impediscano l'effettuazione di versamenti aggiuntivi da parte di soggetti diversi dai cointestatari o dai soggetti delegati;
- adotta sistemi di controllo atti ad impedire l'operatività riguardanti soggetti/Paesi oggetto di restrizioni di natura finanziaria e/o commerciale.

3. Gestione degli adempimenti in materia di Antiriciclaggio

La Società:

- in adempimento alla normativa nazionale, ha istituito una Funzione Antiriciclaggio e nominato il relativo Responsabile. Si tratta di una Funzione indipendente preposta al presidio della conformità dei processi aziendali in relazione alle prescrizioni contenute nelle norme di legge, nelle disposizioni regolamentari, nei codici di comportamento e nella normativa interna in materia di antiriciclaggio;
- la Funzione Antiriciclaggio ha accesso a qualsiasi informazione rilevante per lo svolgimento dei propri compiti e riferisce direttamente agli Organi di vertice;
 - ha provveduto a formalizzare l'attribuzione delle responsabilità per la segnalazione delle operazioni sospette (Responsabile SOS);
 - ha ripartito all'interno della propria struttura le attività connesse ai seguenti "pilastri" fondamentali previsti dalla normativa comunitaria in materia di antiriciclaggio e dal D.Lgs. 231/2007:
 - adeguata verifica della Clientela;
 - determinazione e monitoraggio del profilo di rischio del Cliente;
 - monitoraggio dell'operatività del Cliente ed evidenza dei comportamenti sospetti o anomali;
 - valutazione delle operazioni considerate anomale o inattese, sulla base della correlazione tra le stesse e il profilo di rischio assegnato al Cliente;
 - segnalazione delle operazioni sospette all'Unità di Informazione Finanziaria (UIF);
 - invio mensile all'UIF dei dati raccolti, aggregati secondo criteri prestabiliti dalla UIF stessa;
 - formazione del personale, dei collaboratori e degli intermediari in materia di antiriciclaggio e contrasto del terrorismo.
- Inoltre, la Funzione Antiriciclaggio
 - ha l'onere di verificare nel continuo che le procedure aziendali siano coerenti con l'obiettivo di prevenire e contrastare la violazione della normativa in materia di antiriciclaggio e di contrasto al finanziamento del terrorismo;

- predispone flussi informativi periodici destinati al Collegio Sindacale, all'Amministratore Delegato e all'Organismo di Vigilanza 231, nonché flussi annuali al Consiglio di Amministrazione con riferimento alle attività svolte, alle disfunzioni accertate e alle relative azioni da intraprendere;
- effettua controlli *ex ante* (formulazione di pareri e consulenze, adeguata verifica rafforzata della Clientela) ed *ex post* a presidio del rischio di riciclaggio;
- applica misure rafforzate di adeguata verifica della Clientela oltre che in presenza di un Cliente cui è stato assegnato un profilo di rischio alto, nel caso di operatività a distanza, persone politicamente esposte (PEP/PIL) e conti di corrispondenza con corrispondenti di Stati extra-UE.

4. Selezione di Fornitori, Consulenti e *Partner* e gestione dei relativi rapporti

- La Società ha implementato procedure/*policy* aziendali volte a garantire che il processo di selezione delle terze parti avvenga nel rispetto dei criteri di trasparenza, pari opportunità di accesso, professionalità, affidabilità ed economicità, fermo restando la prevalenza dei requisiti di legalità rispetto a tutti gli altri. Tali procedure/*policy* prevedono: (i) l'espletamento di una adeguata attività di selezione tra differenti fornitori con la comparazione di più preventivi, dalla quale emergano chiaramente i criteri di scelta adottati; (ii) la verifica legale e amministrativa del contratto prima della sua sottoscrizione; (iii) la previsione, nei rapporti contrattuali con Fornitori e Consulenti, di specifiche Clausole 231.
- La Società garantisce la verifica che le controparti contrattuali con le quali vengono concluse operazioni di rilevante entità, non abbiano sede o residenza in Paesi considerati ad alto rischio dal GAFI e non siano ricomprese nelle Liste Nominative pubblicate dalla UIF. Nel caso in cui dalle verifiche emerga un coinvolgimento in operazioni con soggetti i cui nominativi siano contenuti nelle Liste Nominative (o i quali siano notoriamente controllati da soggetti contenuti nelle liste medesime) o con soggetti aventi sede o residenza in Paesi considerati come non cooperativi dal GAFI, le medesime operazioni devono essere automaticamente sospese per essere sottoposte alla valutazione interna da parte dell'OdV e all'espressa autorizzazione del Consiglio di Amministrazione.
- È prevista l'applicazione di regole volte a disciplinare l'*iter* di attestazione della congruità della prestazione ricevuta, da parte della funzione preposta, finalizzato alla successiva autorizzazione al pagamento.
- La Società garantisce la tracciabilità di tutte le attività per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte effettuate e delle informazioni utilizzate.

5. Selezione, assunzione e gestione del personale (compresa la gestione dei rimborsi spese)

- La Società prevede attività di verifica connesse alla gestione della selezione, valutazione e gestione amministrativa del personale. Le attività prevedono tra l'altro:

- l'applicazione di regole volte a disciplinare i criteri di selezione del personale;
- l'applicazione di regole volte a disciplinare le modalità di autorizzazione da parte del responsabile competente delle note spese, a seguito della verifica dei relativi giustificativi

Si rinvia, inoltre, ai presidi indicati con riferimento alla medesima Attività Sensibile nella sezione della Parte Speciale I relativa ai reati di corruzione.

6. Attività di investimento in Paesi a rischio terrorismo

- In relazione alle attività di investimento in “Paesi a rischio terrorismo”, la Società effettua un controllo costante sulle attività di investimento.
- È stato istituito un controllo che prevede il blocco automatico dell'operatività con Paesi presenti nella *black-list* emanata e aggiornata dalle autorità italiane competenti.

7. Formazione e tenuta della contabilità, del bilancio d'esercizio, delle relazioni o di altre comunicazioni societarie previste dalla legge

- La Società ha adottato un sistema di controlli che prevede:
 - segregazione dei compiti nell'ambito delle attività di gestione del processo amministrativo - contabile e di redazione dei documenti di bilancio nel rispetto dei livelli autorizzativi definiti in base al sistema delle deleghe in essere;
 - attività di verifica connesse alla gestione del processo amministrativo-contabile e di redazione dei documenti di bilancio.
- Le attività di verifica riguardano tra l'altro:
 - l'applicazione di regole volte a disciplinare il processo di produzione dei dati per la contabilità e dei *report* gestionali;
 - la verifica di correttezza e completezza delle informazioni relative alle registrazioni contabili;
 - la verifica di correttezza e completezza delle informazioni necessarie alla redazione dei documenti di bilancio;
 - l'applicazione di regole volte a disciplinare l'esecuzione degli adempimenti per il deposito del bilancio a seguito della approvazione;
 - tracciabilità di tutte le attività tramite l'archiviazione della documentazione a supporto dell'attività e dei controlli svolti in relazione alle attività di gestione della contabilità.

8. Gestione degli adempimenti tributari e fiscali

- La Società ha adottato un sistema di controlli che prevede che:
 - non vengano indicati nelle dichiarazioni fiscali elementi passivi fittizi avvalendosi di fatture o altri documenti per operazioni inesistenti;

- non vengano ivi indicati elementi attivi per un ammontare inferiore a quello effettivo ovvero elementi passivi fittizi;
- non venga indicata una base imponibile in misura inferiore a quella effettiva;
- non siano fatti decorrere inutilmente i termini previsti dalla normativa applicabile per la presentazione delle dichiarazioni fiscali così come per il successivo versamento delle imposte dovute.

Si rinvia, inoltre, ai presidi indicati con riferimento alla medesima Attività Sensibile nella sezione della Parte Speciale VIII relativa ai reati tributari.

9. Gestione delle controversie e conclusione di accordi transattivi

Si rinvia ai presidi indicati con riferimento alla medesima Attività Sensibile nella sezione della Parte Speciale I relativa ai reati contro la P.A.

10. Gestione delle operazioni societarie ordinarie e straordinarie

- La Società ha adottato un sistema di controlli che prevede che:
 - la segregazione dei compiti nell'ambito delle attività di gestione delle operazioni sul capitale sociale nel rispetto dei livelli autorizzativi definiti in base al sistema delle deleghe in essere;
 - la verifica del rispetto dei vincoli normativi e statutari in tema di operazioni ordinarie (ad esempio distribuzione degli utili) e straordinarie (ad esempio fusioni);
 - tracciabilità di tutte le attività tramite l'archiviazione degli atti e dei documenti a supporto delle attività.
- Inoltre, tutte le operazioni che hanno un impatto sul capitale sociale della Società e le operazioni straordinarie sono svolte nel rispetto della normativa vigente, dello Statuto sociale e supportate, ove necessario, da valutazioni effettuate da esperti esterni dotati dei requisiti di professionalità e indipendenza.

11. Gestione dei flussi finanziari

- Tutti i flussi finanziari in entrata e in uscita devono essere adeguatamente identificabili e tracciabili, nonché correttamente e regolarmente registrati in appositi libri e registri contabili.
- Tutti i flussi finanziari in entrata e in uscita devono essere supportati da specifica documentazione giustificatrice, che riporti chiaramente e fedelmente le transazioni a cui fa riferimento.
- La Società garantisce il principio di segregazione dei ruoli tra i soggetti (interni o esterni) che autorizzano, coloro che eseguono e coloro che controllano i flussi finanziari in entrata e in uscita.
- La Società individua preventivamente gli esponenti aziendali a cui sono conferiti i poteri di spesa attraverso apposite procure ovvero delibere del Consiglio di Amministrazione, al fine di garantire la chiara individuazione a posteriori del soggetto avente i poteri di spesa per ogni transazione finanziaria effettuata.

- La Società effettua controlli dei flussi finanziari aziendali in entrata ed uscita; tali controlli devono tener conto degli istituti di credito utilizzati (sede delle banche coinvolte nelle operazioni) e di eventuali schermi societari e strutture fiduciarie utilizzate per eventuali operazioni straordinarie, nonché della sede legale della società controparte e del luogo di destinazione o provenienza del denaro in uscita o in entrata (ad esempio, paradisi fiscali, Paesi rientranti nelle black-list internazionali, ecc.).
- È fatto divieto di trasferimento di denaro contante o di titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) in Euro o in valuta estera, effettuato a qualsiasi titolo quando il valore dell'operazione è pari o superiore a Euro 1.000. Il trasferimento può tuttavia essere eseguito per il tramite di banche, istituti di moneta elettronica e Poste Italiane S.p.A.
- Nel caso la Società effettui attività di investimento del patrimonio aziendale, la stessa viene condotta con modalità trasparenti e tali da rendere sempre tracciabili i relativi flussi di denaro.

12. Gestione omaggi, spese di rappresentanza, sponsorizzazioni e beneficenze

- La Società ha adottato un sistema di controlli che prevede che:
 - segregazione dei compiti nell'ambito delle attività connesse con la gestione di omaggi, spese di rappresentanza, sponsorizzazioni e beneficenze nel rispetto dei livelli autorizzativi definiti in base al sistema delle deleghe in essere;
 - attività di verifica connesse alla gestione degli omaggi, spese di rappresentanza sponsorizzazioni e beneficenze.
- Le attività di verifica riguardano tra l'altro:
 - l'applicazione di regole volte a disciplinare l'iter autorizzativo per la gestione delle spese di rappresentanza, sponsorizzazioni ed erogazioni liberali;
 - tracciabilità delle attività tramite l'archiviazione di tutta la documentazione a supporto delle attività svolte e delle autorizzazioni ottenute.

Si rinvia, inoltre, ai presidi indicati con riferimento alla medesima Attività nella sezione della Parte Speciale I relativa ai reati contro la P.A.

* * *

Per ogni aspetto di maggiore dettaglio riferibile – anche indirettamente – alle Attività Sensibili sopra indicate e, in generale, alla prevenzione del rischio di commissione di Reati Presupposto astrattamente rilevanti in relazione alla presente Parte Speciale, si rimanda anche espressamente al contenuto – *inter alia* – dei seguenti documenti normativi interni:

- *policy* di gestione delle risorse umane;
- manuale delle procedure antiriciclaggio per il personale;
- regolamento della funzione antiriciclaggio;
- *policy* antiriciclaggio;



- *policy* di gestione delle risorse umane;
- *policy* delle funzioni esternalizzate;
- *policy* gestione sistema informatico;
- *Policy* delle funzioni esternalizzate e in *Cloud*;
- procedure attività di gestione;
- procedura del servizio di consulenza.

CAPITOLO IV.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

Con riferimento alla presente Parte Speciale, ogni funzione coinvolta deve comunicare per quanto di competenza e con periodicità definita quanto previsto nella seguente tabella (si precisa che i flussi in oggetto, all'occorrenza, possono eventualmente essere forniti in occasione di incontri *de visu* con l'OdV):

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
Responsabile AML	Report di sintesi dell'avvenuta segnalazione SARA (Segnalazioni Antiriciclaggio Aggregate)	Mensile
	Segnalazioni di eventuali operazioni sospette di riciclaggio	Ad evento
	I nuovi incarichi di consulenza di importo significativo conferiti a terzi	Ad evento
	La relazione periodica prodotta dalla funzione antiriciclaggio, in merito all'attività svolta, alle eventuali criticità riscontrate, alle corrispondenti azioni correttive individuate, nonché alle attività di formazione svolte	Annuale
	Esito monitoraggio dell'efficacia delle procedure interne per la prevenzione dei Reati di Riciclaggio, Finanziamento del Terrorismo e Reati con Finalità di Terrorismo	Annuale



PARTE SPECIALE – V – Delitti di criminalità organizzata e reati transnazionali

CAPITOLO V.1 - LE FATTISPECIE DEI REATO

Si fornisce qui di seguito una breve descrizione della fattispecie di cui all'art. 24 *ter* del Decreto ritenuta astrattamente rilevante per la Società.

ASSOCIAZIONE PER DELINQUERE (ART. 416 C.P.)

La condotta sanzionata dall'art. 416 c.p. è integrata mediante la costituzione e la conservazione di un vincolo associativo continuativo con fine criminoso tra tre o più persone, allo scopo di commettere una serie indeterminata di delitti, con la predisposizione di mezzi necessari per la realizzazione del programma criminoso e con la permanente consapevolezza di ciascun associato di far parte di un sodalizio e di essere disponibile ad operare per l'attuazione del programma delinquenziale.

Il reato associativo è caratterizzato, pertanto, dai seguenti elementi fondamentali:

1. stabilità e permanenza: il vincolo associativo deve essere tendenzialmente stabile e destinato a durare anche oltre la realizzazione dei delitti concretamente programmati;
2. indeterminatezza del programma criminoso: l'associazione a delinquere non si configura se i partecipanti si associano al fine di compiere un solo reato; lo scopo dell'associazione deve essere quello di commettere più delitti, anche della stessa specie (in tal caso l'indeterminatezza del programma criminoso ha riguardo solo all'entità numerica);
3. esistenza di una struttura organizzativa: l'associazione deve prevedere un'organizzazione di mezzi e di persone che, seppure in forma rudimentale, siano adeguati a realizzare il programma criminoso e a mettere in pericolo l'ordine pubblico.

In particolare, sono puniti coloro che promuovono, costituiscono o organizzano l'associazione, oltre a coloro che regolano l'attività collettiva da una posizione di superiorità o supremazia gerarchica, definiti dal testo legislativo come "capi".

Sono puniti altresì con una pena inferiore tutti coloro che partecipano all'associazione.

Il reato in questione assume rilevanza ai fini della responsabilità amministrativa degli enti anche se commesso a livello "*transnazionale*" ai sensi dell'art. 10 della Legge 16 marzo 2006, n. 146 (legge di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale).

A tal riguardo giova sottolineare che ai sensi dell'art. 3 della suddetta legge si considera "*transnazionale*" il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

- sia commesso in più di uno Stato;
- ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
- ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;



- ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.



CAPITOLO V.2 – LE ATTIVITÀ SENSIBILI IN RELAZIONE AI REATI DI CRIMINALITÀ ORGANIZZATA

L'Attività Sensibile nell'ambito dei reati di criminalità organizzata che la Società ha individuato al proprio interno è la seguente:

- 1. Selezione delle controparti contrattuali (Clienti e Fornitori, Consulenti e *Partner*)**

CAPITOLO V.3 – PRINCIPI GENERALI DI COMPORTAMENTO

Obiettivo della presente Parte Speciale, al fine di prevenire la commissione dei Reati oggetto della medesima, è che tutti i Destinatari del Modello si attengano al rispetto di tutte le procedure e ai principi che siano direttamente o indirettamente funzionali alla prevenzione dei suddetti Reati.

In particolare, si prevede l'espresso divieto a carico dei Destinatari di:

1. porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
2. instaurare rapporti con soggetti terzi - persone fisiche o giuridiche, italiane o straniere - senza aver rispettato criteri e metodologie di selezione previsti dalle procedure aziendali che consentano di accertarne onorabilità e affidabilità;
3. intestare conti correnti a prestanomi, aprire e gestire fondi extracontabili e intestare beni fittiziamente.

Devono altresì essere rispettati i seguenti obblighi:

1. il processo di selezione delle controparti contrattuali è costantemente regolato dal principio della segregazione dei ruoli;
2. la persistenza in capo a controparti contrattuali dei requisiti richiesti in fase di selezione è sottoposta a periodici controlli.

CAPITOLO V.4 – PRINCIPI SPECIFICI DI COMPORTAMENTO

Ai fini dell'attuazione delle regole elencate al precedente Capitolo, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali qui di seguito descritti. Tali principi potranno trovare attuazione anche per mezzo dell'adozione di specifiche procedure aziendali.

1. Selezione delle controparti contrattuali (Clienti e Fornitori, Consulenti e *Partner*)

1. La Società garantisce la verifica che le controparti contrattuali con le quali vengono concluse operazioni di rilevante entità, non abbiano sede o residenza in Paesi considerati ad alto rischio dal GAFI e non siano ricomprese nelle Liste Nominative pubblicate dalla UIF. Nel caso in cui dalle verifiche emerga un coinvolgimento in operazioni con soggetti i cui nominativi siano contenuti nelle Liste Nominative (o i quali siano notoriamente controllati da soggetti contenuti nelle Liste medesime) o con soggetti aventi sede o residenza in Paesi considerati come non cooperativi dal GAFI, le medesime operazioni devono essere automaticamente sospese per essere sottoposte alla valutazione interna da parte dell'OdV e all'espressa autorizzazione del Consiglio di Amministrazione.
2. Nel processo di approvvigionamento, Compagnia Privata si focalizza sulla qualifica dei fornitori, in modo da assicurare il rispetto da parte di questi delle normative vigenti in materia di salute e sicurezza e in materia di diritto sindacale, nonché gli adempimenti a favore dei lavoratori prescritti dalle principali fonti di contrattazione collettiva.
3. La Società prevede che le pattuizioni contrattuali con le controparti contengano Clausole 231.
4. In relazione ai Consulenti, Fornitori e *Partner* principali e/o esposti a maggior rischio di commissione dei reati alla luce della tipologia dell'attività espletata, la Società effettua una *due diligence* rafforzata (anche avvalendosi di società specializzate) volta a scongiurare il rischio di instaurare rapporti con imprese legate alla criminalità organizzata.
5. La Società prevede specifiche verifiche in relazione alla Clientela secondo le procedure applicabili.

Si rinvia ai presidi indicati nella Parte Speciale IV relativa ai reati di riciclaggio.

* * *

Per ogni aspetto di maggiore dettaglio riferibile – anche indirettamente – alle Attività Sensibili sopra indicate e, in generale, alla prevenzione del rischio di commissione di Reati Presupposto astrattamente rilevanti in relazione alla presente Parte Speciale, si rimanda anche espressamente al contenuto dei seguenti documenti normativi interni:

- *policy* di gestione delle risorse umane;
- *policy* delle funzioni esternalizzate;
- *Policy* delle funzioni esternalizzate e in *Cloud*.

CAPITOLO V.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

Con riferimento alla presente Parte Speciale, ogni funzione coinvolta deve comunicare per quanto di competenza e con periodicità definita quanto previsto nella seguente tabella (si precisa che i flussi in oggetto, all'occorrenza, possono eventualmente essere forniti in occasione di incontri *de visu* con l'OdV):

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
<i>Compliance</i>	Segnalazione di eventuali denunce, indagini e/o procedimenti penali pendenti a carico di Fornitori, Consulenti e <i>Partner</i> o Clienti di cui si abbia conoscenza.	Ad evento



PARTE SPECIALE – VI – Reati di omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, impiego di cittadini di paesi terzi il cui soggiorno è irregolare, delitti contro la personalità individuale e reati ambientali

CAPITOLO VI.1 - LE FATTISPECIE DEI REATO

VI.1.1 Reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies del D.Lgs. 231/2001)

Si provvede qui di seguito a fornire una breve descrizione dei reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro indicati all'art. 25-septies del Decreto.

Detto articolo, originariamente introdotto dalla legge 3 agosto 2007 n. 123, e successivamente sostituito nell'attuale formulazione dall'art. 300 del D.Lgs. 9 aprile 2008, n. 81 ("TUSL"), prevede l'applicazione di sanzioni pecuniarie ed interdittive agli enti i cui Esponenti della Società commettano i reati di cui agli artt. 589 (omicidio colposo) e 590 terzo comma (lesioni personali colpose gravi o gravissime) del codice penale, in violazione delle norme sulla tutela della salute e sicurezza sul lavoro. Le fattispecie delittuose inserite all'art. 25-septies riguardano unicamente le ipotesi in cui l'evento sia stato determinato non già da colpa di tipo generico (e dunque per imperizia, imprudenza o negligenza) bensì da "colpa specifica" che richiede che l'evento si verifichi a causa della inosservanza delle norme sulla salute e sicurezza sul lavoro.

OMICIDIO COLPOSO (ART. 589 C. P.)

Il reato si configura ogni qualvolta un soggetto cagioni per colpa la morte di altro soggetto.

LESIONI PERSONALI COLPOSE GRAVI O GRAVISSIME (ART. 590, COMMA 3, C. P.)

Il reato si configura ogni qualvolta un soggetto, in violazione delle norme per la prevenzione degli infortuni sul lavoro, cagioni per colpa ad altro soggetto lesioni gravi o gravissime.

Ai sensi del comma 1 dell'art. 583 c. p., la lesione è considerata grave nei seguenti casi:

"1) se dal fatto deriva 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 ai quaranta giorni;

2) se il fatto produce l'indebolimento permanente di un senso o di un organo".

Ai sensi del comma 2 dell'art. 583 cod. pen., *"la lesione è considerata invece gravissima se dal fatto deriva:*

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

In questa sede è opportuno ricordare che il TUSL ha stabilito un contenuto minimo essenziale del modello organizzativo in questa materia. L'articolo 30, comma da 1 a 4, TUS, infatti, dispone che:

“Il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al decreto legislativo 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l’adempimento di tutti gli obblighi giuridici relativi:

- a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- d) alle attività di sorveglianza sanitaria;
- e) alle attività di informazione e formazione dei lavoratori;
- f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
- h) alle periodiche verifiche dell’applicazione e dell’efficacia delle procedure adottate.

VI.1.2 Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 25-*duodecies* del D.Lgs. 231/2001)

La presente Parte Speciale si riferisce altresì all’*“impiego di cittadini di Paesi terzi il cui soggiorno è irregolare”* (art. 22, comma 12 bis, D.Lgs. n. 286/1998), fattispecie introdotta nel novero dei Reati Presupposto del Decreto 231, all’art. 25-*duodecies*, dal D. Lgs. 16 luglio 2012, n. 109, il quale, entrato in vigore il 9 agosto 2012, disciplina l’attuazione della Direttiva 2009/52/CE, e ritenuta applicabile alla Società.

Tale reato si configura qualora il soggetto che riveste la qualifica di datore di lavoro occupi alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, o sia stato revocato o annullato, laddove i lavoratori occupati siano:

- a) in numero superiore a tre;
- b) minori in età non lavorativa;
- c) sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell’art. 603-*bis* c.p.

In particolare, le condizioni lavorative di cui al punto c) che precede riguardano l’esposizione dei lavoratori a situazioni di grave pericolo con riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

Si segnala che l'art. 25-*duodecies* è stato oggetto di modifiche ad opera della Legge 161 del 4 novembre 2017, che ha introdotto il richiamo all'art. 12 del D. Lgs. 25 luglio 1998, n. 286 (recante "*Disposizioni contro le immigrazioni clandestine*"), in relazione alle condotte di procurato ingresso illecito di stranieri nel territorio dello Stato e favoreggiamento dell'immigrazione clandestina. Il novellato art. 25-*duodecies* richiama l'art. 12 del D. Lgs. 286/1998 limitatamente ai commi 3, 3-*bis*, 3-*ter* e 5 che riguardano le condotte di chi "*dirige, organizza, finanzia, effettua il trasporto di stranieri nel territorio dello Stato ovvero compie altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato*" o ne favorisce la permanenza "*al fine di trarre un ingiusto profitto dalla condizione di illegalità*".

VI.1.3 Intermediazione illecita e sfruttamento del lavoro (art. art. 25-*quinquies* del D.Lgs. 231/2001)

La presente Parte Speciale si riferisce inoltre al reato di intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.).

Il reato in oggetto dispone che, salvo che il fatto costituisca più grave reato, sia punito chiunque:

1. recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;
2. utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.

È prevista una pena più severa se i fatti sono commessi mediante violenza o minaccia.

Ai fini dell'articolo in parola, costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni: 1) 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; 2) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie; 3) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro; 4) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

Costituiscono, invece, aggravanti del reato: 1) il fatto che il numero di lavoratori reclutati sia superiore a tre; 2) il fatto che uno o più dei soggetti reclutati siano minori in età non lavorativa; 3) l'aver commesso il fatto esponendo i lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

VI.1.4 Reati ambientali (art. art. 25-*undecies* del D.Lgs. 231/2001)

Si indicano qui di seguito le fattispecie contemplate nell'art. 25-*undecies* del Decreto (di seguito i "Reati Ambientali") astrattamente rilevanti per la Società, rinvenibili nel D.Lgs. 3 aprile 2006 n. 152 recante "*Norme in materia ambientale*" e successive modificazioni e integrazioni ("**Codice dell'Ambiente**" o "**Cod. Amb.**").

ATTIVITÀ DI GESTIONE DI RIFIUTI NON AUTORIZZATA (ART. 256 COD. AMB.)

L'art. 256 è la disposizione normativa più importante nel sistema sanzionatorio in materia di gestione dei rifiuti in quanto detta una disciplina per una molteplicità di attività tutte connesse alla nozione di gestione dei rifiuti (i.e. la raccolta, il trasporto, il recupero, lo smaltimento, il deposito temporaneo, il commercio e l'intermediazione, la gestione di una discarica, la miscelazione di rifiuti) siano essi pericolosi oppure non pericolosi.

Si osserva che, quanto all'elemento soggettivo che caratterizza la condotta, la struttura contravvenzionale della fattispecie rende punibili i reati di cui al primo comma del presente articolo sia a titolo di dolo sia a titolo di colpa.

A tal fine è opportuno richiamare il rigore della giurisprudenza nell'interpretare e nell'applicare la norma, in quanto è stato ritenuto che l'intervenuta autorizzazione all'esercizio dell'attività di recupero dei rifiuti da parte di un'impresa non esclude la sua responsabilità a titolo di concorso se essa li abbia ricevuti da un intermediario o da un trasportatore che, invece, sia privo di autorizzazione, in quanto sussiste a carico del ricevente l'obbligo di controllare che coloro che forniscono i rifiuti da trattare siano muniti di regolare autorizzazione.

CAPITOLO VI.2 – LE ATTIVITÀ SENSIBILI

Le Attività Sensibili nell'ambito dei Reati in oggetto che la Società ha individuato al proprio interno sono le seguenti:

1. Adempimento degli obblighi normativi in materia di salute e sicurezza sul lavoro, che comprendono:

- determinazione delle procedure interne in tema di salute e sicurezza sul lavoro volte a definire i compiti e le responsabilità in materia di sicurezza e a garantire una corretta gestione di tutti gli adempimenti posti in capo a ciascun Destinatario così come disposti dal Decreto Sicurezza e dalla normativa primaria e secondaria ad esso collegata;
- attribuzione di responsabilità in materia di salute e sicurezza sul lavoro, con particolare riferimento a: (i) attribuzioni di compiti e doveri in capo a ciascun Destinatario; (ii) attività del Servizio Prevenzione e Protezione e del Medico Competente;
- individuazione dei pericoli all'interno della sede di Compagnia Privata e valutazione dei rischi, con particolare riferimento a: (i) stesura del Documento di Valutazione dei Rischi; (ii) valutazione dei rischi delle interferenze; (iii) gestione dei contratti di appalto;
- sensibilizzazione di tutti i soggetti che, a diversi livelli, operano nell'ambito della struttura aziendale attraverso un'adeguata attività di informazione e mediante la programmazione di piani di formazione in tema di salute e sicurezza nei luoghi di lavoro (compreso il Datore di Lavoro);
- attuazione di adeguate attività di monitoraggio, verifica e ispezione, in particolare per ciò che concerne:
 - l'aggiornamento delle misure in relazione ai mutamenti organizzativi che hanno rilevanza ai fini della salute e sicurezza sul lavoro;
 - gestione, rettifica ed inibizione dei comportamenti posti in violazione delle norme, attraverso l'eventuale irrogazione di provvedimenti disciplinari.

2. Gestione delle attività affidate in appalto

3. Gestione del personale

4. Gestione dei rifiuti

CAPITOLO VI.3 – PRINCIPI GENERALI DI COMPORTAMENTO

Obiettivo della presente Parte Speciale, al fine di prevenire la commissione dei Reati oggetto della medesima, è che tutti i Destinatari del Modello si attengano al rispetto di tutte le procedure e ai principi che siano direttamente o indirettamente funzionali alla prevenzione dei suddetti Reati.

In particolare, i Destinatari, anche in relazione al tipo di rapporto posto in essere con la Società, dovranno attenersi ai seguenti principi di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dalla presente Parte Speciale;
2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne.

In tema di **salute e sicurezza sul lavoro**, la politica della Società (laddove applicabile) e degli appaltatori deve porsi come obiettivo quello di enunciare i principi cui si ispira ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte all'interno della Società, nell'ottica della salute e sicurezza di tutti i lavoratori.

Tale politica deve prevedere:

- una chiara affermazione della responsabilità dell'intera organizzazione aziendale, nella gestione delle tematiche relative alla salute e sicurezza sul lavoro, ciascuno per le proprie attribuzioni e competenze;
- l'impegno a considerare tali tematiche come parte integrante della gestione aziendale;
- l'impegno al miglioramento continuo e alla prevenzione;
- l'impegno a fornire le risorse umane e strumentali necessarie;
- l'impegno a garantire che i destinatari del Modello, nei limiti delle rispettive attribuzioni, siano sensibilizzati a svolgere la propria attività nel rispetto delle norme sulla tutela della salute e sicurezza;
- l'impegno ad un riesame periodico della politica per la salute e sicurezza adottato al fine di garantire la sua costante adeguatezza alla struttura organizzativa della Società.

In tema di **impiego di cittadini di Paesi extra-UE** e di **tutela della personalità individuale**,

- la Società adotta presidi volti ad assicurare il rispetto degli obblighi di legge in tema di impiego di lavoratori stranieri e permesso di soggiorno;
- la Società pone il rispetto della dignità e della personalità individuale dei lavoratori al di sopra di ogni valutazione di carattere economico o di *business*.

In relazione ai reati ambientali, la politica dell'impresa in materia di contenimento dei rischi ambientali si ispira ai seguenti principi:

1. promozione tra tutti i Destinatari di un senso di responsabilità verso l'ambiente;
2. generale valutazione delle potenziali ripercussioni delle attività svolte sull'ambiente locale;
3. riduzione della produzione di rifiuti;
4. cooperazione con le autorità pubbliche competenti *ratione materiae*;
5. richiamo dei Fornitori al rispetto ambientale;
6. rispetto della normativa tempo per tempo vigente.

Inoltre, la Società:

- garantisce l'identificazione e la corretta applicazione delle prescrizioni delle leggi e dei regolamenti applicabili in tema di tutela ambientale
- sensibilizza tutti i soggetti che, a diversi livelli, operano nell'ambito della struttura aziendale al massimo rispetto dell'ambiente e della sostenibilità.

CAPITOLO E.4 – PRINCIPI SPECIFICI DI COMPORTAMENTO

Ai fini dell'attuazione delle regole elencate al precedente Capitolo, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali qui di seguito descritti per le singole Attività Sensibili. Tali principi potranno trovare attuazione anche per mezzo dell'adozione di specifiche procedure aziendali.

1. Adempimento degli obblighi normativi in materia di salute e sicurezza nei luoghi di lavoro

- Al fine di prevenire infortuni e malattie nei luoghi di lavoro, la Società:
 - adempie puntualmente alle disposizioni normative applicabili in materia di salute e sicurezza nei luoghi di lavoro;
 - identifica i vari ruoli nell'organigramma della sicurezza;
 - definisce e l'adotta adeguate misure per il controllo di situazioni di rischio in caso di emergenza;
 - identifica una squadra di emergenza costituita da un numero adeguato di lavoratori debitamente formati e con specifico addestramento in materia di antincendio, primo soccorso ed evacuazione;
 - fornisce adeguata informazione e formazione a tutti i soggetti interessati circa i rischi specifici dell'impresa, le conseguenze di questi e le misure di prevenzione e protezione adottate;
 - cura che tutti gli attori dell'organigramma prevenzionistico siano adeguatamente individuati e debitamente formati;
 - garantisce la manutenzione ordinaria e straordinaria dei dispositivi di sicurezza aziendale (ad esempio, porte tagliafuoco, lampade di emergenza, estintori, ecc.). Inoltre, sono effettuate manutenzioni ordinarie e programmate sugli ambienti, sugli impianti, sui macchinari e sulle attrezzature generiche e specifiche in conformità alle indicazioni dei costruttori;
 - provvede a conservare i documenti relativi alla gestione della salute e sicurezza nei luoghi di lavoro;
 - assicura un controllo periodico delle misure di prevenzione e protezione adottate sui luoghi di lavoro. In particolare, assicura un controllo periodico su:
 - a. le misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro e
 - b. l'adeguatezza e la funzionalità di tali misure;

- sulla base degli esiti delle attività di controllo, pianifica gli interventi necessari per eliminare le criticità rilevate: ciò al fine di assicurare che il sistema di salute e sicurezza sia adeguatamente attuato e siano raggiunti gli obiettivi prefissati;
- prevede flussi informativi periodici tra l'Organismo di Vigilanza e i soggetti coinvolti nei processi ritenuti sensibili in relazione ai reati in materia di salute e sicurezza sul lavoro.

2. Gestione delle attività affidate in appalto

- Le modalità di gestione e di coordinamento dei lavori in appalto che rientrino nel perimetro dell'art. 26 del TUSL devono essere formalizzate in contratti scritti nei quali siano presenti riferimenti agli adempimenti di cui all'art. 26, TUSL, tra questi, in capo al Datore di Lavoro:
 - verificare l'idoneità tecnico-professionale delle imprese appaltatrici in relazione ai lavori da affidare in appalto attraverso i) acquisizione del certificato di iscrizione alla camera di commercio, industria e artigianato ii) acquisizione dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei requisiti di idoneità tecnico professionale ai sensi dell'art. 4, D.P.R. 28 dicembre 2000, n. 445;
 - prevedere all'interno degli accordi contrattuali con gli appaltatori e i subappaltatori, specifica indicazione del personale dell'appaltatore-subappaltatore che svolge la funzione di preposto;
 - fornire informazioni dettagliate agli appaltatori circa gli eventuali rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
 - cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
 - coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori.
- Nei contratti di appalto deve essere chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto.
- Nei contratti di somministrazione, di appalto e di subappalto, devono essere specificamente indicati i costi relativi alla sicurezza del lavoro. La Società, in fase di selezione (e di successiva contrattualizzazione), cura che eventuali scontistiche applicate dall'appaltatore non incidano sull'impegno di spesa programmato per la tutela della salute e della sicurezza dei Lavoratori.

3. Gestione del personale

- Quanto all'impiego diretto di personale, la Società

- adotta presidi formali volti ad assicurare il rispetto degli obblighi di legge in tema di impiego di lavoratori stranieri e permesso di soggiorno;
 - non impiega lavoratori provenienti da Paesi terzi privi di permesso di soggiorno o con un permesso revocato o scaduto, del quale non sia stata presentata domanda di rinnovo, documentata dalla relativa ricevuta;
 - non impiega lavoratori provenienti da Paesi terzi soggiornanti in Italia per motivi di turismo, anche se regolarmente muniti della prescritta dichiarazione di presenza;
 - in caso di assunzione di cittadini stranieri residenti in Paesi extra-UE, si attiva presso le Autorità competenti al fine di ottenere tutta la documentazione necessaria a consentire l'ingresso legale in Italia del cittadino straniero e l'instaurazione di un rapporto di lavoro regolare;
 - in caso di assunzione di cittadini stranieri già soggiornanti in Italia, garantisce la verifica che i medesimi siano in possesso di un permesso di soggiorno regolare o che, in caso di scadenza dello stesso, i medesimi abbiano provveduto ad avviare le pratiche per il rinnovo;
 - garantisce che il rinnovo del contratto di lavoro ovvero il proseguimento del rapporto di lavoro siano subordinati al mantenimento/rinnovo del permesso di soggiorno e che, al venir meno di tale requisito, il rapporto di lavoro si sospenda fino all'avvenuta regolarizzazione della posizione;
 - assicura che, in caso di utilizzo di lavoratori con contratto di somministrazione, il rapporto con l'agenzia fornitrice sia disciplinato da accordo scritto;
 - garantisce sempre il rispetto, nei confronti dei lavoratori, di condizioni di lavoro dignitose;
 - considera la tutela dei diritti delle persone e dei lavoratori sempre prevalente rispetto a qualsiasi considerazione di natura economica.
- Quanto all'impiego di personale da parte di appaltatori, la Società prevede:
 - la garanzia da parte dell'appaltatore di impiegare nella prestazione a favore della Società lavoratori lecitamente soggiornanti in Italia e con rapporto di lavoro regolare e di aver assolto nei termini di legge tutti i dovuti adempimenti retributivi, previdenziali, assicurativi, fiscali, ecc. nei confronti degli stessi;
 - l'impegno da parte dell'appaltatore a fornire all'atto della sottoscrizione del contratto e successivamente, con periodicità stabilita dalle parti, copia del Documento Unico di Regolarità Contributiva relativo alla posizione amministrativa dell'appaltatore e dei propri subappaltatori rilasciato dalle Autorità competenti;

- l'obbligo da parte dell'appaltatore di instaurare rapporti solo con subappaltatori che garantiscano il rispetto delle disposizioni giuslavoristiche vigenti, comprese quelle relative all'assunzione di lavoratori provenienti da paesi terzi, a pena di risoluzione di diritto del contratto di appalto;
- il divieto per l'appaltatore di sub-appaltare le attività senza la preventiva autorizzazione della Società.

4. Gestione dei rifiuti

- La Società
 - adotta una classificazione dei rifiuti prodotti nell'ambito delle attività aziendali in conformità a quanto stabilito dalle disposizioni legislative vigenti e dalle Autorità competenti nonché una gestione dei rifiuti orientata alla diminuzione della produzione e al recupero degli stessi;
 - definisce i principali adempimenti da adottare in ambito aziendale in merito alla gestione delle diverse tipologie di rifiuti;
 - vigila sulla corretta gestione dei rifiuti, anche laddove affidati a terzi, segnalando eventuali irregolarità alle direzioni competenti e, in particolare,
 - ove necessario (ad esempio, con riferimento allo smaltimento di *toner* esausti o RAEE), affida le attività di raccolta, trasporto, recupero e smaltimento dei rifiuti esclusivamente a imprese autorizzate e affidabili.

* * *

CAPITOLO VI.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

Con riferimento alla presente Parte Speciale, ogni funzione coinvolta deve comunicare per quanto di competenza e con periodicità definita quanto previsto nella seguente tabella (si precisa che i flussi in oggetto, all'occorrenza, possono eventualmente essere forniti in occasione di incontri *de visu* con l'OdV):

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
<i>Compliance</i>	Segnalazione di criticità in materia di salute e sicurezza sul lavoro (ad esempio, infortuni).	Ad evento
<i>Compliance</i>	Segnalazione su criticità in relazione a eventuali contratti di appalto sottoscritti.	Ad evento
<i>Compliance</i>	Modifiche alla struttura organizzativa e modifiche al DVR (e/o altra documentazione rilevante)	Ad evento
<i>Compliance</i>	Relazioni/verbali redatti in occasione di riunioni periodiche in materia di sicurezza	Annuale
<i>Compliance</i>	Indicazioni infortuni	Annuale
<i>Compliance</i>	Piani di formazione e <i>report</i> relativi alla formazione svolta in materia di salute e sicurezza sul lavoro	Annuale
<i>Compliance</i>	Segnalazione di criticità in ambito di gestione di rifiuti o altri eventi ad impatto ambientale	Ad evento



PARTE SPECIALE – VII – Delitti informatici e delitti in violazione del diritto d'autore

CAPITOLO VII.1 - LE FATTISPECIE DI REATO

La presente Parte Speciale si riferisce ai Delitti Informatici e ai Delitti in Violazione del Diritto d'Autore introdotti nel *corpus* del Decreto 231 rispettivamente all'art. 24 *bis* e all'art. 25 *novies*.

A tal riguardo si sottolinea che, nonostante le due tipologie di Reato tutelino interessi giuridici differenti, si è ritenuto opportuno procedere alla predisposizione di un'unica Parte Speciale in quanto:

- entrambe le fattispecie di reato presuppongono, tra l'altro, un corretto utilizzo delle risorse informatiche;
- le attività sensibili potenzialmente interessate dalle due tipologie di reato in commento risultano, in virtù di tale circostanza, in parte sovrapponibili;
- i principi specifici di comportamento mirano, in entrambi i casi, a garantire tra l'altro la sensibilizzazione dei Destinatari in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

VII.1.1 I delitti informatici

FALSITÀ IN DOCUMENTI INFORMATICI (ART. 491-BIS C.P.)

L'articolo in oggetto stabilisce che tutti i delitti relativi alla falsità in atti, tra i quali rientrano sia le falsità ideologiche che le falsità materiali in atti pubblici sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico.

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali.

Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, comma 1, lett. p), D.Lgs. 82/2005, salvo modifiche ed integrazioni).

A titolo esemplificativo, integrano il delitto di falsità in documenti informatici la condotta di inserimento fraudolento di dati falsi nelle banche dati pubbliche oppure la condotta dell'addetto alla gestione degli archivi informatici che proceda, deliberatamente, alla modifica di dati in modo da falsificarli.

Inoltre, il delitto potrebbe essere integrato tramite la cancellazione o l'alterazione di informazioni a valenza probatoria presenti sui sistemi dell'ente, allo scopo di eliminare le prove di un altro reato.

ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (ART. 615-TER C.P.)

Tale reato si realizza quando un soggetto "*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 diritto ad escluderlo*".

La pena è aumentata:

- 1) 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;

- 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
- 3) 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.

La pena è aumentata anche qualora il delitto in oggetto riguardi 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.

Il delitto di accesso abusivo al sistema informatico rientra tra i delitti contro la libertà individuale. Il bene che viene protetto dalla norma è il domicilio informatico seppur vi sia chi sostiene che il bene tutelato è, invece, l'integrità dei dati e dei programmi contenuti nel sistema informatico. L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema.

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

Il delitto di accesso abusivo a sistema informatico si integra, ad esempio, nel caso in cui un soggetto accede abusivamente ad un sistema informatico e procede alla stampa di un documento contenuto nell'archivio del PC altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura).

Il delitto potrebbe essere astrattamente commesso da parte di qualunque dipendente della Società accedendo abusivamente ai sistemi informatici di proprietà di terzi (*outsider hacking*), ad esempio, per prendere cognizione di dati riservati di un'impresa concorrente, ovvero tramite la manipolazione di dati presenti sui propri sistemi come risultato dei processi di business allo scopo di produrre un bilancio falso o, infine, mediante l'accesso abusivo a sistemi aziendali protetti da misure di sicurezza, da parte di utenti dei sistemi stessi, per attivare servizi non richiesti dalla Clientela.

DETENZIONE E DIFFUSIONE ABUSIVA DI APPARECCHIATURE, CODICI E ALTRI MEZZI ATTENTI ALL'ACCESSO A SISTEMI INFORMATICI O TELEMATICI (ART. 615-QUATER C.P.)

Tale reato si realizza quando un soggetto, *"al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, 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 di un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo"*.

Il legislatore ha introdotto questo reato al fine di prevenire le ipotesi di accessi abusivi a sistemi informatici. Per mezzo dell'art. 615-*quater* c.p., pertanto, sono punite le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.

I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, *password* o schede informatiche (ad esempio, *badge*, carte di credito, bancomat e *smart card*).

Questo delitto si integra sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi. La condotta è abusiva nel caso in cui i codici di accesso siano ottenuti a seguito della violazione di una norma, ovvero di una clausola contrattuale, che vieti detta condotta (ad esempio, *policy* Internet).

L'art. 615-*quater*, inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

Risponde, ad esempio, del delitto di diffusione abusiva di codici di accesso, il dipendente della Società autorizzato ad un certo livello di accesso al sistema informatico che ottenga illecitamente il livello di accesso superiore, procurandosi codici o altri strumenti di accesso mediante lo sfruttamento della propria posizione all'interno della Società oppure carisca in altro modo fraudolento o ingannevole il codice di accesso.

INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-QUATER C.P.)

Tale ipotesi di reato si integra qualora un soggetto fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisce o interrompe tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione al pubblico.

La norma tutela la libertà e la riservatezza delle comunicazioni informatiche o telematiche durante la fase di trasmissione al fine di garantire l'autenticità dei contenuti e la riservatezza degli stessi.

La fraudolenza consiste nella modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione.

Perché possa realizzarsi questo delitto è necessario che la comunicazione sia attuale, vale a dire in corso, nonché personale ossia diretta ad un numero di soggetti determinati o determinabili (siano essi persone fisiche o giuridiche). Nel caso in cui la comunicazione sia rivolta ad un numero indeterminato di soggetti la stessa sarà considerata come rivolta al pubblico.

Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

Il reato si integra, ad esempio, con il vantaggio concreto dell'ente, nel caso in cui un dipendente esegua attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazioni di un concorrente.

DETENZIONE, DIFFUSIONE E INSTALLAZIONE ABUSIVA DI APPARECCHIATURE E DI ALTRI MEZZI ATTI A INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-QUINQUIES C.P.)

Questa fattispecie di reato si realizza quando qualcuno, "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 a intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi".

La condotta vietata dall'art. 617-*quinqies* è, pertanto, costituita dalla detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi, a prescindere dalla circostanza che le stesse siano o meno utilizzate. Si tratta di un reato che mira a prevenire quello precedente di intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche.

Anche la semplice installazione di apparecchiature idonee all'intercettazione viene punita dato che tale condotta rende probabile la commissione del reato di intercettazione. Ai fini della condanna il giudice dovrà, però, limitarsi ad accertare se l'apparecchiatura installata abbia, obiettivamente, una potenzialità lesiva.

Qualora all'installazione faccia seguito anche l'utilizzo delle apparecchiature per l'intercettazione, interruzione, impedimento o rivelazione delle comunicazioni, si applicheranno nei confronti del soggetto agente, qualora ricorrano i presupposti, più fattispecie criminose.

Il reato si integra, ad esempio, a vantaggio dell'ente, nel caso in cui un dipendente, direttamente o mediante conferimento di incarico ad un investigatore privato (se privo delle necessarie autorizzazioni) si introduca fraudolentemente presso la sede di un concorrente o di un Cliente insolvente al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche.

ESTORSIONE INFORMATICA (ART. 629, COMMA 3, C.P.)

Il reato di "estorsione informatica" punisce chiunque, mediante le condotte di cui agli articoli 615-*ter*, 617-*quater*, 617-*sexies*, 635-*bis*, 635-*quater* e 635-*quinqies* c.p. ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (ART. 635-BIS C.P.)

Tale fattispecie reato si realizza quando un soggetto "*distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui*".

La pena aumentata se il fatto è commesso con violenza alla persona o con minaccia o se è commesso abusando della qualità di operatore del sistema.

Il reato, ad esempio, si integra nel caso in cui il soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.

Il danneggiamento potrebbe essere commesso a vantaggio dell'ente laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte del fornitore dell'ente o al fine di contestare il corretto adempimento delle obbligazioni da parte del fornitore.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI PUBBLICI O DI INTERESSE PUBBLICO (ART. 635-TER C.P.)

Tale reato si realizza quando un soggetto *“commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici 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 nelle seguenti ipotesi:

- 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di 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;
- 2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;
- 3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.

Questo delitto si distingue da quello dianzi analizzato poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati alla soddisfazione di un interesse di natura pubblica.

Perché il reato si integri è sufficiente che si tenga una condotta finalizzata al deterioramento o alla soppressione del dato.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (ART. 635-QUATER C.P.)

Questo reato si realizza quando un soggetto *“mediante le condotte di cui all'art. 635-bis (danneggiamento di dati, informazioni e programmi informatici), 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”*.

La pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema.

Si tenga conto che qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635-*bis*.

Il reato si integra in caso di danneggiamento o cancellazione dei dati o dei programmi contenuti nel sistema, effettuati direttamente o indirettamente (per esempio, attraverso l'inserimento nel sistema di un *virus*).

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICO INTERESSE (ART. 635-QUINQUIES C.P.)

Questo reato si configura nei confronti di chiunque "mediante le condotte di cui *all'art. 635-quater (Danneggiamento di sistemi informatici o telematici)* ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, compie atti diretti a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento".

La pena è aumentata nelle seguenti ipotesi:

- a) 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;
- b) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;
- c) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblico interesse, diversamente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità (art. 635-*ter*), quel che rileva è che il sistema sia utilizzato per il perseguimento di pubblico interesse indipendentemente dalla proprietà privata o pubblica del sistema stesso.

Il reato si può configurare nel caso in cui un Dipendente cancelli file o dati, relativi ad un'area per cui sia stato abilitato ad operare, per conseguire vantaggi interni (ad esempio, far venire meno la prova del credito da parte di un ente o di un fornitore) ovvero che l'amministratore di sistema, abusando della sua qualità, ponga in essere i comportamenti illeciti in oggetto per le medesime finalità già descritte.

VII.1.2 I delitti in violazione del diritto d'autore

La Legge 23 luglio 2009, n. 99, introducendo nell'ambito del Decreto 231 l'art 25-*novies* concernente i "delitti in materia di violazione del diritto d'autore", ha esteso la responsabilità amministrativa degli enti anche ai reati di cui alla Legge 22 aprile 1941, n. 633 relativa alla protezione del diritto d'autore e di altri diritti connessi al suo esercizio (di seguito "*Legge sul Diritto d'Autore*").

Si provvede a descrivere qui di seguito le fattispecie di reato punibili ai sensi dell'art. 25-novies del Decreto 231 e ritenute, a seguito dell'analisi dei rischi e suggerimenti, applicabili alla Società.

DIVULGAZIONE TRAMITE RETI TELEMATICHE DI UN'OPERA DELL'INGEGNO PROTETTA (ART. 171 COMMA 1 LETT. A-BIS E COMMA 3. LEGGE SUL DIRITTO D'AUTORE)

In relazione alla fattispecie delittuosa di cui all'art. 171 della Legge sul Diritto d'Autore, il Decreto ha preso in considerazione esclusivamente due fattispecie, ovvero:

- (i) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa;
- (ii) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore o alla reputazione dell'autore.

Se dunque nella prima ipotesi ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere lese le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete, nella seconda ipotesi il bene giuridico protetto non è, evidentemente, l'aspettativa di guadagno del titolare dell'opera, ma il suo onore e la sua reputazione.

Tale reato potrebbe ad esempio essere commesso nell'interesse della Società qualora venissero caricati sulla rete aziendale dei contenuti coperti dal diritto d'autore affinché gli stessi potessero essere utilizzati nell'ambito dell'attività lavorativa.

DUPLICAZIONE, A FINI DI LUCRO, DI PROGRAMMI INFORMATICI O IMPORTAZIONE, DISTRIBUZIONE, VENDITA, DETENZIONE PER FINI COMMERCIALI DI PROGRAMMI CONTENUTI IN SUPPORTI NON CONTRASSEGNA TI DALLA SIAE (ART. 171-BIS LEGGE SUL DIRITTO D'AUTORE)

La norma in esame è volta a tutelare il corretto utilizzo dei *software* e delle banche dati.

Per ciò che concerne i *software*, è prevista la rilevanza penale dell'abusiva duplicazione nonché dell'importazione, distribuzione, vendita e detenzione a scopo commerciale o imprenditoriale e locazione di programmi "pirata".

Il reato in ipotesi si configura nel caso in cui chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla SIAE o da altri organismi di gestione collettiva o da entità di gestione indipendenti.

Il fatto è punito anche se la condotta ha ad oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

Il secondo comma della stessa norma punisce inoltre chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE o da altri organismi di gestione collettiva o da entità di gestione indipendenti,



riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui alla Legge sul Diritto d'Autore.

Sul piano soggettivo, per la configurabilità del reato è sufficiente lo scopo di lucro, sicché assumono rilevanza penale anche tutti quei comportamenti che non sono sorretti dallo specifico scopo di conseguire un guadagno di tipo prettamente economico (come nell'ipotesi dello scopo di profitto).

Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora venissero utilizzati, per scopi lavorativi, programmi non originali ai fine di risparmiare il costo derivante dalla licenza per l'utilizzo di un *software* originale.

CAPITOLO VII.2 – LE ATTIVITÀ SENSIBILI IN RELAZIONE AI DELITTI INFORMATICI E IN VIOLAZIONE DEL DIRITTO D'AUTORE

Le Attività Sensibili che la Società ha individuato al proprio interno in relazione ai Reati in oggetto sono le seguenti:

- 1. Gestione e utilizzo dei sistemi informatici e del patrimonio informativo aziendale**
- 2. Utilizzo di contenuti coperti dal diritto d'autore**

CAPITOLO VII.3 – PRINCIPI GENERALI DI COMPORTAMENTO

Obiettivo della presente Parte Speciale è che tutti i Destinatari del Modello si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire e impedire il verificarsi dei Reati Informatici e dei Delitti commessi in violazione del diritto d'autore.

Nell'espletamento delle attività aziendali e, in particolare, nelle Attività Sensibili, è espressamente vietato ai soggetti sopra indicati, anche in relazione al tipo di rapporto posto in essere con la Società, porre in essere, collaborare o dare causa alla realizzazione di comportamenti, anche omissivi, tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente Parte Speciale.

Compagnia Privata assicura la tracciabilità degli strumenti informatici assegnati ai propri dipendenti e la preventiva verifica delle caratteristiche tecniche, delle configurazioni e degli accessi alla rete aziendale.

L'utilizzo dei sistemi informatici da parte dei soggetti assegnatari deve essere conforme alla normativa aziendale interna e alle prescrizioni normative vigenti di riferimento.

Compagnia Privata assicura il corretto impiego e la regolare funzionalità della posta elettronica e della rete internet definendo le modalità d'uso consentite nello svolgimento dell'attività lavorativa.

Si precisa che i dati, le informazioni e i documenti dei quali si viene a conoscenza nello svolgimento delle proprie mansioni, devono essere utilizzati esclusivamente per motivi di ufficio e gestiti nel rispetto delle politiche e delle procedure aziendali, nonché delle deleghe e procure, volte ad assicurare un'adeguata gestione e protezione degli stessi.

In particolare, non è ammesso:

- porre in essere quei comportamenti che (i) integrano le fattispecie di reato o, (ii) sebbene non costituiscano di per sé un'ipotesi di reato, possano esserne il presupposto (ad esempio, mancato controllo);
- divulgare informazioni relative ai sistemi informatici aziendali che possano rivelare carenze e/o modalità di utilizzo distorte e non consentite degli stessi;
- utilizzare i sistemi informatici della Società per finalità non connesse alla mansione svolta;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di terze parti, comprensivo di archivi, dati e programmi;
- lasciare il proprio *Personal Computer* sbloccato e incustodito;
- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale;

- detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato;
- duplicare abusivamente programmi/software per i *Personal Computer*;
- detenere programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE);
- mettere a disposizione di terzi, riprodurre, divulgare, trasmettere o diffondere, in tutto o in parte, opere dell'ingegno tutelate dal diritto d'autore;
- installare sui sistemi informativi di Compagnia Privata programmi per elaboratore non assistiti da valida licenza d'utilizzo;
- installare sui sistemi informatici di Compagnia Privata *software* mediante i quali sia possibile scambiare con altri soggetti all'interno della rete internet ogni tipologia di *file*, quali filmati, documenti, canzoni, opere letterarie
- utilizzare illecitamente materiale tutelato da altrui diritto d'autore
- utilizzare opere dell'ingegno senza l'autorizzazione del soggetto che legittimamente ne detiene i diritti, ovvero senza aver stipulato un valido contratto di licenza.

I Destinatari devono

- utilizzare esclusivamente i *software*, le applicazioni e le apparecchiature informatiche fornite da Compagnia Privata e farlo per finalità strettamente attinenti allo svolgimento delle proprie mansioni;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendale per la protezione e il controllo dei sistemi informatici ed ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio informativo di Compagnia Privata;
- custodire le *password* di accesso alla rete aziendale ed alle diverse applicazioni e le chiavi personali secondo criteri idonei a impedirne una facile individuazione ed un uso improprio.

CAPITOLO VII.4 – PRINCIPI SPECIFICI DI COMPORTAMENTO

Ai fini dell'attuazione delle regole elencate al precedente Capitolo, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali qui di seguito descritti per le singole Attività Sensibili. Tali principi potranno trovare attuazione anche per mezzo dell'adozione di specifiche procedure aziendali.

1. Gestione e utilizzo dei sistemi informatici e del patrimonio informativo aziendale

- È fatto divieto di collegare al sistema informatico aziendale computer, periferiche, altre apparecchiature o *software* senza preventiva autorizzazione del soggetto responsabile individuato;
- è vietato acquisire, possedere o utilizzare strumenti *software* e/o *hardware* che potrebbero essere adoperati per compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le *password*, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.);
- è vietato ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla Società;
- è vietato divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- è vietato accedere ad un sistema informatico altrui (anche di un collega) e manomettere ed alterarne i dati ivi contenuti;
- è vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici, a meno che non sia esplicitamente previsto nei propri compiti lavorativi;
- è vietato tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei propri compiti lavorativi;
- è vietato modificare in qualsiasi modo la configurazione delle postazioni di lavoro fisse o mobili assegnate dalla Società;
- è vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- è vietato comunicare a persone non autorizzate, interne o esterne alla Società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;

- è proibito distorcere, oscurare sostituire la propria identità e inviare *e-mail* riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati;
- la Società si impegna, a sua volta, a porre in essere i seguenti adempimenti:
 - i. fare sottoscrivere al personale uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo delle risorse informatiche aziendali;
 - ii. diffidare il personale dall'utilizzare il PC aziendale per uso personale;
 - iii. informare il personale e gli altri soggetti eventualmente autorizzati della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;
 - iv. impostare i sistemi informatici in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;
 - v. fornire un accesso da e verso l'esterno (connessione alla rete internet) esclusivamente ai sistemi informatici del personale o di eventuali soggetti terzi che ne abbiano la necessità ai fini lavorativi o connessi all'amministrazione societaria;
 - vi. limitare gli accessi al *server* unicamente al personale autorizzato;
 - vii. proteggere, per quanto possibile, ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi *hardware* in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;
 - viii. fornire ogni sistema informatico di adeguato *software firewall* e antivirus e far sì, ove possibile, che questi non possano venir disattivati;
 - ix. impedire l'installazione e l'utilizzo di *software* non approvati dalla Società e non correlati con l'attività professionale espletata per la stessa;
 - x. limitare l'accesso alle aree ed ai siti internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di virus capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e file);
 - xi. impedire l'installazione e l'utilizzo, sui sistemi informatici della Società, di *software* (cosiddetti "P2P", di *files sharing* o di *istant messaging*) mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di file (quali filmati, documenti, canzoni, virus, ecc.) senza alcuna possibilità di controllo da parte della Società;
 - xii. qualora per la connessione alla rete internet si utilizzino collegamenti *wireless*, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti

terzi, esterni alla Società, possano illecitamente collegarsi alla rete Internet tramite i *routers* della stessa e compiere illeciti;

- xiii. prevedere un procedimento di autenticazione mediante *username* e password al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ogni risorsa della Società e per gli altri soggetti eventualmente autorizzati;
- xiv. informare adeguatamente il personale e gli altri soggetti eventualmente autorizzati dell'importanza di mantenere i propri codici di accesso (*username* e password) confidenziali e di non divulgare gli stessi a soggetti terzi;
- xv. informare tempestivamente i responsabili del sistema informatico dell'avvio e della cessazione di rapporti di lavoro del personale al fine di attivare il processo di rilascio, modifica e revoca delle abilitazioni;
- xvi. limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno del personale e degli altri soggetti eventualmente autorizzati.

L'applicazione dei principi sopra elencati è garantita dal sistema dei controlli adottato dalla Società.

Tale sistema di controlli prevede:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica dei processi sopra descritti. In particolare:
 - la gestione delle abilitazioni avviene tramite la definizione di "profili di accesso" in ragione delle funzioni svolte all'interno della SIM;
 - le variazioni al contenuto dei profili sono eseguite dal soggetto a ciò delegato su richiesta del Responsabile delle strutture interessate.
- Segregazione dei compiti. Sono assegnati distinti ruoli e responsabilità di gestione della sicurezza delle informazioni; in particolare:
 - sono attribuite precise responsabilità per la gestione degli aspetti di sicurezza alle funzioni organizzative che sviluppano e gestiscono sistemi informativi;
 - sono definite le responsabilità ed i meccanismi atti a garantire la gestione di eventi di sicurezza anomali e di situazioni di emergenza e crisi;
 - le attività di implementazione e modifica dei *software*, gestione delle procedure informatiche, controllo degli accessi fisici, logici e della sicurezza del software sono organizzativamente demandate a strutture differenti rispetto agli utenti, a garanzia della corretta gestione e del presidio continuativo sul processo di gestione e utilizzo dei sistemi informativi;

- sono attribuite precise responsabilità per garantire che il processo di sviluppo e manutenzione delle applicazioni, effettuato internamente o presso terzi, sia gestito in modo controllato e verificabile attraverso un opportuno iter autorizzativo.
- Attività di controllo: le attività di gestione e utilizzo dei sistemi informativi e del Patrimonio Informativo di Compagnia Privata sono soggette ad una costante attività di controllo che si esplica sia attraverso l'utilizzo di adeguate misure per la protezione delle informazioni, salvaguardandone la riservatezza, l'integrità e la disponibilità con particolare riferimento al trattamento dei dati personali, sia tramite l'adozione, per l'insieme dei processi aziendali, di un piano di *Business Continuity* che prevede specifiche soluzioni di continuità operativa atte a garantire la continuità anche a fronte di situazioni di emergenza.
- Con riferimento alla sicurezza fisica:
 - protezione e controllo delle aree fisiche (perimetri/zone riservate) in modo da scongiurare accessi non autorizzati, alterazione o sottrazione degli asset informativi.
- Con riferimento alla sicurezza logica:
 - identificazione e autenticazione dei codici identificativi utenti;
 - autorizzazione all'accesso a informazioni o specifiche risorse del sistema (così come previsto anche dal Regolamento UE 2016/679)
- Con riferimento all'esercizio ed alla gestione di applicazioni, sistemi e reti:
 - pianificazione e gestione dei salvataggi di sistemi operativi, software, dati e delle configurazioni di sistema;
 - monitoraggio delle applicazioni e dei sistemi, al fine di consentire l'individuazione e la prevenzione di azioni non conformi;
 - gestione delle apparecchiature e dei supporti di memorizzazione per garantire nel tempo la loro integrità e disponibilità, al fine di proteggerli da danneggiamenti, furti o accessi non autorizzati;
 - prevenzione da software dannoso tramite sia l'utilizzo di sistemi antivirus;
 - adozione di opportune contromisure per rendere sicura la rete di telecomunicazione e gli apparati
 - a supporto e garantire la corretta e sicura circolazione delle informazioni;
- previsione di specifiche procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme alle disposizioni di legge e contrattuali.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:

- l'attività di gestione e utilizzo di sistemi informatici, è garantita dalla completa tracciabilità a sistema;
- tutti gli eventi e le attività effettuate (tra le quali gli accessi alle informazioni, le operazioni correttive effettuate tramite sistema, ad esempio rettifiche contabili, variazioni dei profili utente, ecc.), risultano tracciate attraverso sistematica registrazione (sistema di log files).
- Le Strutture di Compagnia Privata, a qualsiasi titolo coinvolte nelle attività di gestione e utilizzo di sistemi informatici e del Patrimonio Informativo aziendale sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.
- In particolare:
 - i soggetti coinvolti nel processo devono essere appositamente incaricati;
 - ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate (es. personal computer fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività.
 - i contratti con soggetti terzi/outsourcer coinvolti nella gestione dei sistemi informatici e del Patrimonio Informativo aziendale nonché nell'interconnessione/utilizzo dei software della Pubblica Amministrazione o delle Autorità di Vigilanza, contengono apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. n. 231/2001 e di impegno al suo rispetto (Clausola 231).

2. Utilizzo di contenuti coperti dal diritto d'autore

1. La Società effettua periodicamente controlli (tramite funzioni a ciò preposte) al fine di verificare che non vi sia l'utilizzo di un numero di licenze superiori rispetto a quelle concordate con gli eventuali fornitori dei relativi *software*.
2. La funzione *Compliance* effettua controlli preliminari sui materiali pubblicitari suggerendo eventuali correzioni.
3. la Società verifica periodicamente la corrispondenza tra le eventuali banche dati in uso e il numero delle licenze ottenute per il relativo utilizzo;
4. la Società garantisce l'effettuazione di attività di formazione del personale in relazione all'Attività Sensibile in oggetto, anche al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali.



* * *

Per ogni aspetto di maggiore dettaglio riferibile – anche indirettamente – alle Attività Sensibili sopra indicate e, in generale, alla prevenzione del rischio di commissione di Reati Presupposto astrattamente rilevanti in relazione alla presente Parte Speciale, si rimanda anche espressamente al contenuto dei seguenti documenti normativi interni:

- *policy* di gestione delle risorse umane;
- *policy* delle funzioni esternalizzate;
- *Policy* delle funzioni esternalizzate e in *Cloud*;
- *policy* gestione sistema informatico.

**CAPITOLO VII.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA**

Con riferimento alla presente Parte Speciale, ogni funzione coinvolta deve comunicare per quanto di competenza e con periodicità definita quanto previsto nella seguente tabella (si precisa che i flussi in oggetto, all'occorrenza, possono eventualmente essere forniti in occasione di incontri *de visu* con l'OdV):

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
<i>Compliance</i>	Eventuali anomalie riscontrate con riferimento al puntuale rispetto della normativa aziendale interna adottata in relazione alla gestione dei sistemi informatici e del patrimonio informativo aziendale	Annuale (se presenti)
<i>Compliance</i>	Segnalazione di eventuali <i>data breach</i> o, comunque, attacchi <i>hacker</i> , <i>ransomware</i> , ecc.	Ad evento
<i>Compliance</i>	Eventuali contenziosi legali avviati da terzi in materia di violazione del diritto di autore da parte di Compagnia Privata	Ad evento
<i>Compliance</i>	Eventuali contestazioni promosse da concorrenti in merito ai messaggi promozionali veicolati (ad es. relativamente all'utilizzo di nomi e marchi, a claim funzionali, ecc.).	Ad evento



PARTE SPECIALE – VIII – Reati tributari

CAPITOLO VIII.1 - LE FATTISPECIE DI REATO

Il Decreto Legge 26 ottobre 2019, n. 124 recante “*Disposizioni urgenti in materia fiscale e per esigenze indifferibili*”, convertito con modificazioni dalla Legge 19 dicembre 2019, n. 157 (entrata in vigore il 25 dicembre 2019) ha introdotto nel D.Lgs. 231/2001 l’art. 25-*quiquiesdecies* (“**Reati tributari**”).

Al fine di assicurare una corretta comprensione della presente Parte Speciale da parte di tutti i Destinatari del presente Modello, vengono di seguito descritte le fattispecie previste dal D.Lgs. 5 novembre 2024, n. 173 (e in precedenza dal D. Lgs. 10 marzo 2000, n. 74⁴) che assumono rilevanza in relazione all’attività svolta dalla Società.

DICHIARAZIONE FRAUDOLENTA MEDIANTE USO DI FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 74 D.LGS. 173/2024, GIÀ 2 D.LGS. 74/2000)

Il reato in oggetto è commesso da chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indichi in una delle dichiarazioni relative a dette imposte elementi passivi fittizi. Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell’amministrazione finanziaria. È prevista una pena più mite se l’ammontare degli elementi passivi fittizi è inferiore a Euro centomila.

DICHIARAZIONE FRAUDOLENTA MEDIANTE ALTRI ARTIFICI (ART. 75 D.LGS. 173/2024, GIÀ ART. 3 D.LGS. 74/2000)

Fuori dai casi previsti dall’articolo precedente, il reato in oggetto è commesso da chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l’accertamento e ad indurre in errore l’amministrazione finanziaria, indichi in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente: a) l’imposta evasa è superiore, con riferimento a taluna delle singole imposte, a Euro trentamila; b) l’ammontare complessivo degli elementi attivi sottratti all’imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell’ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a Euro unmilioneacinquecentomila, ovvero

⁴ Si precisa che il D.Lgs. 5 novembre 2024, n. 173, recante il “*Testo unico delle sanzioni tributarie amministrative e penali*” raccoglie le disposizioni penali in materia tributaria e la disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto. In particolare, nella seconda parte del Testo Unico, è stato recepito (a far data dal 1° gennaio 2026) il testo del D.Lgs. 10 marzo 2000, n. 74, dedicato ai reati tributari.



qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a Euro trentamila. Anche per tale fattispecie, è previsto che il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria. Non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

EMISSIONE DI FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 79 D.LGS. 173/2024, GIÀ ART. 8 D.LGS. 74/2000)

Il reato in oggetto è commesso da chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emetta o rilasci fatture o altri documenti per operazioni inesistenti. Al comma 2, viene precisato che l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato. È prevista una pena più mite se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a Euro centomila.

OCCULTAMENTO O DISTRUZIONE DI DOCUMENTI CONTABILI (ART. 81 D.LGS. 173/2024, GIÀ ART. 10 D.LGS. 74/2000)

Il reato in oggetto è commesso da chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulti o distrugga, in tutto o in parte, le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

SOTTRAZIONE FRAUDOLENTA AL PAGAMENTO DI IMPOSTE (ART. 85 D.LGS. 173/2024, GIÀ ART. 11 D.LGS. 74/2000)

La fattispecie prevista al primo comma dell'articolo in oggetto è commessa da chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore a Euro cinquantamila, alieni simulatamente o compia altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. È prevista una pena più severa se l'ammontare delle imposte, sanzioni ed interessi è superiore a Euro duecentomila. La fattispecie prevista al secondo comma è commessa da chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indichi nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo



o elementi passivi fittizi per un ammontare complessivo superiore ad Euro cinquantamila. È prevista una pena più severa se l'ammontare delle imposte, sanzioni ed interessi è superiore a Euro duecentomila.

L'art. 25-*quinqüesdecies* del D. Lgs. 231/2001 è poi stato integrato dal D.Lgs. 14 luglio 2020, n. 75. In particolare, tale ultimo decreto ha aggiunto all'art. 25-*quinqüesdecies* un nuovo comma 1-*bis* (poi modificato dal D.Lgs. 4 ottobre 2022, n. 156), ai sensi del quale viene previsto il richiamo ai reati di dichiarazione infedele, di omessa dichiarazione e di indebita compensazione, che acquisiscono rilevanza, ai fini della responsabilità amministrativa degli enti, laddove siano commessi 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 dieci milioni di euro.

Nonostante sulla base dell'analisi dei rischi condotta, la configurabilità di tali condizioni sia apparsa prettamente astratta e remota, la presente Parte Speciale prevede principi valevoli anche quale presidio del rischio di commissione di dette fattispecie.



CAPITOLO VIII.2 – LE ATTIVITÀ SENSIBILI NELL’AMBITO DEI REATI TRIBUTARI

Le Attività Sensibili nell’ambito dei reati in oggetto che la Società ha individuato al proprio interno sono le seguenti:

- 1. Gestione della contabilità e degli adempimenti fiscali**
- 2. Gestione delle operazioni straordinarie**
- 3. Gestione dei rimborsi spese**
- 4. Selezione di Fornitori, Consulenti e *Partner* e gestione dei relativi rapporti**
- 5. Gestione dei rapporti con l’Amministrazione Fiscale**

CAPITOLO VIII.3 – PRINCIPI GENERALI DI COMPORTAMENTO

Obiettivo della presente Parte Speciale, al fine di prevenire la commissione dei Reati nella stessa considerati, è che tutti i Destinatari del Modello si attengano al rispetto di tutte le procedure e ai principi che siano direttamente o indirettamente funzionali alla prevenzione di condotte idonee a integrare i reati tributari sopra richiamati.

I Destinatari dovranno attenersi ai seguenti principi di condotta:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le Attività Sensibili individuate nella presente Parte Speciale;
2. agevolare il monitoraggio del rispetto dei principi che regolano la compilazione, tenuta e conservazione delle dichiarazioni di natura contabile rilevanti ai fini fiscali;
3. conservare in modo adeguato le scritture contabili e gli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali;
4. attuare la cosiddetta “segregazione dei ruoli” nella gestione delle contabilità aziendale e nel processo di predisposizione delle dichiarazioni fiscali;
5. garantire la massima correttezza nell’ambito dei rapporti con l’amministrazione fiscale e la massima trasparenza nella comunicazione di dati e informazioni alla stessa.

Ai Destinatari è, altresì, fatto divieto di:

- emettere fatture o altri documenti contabili relativi ad operazioni in tutto o in parte inesistenti;
- emettere fatture o altri documenti contabili per corrispettivi superiori agli importi reali;
- effettuare pagamenti a fronte dell’emissione di fatture relative ad attività non ricevute;
- indicare nelle dichiarazioni fiscali elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi ovvero una base imponibile in misura inferiore a quella effettiva (ad esempio costi fittiziamente sostenuti e/o ricavi indicati in misura inferiore a quella reale) facendo leva su una falsa rappresentazione nelle scritture contabili obbligatorie e/o avvalendosi di mezzi idonei ad ostacolarne l’accertamento;
- far decorrere inutilmente i termini previsti dalla normativa applicabile per la presentazione delle dichiarazioni annuali relative alle imposte sui redditi e sul valore aggiunto così come per il successivo versamento delle imposte da esse risultanti;



- utilizzare in compensazione, all'atto del versamento di somme dovute a titolo di imposte o contributi, crediti non effettivamente esistenti e spettanti;
- occultare o distruggere scritture o documenti contabili la cui tenuta è obbligatoria per legge, in modo da impedire la ricostruzione dei redditi;
- compiere operazioni simulate oggettivamente o soggettivamente nonché avvalersi di documenti falsi o di altri mezzi fraudolenti idonei a ostacolare l'accertamento e a indurre in errore l'Amministrazione Finanziaria;
- alienare simulatamente o compiere altri atti fraudolenti sui propri o su altrui beni in modo da rendere in tutto o in parte inefficace la procedura di riscossione coattiva da parte dell'amministrazione finanziaria, con il fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte;
- effettuare pagamenti senza essere investiti dei necessari poteri di spesa ovvero concludere contratti senza essere muniti di formali poteri di firma;
- accettare pagamenti in contanti da parte di terzi (es. clienti, *Partner*) al di fuori dei casi ammessi dalle procedure aziendali e dalla normativa applicabile;
- effettuare pagamenti in contanti se non per spese di modico valore e nel rispetto delle procedure aziendali, delle deleghe di potere e della normativa applicabile;
- rimborsare le spese sostenute dal personale della Società in caso di mancata presentazione dei giustificativi di spesa;
- effettuare prestazioni (es. cessione di beni) e/o pagamenti in favore di terzi (es. clienti, partner commerciali, consulenti, ecc.) che non trovino adeguata giustificazione nel contesto del rapporto intercorrente con gli stessi;
- richiedere l'apertura di conti corrente ovvero compiere operazioni sui conti senza l'autorizzazione della funzione aziendale competente e munita dei necessari poteri;
- effettuare operazioni relative al ciclo attivo o passivo in violazione delle istruzioni, procedure e *policy* aziendali che prescrivono l'utilizzo di sistemi per il monitoraggio e la tracciabilità delle transazioni;
- nel caso in cui sia instaurata una procedura di transazione fiscale, indicare nella documentazione presentata ai fini della procedura elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi, con il fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori.

CAPITOLO VIII.4 - PRINCIPI SPECIFICI DI COMPORTAMENTO

Ai fini dell'attuazione delle regole elencate al precedente Capitolo, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, i principi procedurali qui di seguito descritti per le singole Attività Sensibili. Tali principi potranno trovare attuazione anche per mezzo dell'adozione di specifiche procedure aziendali.

1. Gestione della contabilità e degli adempimenti fiscali

- I livelli autorizzativi, le deleghe e le procure garantiscono l'attribuzione di precise responsabilità e la segregazione delle attività affinché non vi sia identità soggettiva fra coloro che assumono e autorizzano le decisioni, chi le attua, chi deve darne evidenza (anche sotto il profilo contabile) e coloro che sono tenuti a svolgere su dette attività i controlli previsti dalla legge e dalle procedure aziendali.
- Tutte le fasi di formazione e autorizzazione devono essere sempre adeguatamente documentate, tracciabili e ricostruibili. In particolare, i documenti riguardanti la formazione delle decisioni e l'attuazione delle stesse devono essere archiviati e conservati a cura della funzione aziendale competente ed essere accessibili alle persone autorizzate in base alle procedure aziendali, nonché, in ogni caso, al Consiglio di Amministrazione, al Collegio Sindacale e all'OdV.
- La Società assicura la prevenzione delle rischi potenzialmente connesse a tali Attività Sensibili, attraverso:
 - il controllo della corrispondenza degli importi indicati nelle fatture (attive e passive) o negli altri documenti rilevanti con quanto previsto contrattualmente;
 - il controllo circa la corrispondenza degli importi indicati nelle fatture (attive o e passive) o negli altri documenti rilevanti con l'entità del correlato pagamento;
 - il controllo circa la corrispondenza tra i soggetti indicati nelle fatture (attive e passive) o negli altri documenti rilevanti e gli effettivi titolari del rapporto contrattuale in essi descritto;
 - la tracciabilità del processo di gestione del ciclo passivo, nonché l'archiviazione dei documenti sottostanti a ciascun pagamento effettuato (deve essere chiaramente individuabile la documentazione giustificativa a supporto di ciascun pagamento effettuato dalla Società);

- l'attuazione del principio di segregazione dei ruoli in relazione alle attività di gestione delle contabilità aziendale e nella successiva trasposizione nelle dichiarazioni tributarie;
 - la tracciabilità delle comunicazioni di maggiore rilevanza con i Consulenti coinvolti nella redazione delle suddette scritture e dichiarazioni;
 - la custodia in modo corretto e ordinato delle scritture contabili e degli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali, assicurando difese fisiche e informatiche che impediscano eventuali atti di distruzione od occultamento;
 - il monitoraggio – anche attraverso l'ausilio di Consulenti – del rispetto dei principi che regolano la compilazione, tenuta e conservazione delle dichiarazioni di natura fiscale; in particolare, devono essere previsti meccanismi di monitoraggio che consentano la rilevazione di eventuali carenze o errori nella gestione degli aspetti fiscali e la tempestiva individuazione e implementazione delle necessarie azioni correttive;
 - l'individuazione preliminare della persona competente all'effettuazione di un pagamento per la Società e che la stessa sia dotata dei poteri per procedere al pagamento e a operare sui conti correnti della Società;
 - l'adozione nello svolgimento delle operazioni sugli *asset* della Società – siano essi asset fisici ovvero partecipazioni societarie – di modalità trasparenti e tracciabili per tutti i passaggi del relativo *iter* e per quanto riguarda gli spostamenti di denaro che gli stessi comportano;
 - l'astensione, nello svolgimento delle operazioni di cui al punto che precede, dal porre in essere alcuna azione volta a pregiudicare in qualsivoglia modo le ragioni dell'erario (anche in relazione alla soddisfazione di eventuali pagamenti di imposte ovvero di interessi o sanzioni amministrative relativi a dette imposte).
- La compilazione dei modelli di dichiarazione e dei moduli di pagamento (es. F24) è sottoposta ad adeguati controlli in merito alla correttezza dei dati inseriti. A tal fine è garantita (i) la segregazione di ruoli tra le funzioni preposte alla compilazione e quelle preposte alla verifica prima dell'invio definitivo nonché (ii) il necessario coinvolgimento degli organi di controllo (Collegio Sindacale, Società di Revisione) per le verifiche di loro competenza e dei consulenti esterni eventualmente incaricati.

Si rinvia inoltre a quanto previsto per gli aspetti contabili all'interno della Parte Speciale II relativa ai reati societari.

2. Gestione delle operazioni straordinarie

- tutte le transazioni commerciali devono essere supportate da adeguata documentazione contrattuale che contenga una chiara indicazione dei soggetti coinvolti, dell'attività/prestazione a carico di ciascuna delle parti, delle caratteristiche dell'operazione, dei corrispettivi pattuiti e delle relative modalità di pagamento;
- ogni operazione e transazione, anche internazionale, deve essere supportata da adeguata documentazione giustificativa che trovi riscontro nei sistemi utilizzati per la tracciabilità delle operazioni aziendali.

Si rinvia inoltre a quanto previsto per la medesima Attività Sensibile all'interno della Parte Speciale II relativa ai reati societari.

3. Gestione dei rimborsi spese

Si rinvia a quanto previsto all'interno della Parte Speciale I relativa ai reati contro la P.A.

4. Selezione di Fornitori, Consulenti e Partner e gestione dei relativi rapporti

- Ai fini della qualifica e del conseguente inserimento di un nuovo fornitore in anagrafica sono svolte verifiche preliminari sull'affidabilità dello stesso sotto il profilo fiscale, con richiesta, nei casi dubbi, di autodichiarazioni e/o certificati che attestino l'assenza di precedenti e/o carichi fiscali e tributari pendenti nonché la regolarità retributiva e contributiva.

Si rinvia a quanto previsto all'interno della Parte Speciale II relativa ai reati societari.

5. Rapporti con l'Amministrazione Fiscale

- La Società si impegna a garantire la massima collaborazione e trasparenza nell'ambito dei rapporti con l'Amministrazione Fiscale (Agenzia delle Entrate, Guardia di Finanza, ecc.). In particolare, si impegna a garantire che:
 - siano individuati espressamente i soggetti autorizzati a trasmettere comunicazioni nei confronti dell'Agenzia delle Entrate e a riscontrarne le richieste;
 - qualsivoglia comunicazione di informazioni/dati/notizie nei confronti dell'Agenzia delle Entrate sia effettuata in maniera corretta ed esaustiva.

* * *

**CAPITOLO VIII.5 – FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA**

Con riferimento alla presente Parte Speciale, ogni funzione coinvolta deve comunicare per quanto di competenza e con periodicità definita quanto previsto nella seguente tabella (si precisa che i flussi in oggetto, all'occorrenza, possono eventualmente essere forniti in occasione di incontri *de visu* con l'OdV):

Unità Organizzativa	Descrizione del flusso informativo	Periodicità
<i>Compliance</i> Amministrazione	Esiti dei controlli interni svolti su: - effettività delle prestazioni effettuate rispetto alle fatture emesse; - effettività delle prestazioni ricevute rispetto alle relative fatture; - veridicità delle dichiarazioni fiscali rispetto alle scritture contabili.	Annuale
<i>Compliance</i> Amministrazione	Criticità emerse nella gestione della fiscalità aziendale e ispezioni/accertamenti effettuate dall'Amministrazione fiscale.	Ad evento
<i>Compliance</i> Amministrazione	Informativa in merito alla eventuale cessione di <i>asset</i> rilevanti o di partecipazioni societarie.	Ad evento
<i>Compliance</i> Amministrazione	Informativa in merito a eventuali contenziosi fiscali	Ad evento