TSG Italia S.r.l.

Modello di organizzazione, di gestione e controllo ex Decreto Legislativo 8 giugno 2001 n. 231

Asti, 4 settembre 2023

Indice

SEZIONE A. IL DECRETO LEGISLATIVO N. 231/2001 ED I SUCCESSIVI EMENDAMENTI 6
A.1 Il regime di responsabilità amministrativa previsto a carico delle persone giuridiche, società e associazioni 6
A.2 L'adozione del "Modello di Organizzazione e di Gestione" quale possibile esimente della responsabilità amministrativa 7
A.3 Adozione del Modello da parte di TSG Italia 8
A.3.1 Organismo di Vigilanza e Controllo (OdV) 9
A.4 Funzione del Modello 11
A.5 Modifiche e integrazioni del Modello 11
A.6 Individuazione delle Funzioni Direttive ed attribuzione dei compiti di vigilanza 12
sull'attuazione del modello 12
A.6.1 Destinatari del Modello 13
A.6.2 Diffusione, comunicazione e formazione 13
A.7 Sistema disciplinare 13
A.7.1 Sanzioni per i lavoratori dipendenti 13
A.7.2 Misure nei confronti dei dirigenti 15
A.7.3 Vertici aziendali 15
A.7.4 Collaboratori, consulenti 15
A.8 Verifiche periodiche 15
A.9 Modello e Codice etico comportamentale 15
A.10 Perimetro delle attività di TSG ed aree di reati non pertinenti 16
SEZIONE B. REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE 16
B.1 La tipologia dei reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del Decreto) 16
B.2 Aree a rischio 18
B.3 Principi generali di comportamento e di attuazione del processo decisionale nelle aree di attività a rischio 19
SEZIONE C. REATI SOCIETARI 21
C.1 Le tipologie dei reati societari - art. 25 ter del Decreto 21
C.1.1 False comunicazioni sociali – art. 2621 c.c. 21
C.1.2 Fatti di lieve entità – art. 2621 bis c.c. 21
C.1.3 False comunicazioni sociali delle società quotate – art. 2622 c.c. 22
C.1.4 Impedito controllo – art. 2625 II° comma c.c. 22

C.1.5 Indebita restituzione dei conferimenti – art. 2626 c.c. 22

C.1.6 Illegale ripartizione degli utili o delle riserve – art. 2627 c.c. 22

C.1.7 Illecite operazioni sulle azioni o quote sociali o della società controllante – art. 2628 c.c. 22

C.1.8 Operazioni in pregiudizio dei creditori – art. 2629 c.c. 23

C.1.9 Omessa comunicazione del conflitto di interessi – art. 2629 bis c.c. 23

C.1.10 Formazione fittizia del capitale – art. 2632 c.c. 23

C.1.11 Indebita ripartizione dei beni sociali da parte dei liquidatori – art. 2633 c.c. 23

C.1.12 Corruzione tra privati – art. 2635 c.c. 23

C.1.13 Illecita influenza sull'assemblea – art. 2636 c.c. 24

C.1.14 Aggiotaggio – art. 2637 c.c. 24

C.1.15 Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza – art. 2638 I e II comma c.c. 25
C.2 Aree a rischio 25
C.3 Principi generali di comportamento e di attuazione 26
C.4 Istruzioni e verifiche dell'OdV 27
SEZIONE D. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI 28
D.1 Delitti informatici e trattamento illecito di dati: tipologia 28
D.2 Falsità in un documento informatico pubblico avente efficacia probatoria (art. 491- bis c.p.) .. 29
D.3 Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) 29
D.4 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.) 30
D.5 Diffusione ed installazione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615- quinquies c.p.) 31
D.6 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) 31
D.7 Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) 32
D.8 Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.) 32
D.9 Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.) 33
D.10 Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.) 33
D.11 Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635- quinquies c.p.) 33
D.12 Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.) 34
D.13 Aree a rischio 34
D.14 Destinatari della parte speciale, principi generali di comportamento e di decisione 35
D.15 Principi generali di comportamento 35
D.16 Istruzioni e verifiche dell'OdV 36
SEZIONE E. REATI IN MATERIA DI SICUREZZA E SALUTE SUL LAVORO 37
E.1 Normativa specifica sul modello 38
E.2 Aree a rischio 39
E.3 Principi generali di comportamento e di attuazione 39
E.4 Istruzioni e verifiche dell'OdV 40
SEZIONE F. RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA

ILLECITA, AUTORICICLAGGIO (art.25-octies) 40
F.1 Tipologie di reato 40
F.2 Aree a rischio 42
F.3 Destinatari della parte speciale 42
F.4 Principi generali di gestione 42
F.5 Regole generali di comportamento 43
F.6 Istruzioni e verifiche dell'OdV 44
SEZIONE G. INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA (art.25-decies) 44
G.1 La tipologia dei reati contro l'Amministrazione della Giustizia (Legge 3 Agosto 2009, n. 116) .. 44
G.2 Aree ed Attività a rischio 45
G.3 Destinatari della parte speciale, principi generali di comportamento e di decisione 45
G.4 Procedimento di formazione ed attuazione della volontà decisionale nelle aree di attività a rischio di commissione dei reati 46

G.4.1 Criteri ai quali uniformare il processo decisionale afferente le aree di attività a rischio di commissione dei reati 46

G.4.2 Principi di comportamento in riferimento ad attività a rischio di commissione di reati 46

G.5 Organismo di Vigilanza 46
SEZIONE H. IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (art.25-duodecies) 47
H.1 Area a rischio ed obblighi da osservare 47
SEZIONE I. REATI AMBIENTALI 47

I.1 Aree a rischio 48

I.2 Principi generali di comportamento e di attuazione 48
SEZIONE L. DISCIPLINA DEL WHISTLEBLOWING 49
L.1 PRIMA PARTE – PRINCIPI GENERALI 49
COS'É IL WHISTLEBLOWING 49
PRINCIPI GENERALI 50
L.2 PROCEDURA DI GESTIONE DELLE SEGNALAZIONI: IL CANALE INTERNO 55
SEZIONE M. REATI TRIBUTARI 60
M.1 I reati tributari (art. 25 quinquiesdecies) – Tipologia e caratteristiche 60

M.1.1 Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (articolo 2 commi 1 e 2 bis del D.LGS. n. 74/2000). 60

M.1.2 Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000) 62

M.1.3 Emissione di fatture o altri documenti per operazioni inesistenti (articolo 8, commi 1 e 2 bis del D.Lgs. n. 74/2000) 64

M.1.4 Distruzione od occultamento di documenti contabili (articolo 10 D.Lgs. n 74/2000) 65

M.1.5 Sottrazione fraudolenta al pagamento delle imposte (art. 11 D.Lgs. n. 74/2000) 66
M.2 La confisca del prezzo o del profitto del reato 68
M.3 La Direttiva dell'Unione Europea sulla protezione degli interessi finanziari 69
M.4 Aree potenzialmente a rischio di commissione dei reati di cui all'Articolo 25 quinquiesdecies Decreto 231 69

M.5 I destinatari della parte speciale 70
M.6 Principi generali di gestione 70
M.7 Il transfer pricing 71
M.8 Il cash pooling 72
M.9 Principi di comportamento 72
M.10 Procedure e istruzioni di lavoro 74
M.11 Flussi di comunicazione all'OdV 74
M.12 Compiti dell'OdV 75

SEZIONE A. IL DECRETO LEGISLATIVO N. 231/2001 ED I SUCCESSIVI EMENDAMENTI

A.1 Il regime di responsabilità amministrativa previsto a carico delle persone giuridiche, società e associazioni

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 Decreto Legislativo n. 231 (di seguito denominato anche il "Decreto"), 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 a cui l'Italia ha già da tempo aderito, quali la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione anch'essa firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

Con tale Decreto, dal titolo "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", è stato introdotto nell'ordinamento italiano un regime di responsabilità c.d. amministrativa (riferibile sostanzialmente alla responsabilità penale) a carico degli enti (da intendersi come società, consorzi, ecc., di seguito denominati "Enti") per una lunga serie di reati commessi, nell'interesse o vantaggio degli stessi,

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 e 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)."*

Tale responsabilità si aggiunge a quella della persona fisica autore dell'illecito.
L'ampliamento della responsabilità mira a coinvolgere nella punizione di taluni illeciti penali gli Enti che abbiano tratto vantaggio dalla commissione del reato. Tra le sanzioni previste, le più gravi per l'impresa sono rappresentate da misure interdittive quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la PA, l'interdizione dall'esercizio dell'attività, l'esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi, anche se non sono da trascurare le pesanti sanzioni pecuniarie.

La responsabilità prevista dal suddetto Decreto si configura anche in relazione a reati commessi all'estero, purché per gli stessi non proceda lo Stato del luogo in cui è stato commesso il reato.

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 e precisamente:

- indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico (art. 316-ter c.p.);
- truffa in danno dello Stato o di altro ente pubblico (art. 640, 2° comma, n. 1 c.p.);
- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.);
- corruzione per un atto d'ufficio (art. 318 c.p.);
- corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
- corruzione in atti giudiziari (art. 319-ter c.p.);
- istigazione alla corruzione (art. 322 c.p.);
- concussione (art. 317 c.p.);
- malversazione a danno dello Stato o di altro ente pubblico (art. 316-bis c.p.).

Successivamente, l'art. 6 della Legge 23 novembre 2001 n. 409, recante "Disposizioni urgenti in vista dell'introduzione dell'Euro", ha inserito nell'ambito del Decreto l'art. 25-bis, che mira a punire il reato di "falsità in monete, in carte di pubblico credito e in valori di bollo".

In seguito l'art. 3 del Decreto Legislativo 11 aprile 2002 n. 61, in vigore dal 16 aprile 2002, nell'ambito della nuova riforma del diritto societario ha introdotto il nuovo art. 25-ter del Decreto 231/2001, estendendo il regime di responsabilità amministrativa degli Enti anche nei confronti dei c.d. reati societari, così come configurati dallo stesso Decreto n. 61/2002 (false comunicazioni sociali, false comunicazioni sociali in danno dei soci o dei creditori, falso in prospetto, falsità nelle relazioni o nelle comunicazioni della società di revisione, impedito controllo, indebita restituzione dei conferimenti, illegale ripartizione degli utili e delle riserve, illecite operazioni sulle azioni o quote sociali o della società controllante, operazioni in giudizio dei creditori, formazione fittizia del capitale, indebita ripartizione dei beni sociali da parte dei liquidatori, illecita influenza sull'assemblea, aggiotaggio, ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza).

Dal 2002 ad oggi sono stati apportati al D.lgs. n.231 una serie di emendamenti che riguardano soprattutto la sua applicabilità a nuove categorie di reati. Fra di esse selezioniamo quelle che, per la sua struttura ed attività in Italia, potrebbero interessare, come aree di rischio, la TSG Italia:

i. Sicurezza sul lavoro (art.25 septies);
ii. Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio (art. 25 octies);
iii. Concussione, induzione indebita a dare o promettere utilità e corruzione (nuove ipotesi delittuose o aggravanti di ipotesi già indicate nell'art.24,I°comma: artt.319 bis,319 ter,319 quater,320,321,322 bis) (art.25);
iv. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies);
v. Reati ambientali (art.25 undecies);
vi. Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art.25 duodecies);
vii. Disciplina del Whistleblowing (art. 6 c. 2-bis, 2-ter, 2-quater);
viii. Reati tributari (art. 25 quinquiesdecies)

A.2 L'adozione del "Modello di Organizzazione e di Gestione" quale possibile esimente della responsabilità amministrativa

L'articolo 6 del Decreto, nell'introdurre il suddetto regime di responsabilità amministrativa, prevede, tuttavia, una forma specifica di esonero da detta responsabilità qualora l'Ente dimostri che:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b)".

Ne deriva pertanto che la preventiva adozione ed efficace attuazione di un idoneo modello organizzativo, peraltro facoltativo, esonera l'Ente dalla responsabilità amministrativa per i reati commessi dalle persone fisiche operanti nell'Ente stesso.
"In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di cui alla lettera a), del comma 1, devono rispondere alle seguenti esigenze:

a) *individuare le attività nel cui ambito possono essere commessi reati;*
b) *prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;*
c) *individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;*
d) *prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;*
e) *introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello".*

È infine previsto che, negli Enti di piccole dimensioni, il compito di vigilanza possa essere svolto direttamente dall'organo dirigente (art.6.4). Nel 2012 è stato aggiunto il comma 4 bis a norma del quale *"nelle società di capitali il collegio sindacale, il consiglio di sorveglianza e il comitato per il controllo della gestione possono svolgere le funzioni dell'organismo di vigilanza di cui al comma 1, lettera b)".*

A.3 Adozione del Modello da parte di TSG Italia

Secondo l'art.4 dello statuto in vigore la Società ha per oggetto:

- La progettazione e l'assemblaggio di macchine e attrezzature in genere, sia meccaniche che elettroniche, il relativo sviluppo e commercializzazione sia del prototipo che della serie;
- La produzione e/o la vendita di apparecchi di distribuzione e/o misurazione dei carburanti, di liquidi e gas, nonché di fluidi in genere e di prodotti e apparecchiature per la sicurezza stradale;
- La produzione e/o vendita di accessori, parti e componenti degli apparecchi suddetti;
- La produzione e/o vendita di tutte le apparecchiature meccaniche, elettriche ed elettroniche connesse al funzionamento delle stazioni di erogazione di carburanti liquidi e gassosi, nonché degli impianti di distribuzione di fluidi in genere;
- L'installazione e manutenzione di tutte le apparecchiature, loro parti e componenti;
- La progettazione e/o la costruzione e/o la vendita di stazioni di erogazione di carburanti liquidi e gassosi ovvero loro parti e componenti;
- Assumere e dismettere partecipazioni in società nazionali ed estere, costituite o costituende;
- Effettuare in qualunque modo, anche sotto forma di interessenza, l'acquisto, l'esercizio, la vendita e la liquidazione di aziende nazionali ed estere aventi scopi analoghi ed affini;
- Effettuare l'esercizio dell'attività di valutazione della conformità, effettuazione di verificazione degli strumenti di misura utilizzati per funzioni di misura legale.

La Società potrà, in via secondaria, per il raggiungimento degli scopi sociali:

- Assumere e dismettere locazioni di aziende commerciali ed industriali, nazionali ed estere;
- Assumere o riconcedere e dismettere rappresentanze di case nazionali ed estere;
- Ottenere e sfruttare concessioni, licenze, privative, brevetti di ogni genere e specie;
- Effettuare finanziamenti a società del gruppo;
- Concedere garanzie reali e fideiussioni a favore di terzi anche per conto ed a garanzia di obbligazioni di società controllate, collegate e di altre società del gruppo;
- Svolgere tutte quelle operazioni industriali, commerciali, mobiliari ed immobiliari che fossero ritenute utili per l'esplicazione degli scopi sociali o di altri affini e/o inerenti (fatta esclusione per le operazioni di raccolta del risparmio e per quelle altre operazioni che risultassero vietate dalla vigente o futura legislazione) ed effettivamente connesse.

In relazione a quanto sopra, TSG Italia [d'ora innanzi anche "Società"], nell'esigenza di assicurare condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, ha

ritenuto necessario procedere fin dal 19 settembre 2005 alla adozione del Modello di organizzazione e di gestione previsto dal Decreto Legislativo 231/2001. Tale iniziativa è stata assunta nella convinzione che l'adozione di tale Modello – al di là delle prescrizioni del Decreto, che indicano il Modello stesso come elemento facoltativo e non obbligatorio – possa costituire un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano all'interno di TSG, affinché seguano, nell'espletamento delle proprie attività, dei comportamenti lineari e corretti, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto.

Tale Modello, qui aggiornato, si fonda sulla implementazione di un sistema di procedure organizzative operative e di controllo e si propone le seguenti finalità:

- Individuare le aree ed i processi di possibile rischio nell'attività aziendale, ovvero quelle attività nel cui ambito si ritiene maggiore la possibilità che siano commessi reati;
- Definire un sistema normativo interno diretto a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai rischi/reati da prevenire tramite:
    - il Codice Etico Comportamentale
    - il Sistema certificato ***UNI EN ISO 14001:2015*** di Gestione Ambientale ed il Sistema certificato ***UNI ISO 45001:2018*** di Gestione per la Salute e la Sicurezza sul Lavoro per i servizi di progettazione e realizzazione di complessi di misura (erogatori di carburante) e sistemi di gestione pre e post pagamento, costruzione, installazione, manutenzione e ristrutturazione di impianti di distribuzione carburante e commercializzazione dei relativi componenti;
    - il Sistema certificato ***UNI ISO 9001:2015*** di Gestione per la Qualità dell'Organizzazione per i servizi di cui al punto precedente e per l'attività di laboratorio misure e verifiche periodiche degli strumenti di misura di liquidi diversi dall'acqua;
    - un sistema di deleghe e attribuzione di poteri aziendali che assicuri una chiara e trasparente rappresentazione del processo aziendale di formazione e di attuazione delle decisioni;
- Adottare una struttura organizzativa volta ad ispirare controllare la correttezza dei comportamenti, a garantire una chiara ed organica attribuzione dei compiti, applicando la segregazione delle funzioni e ad assicurare che gli assetti voluti della struttura organizzativa siano realmente attutati;
- Individuare i processi di gestione e controllo delle risorse finanziarie nelle attività a rischio;
- Attribuire all'Organismo di Vigilanza e Controllo il compito di vigilare sul funzionamento e sull'osservanza del Modello e di proporne l'aggiornamento.

A.3.1 Organismo di Vigilanza e Controllo (OdV)

In attuazione a quanto previsto dal Decreto, il Consiglio di Amministrazione (CdA), con delibera del 29 Dicembre 2014 ha istituito un Organismo di vigilanza e di controllo (OdV) con l'incarico di assumere le funzioni di Organo di controllo, e con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di curarne l'aggiornamento.

La nomina dell'OdV, nonché l'eventuale revoca sono di competenza del Consiglio di Amministrazione.

L'OdV sarà composto da due persone, una esterna alla Società e l'altra interna, per poter fornire ed avere agevole accesso a tutte le informazioni necessarie, individuata nella figura del Responsabile Qualità/Ambiente.

L'OdV dura in carica tre anni e fino alla data in cui si riunisce il primo Consiglio di Amministrazione successivo alla scadenza di detto termine. Il rinnovo dell'incarico non è tacito e deve essere

confermato dal Consiglio di Amministrazione.

All'OdV sono assegnati poteri di natura ispettiva e di controllo in ordine al funzionamento ed all'osservanza del Modello nel suo complesso. Pertanto, i membri dell'OdV possono procedere in qualsiasi momento, anche individualmente, ad atti di ispezione e controllo, riferendo poi in sede di riunione all'intero OdV.

Per esercitare efficacemente le proprie funzioni l'OdV, in particolare, può:

- avere libero accesso a tutti i documenti e a tutte le informazioni presso tutte le funzioni aziendali, ritenuti necessari per lo svolgimento dei compiti previsti;
- avvalersi, sotto la propria sorveglianza e responsabilità, dell'ausilio delle Risorse Umane che riterrà necessarie per lo svolgimento dei propri compiti, ovvero di consulenti esterni.

Sul piano operativo l'OdV, ai sensi degli artt. 6 e 7 del Decreto, ha il compito di:

- verificare periodicamente la mappa delle aree sensibili, al fine di adeguarla ai mutamenti dell'attività e/o della struttura della Società;
- effettuare periodicamente verifiche volte all'accertamento di quanto previsto dal Modello, documentando dette attività;
- verificare l'adeguatezza e l'efficacia del Modello nella prevenzione dei reati di cui al Decreto, curandone l'aggiornamento.

L' OdV è destinatario di qualsiasi informazione, documentazione e/o comunicazione, proveniente anche da terzi, ed attinente all'attuazione del Modello stesso che possa influire sull'organizzazione della Società e sul presente Modello, o comunque attinenti alle attività svolte.

Chiunque venga a conoscenza di informazioni e/o notizie, anche ufficiose, relative alla commissione dei reati previsti dal Decreto, o comunque riguardanti possibili violazioni del Modello, deve:

- rivolgersi al proprio Responsabile, il quale riferirà direttamente all'OdV;
- rivolgersi direttamente all'OdV qualora, per motivi di opportunità, non fosse possibile rivolgersi al proprio responsabile.

Con cadenza semestrale l'OdV redige una relazione e la trasmette al Consiglio di Amministrazione e, per conoscenza, al Sindaco Unico/Collegio Sindacale. Questa relazione deve contenere i risultati dell'attività di sorveglianza, effettuata attraverso verifiche (sia periodiche che a campione) e deve essere firmata dai membri dell'OdV. All'interno del documento vengono descritti i controlli effettuati nel periodo preso in considerazione ed il loro esito, con l'eventuale indicazione delle violazioni del Modello rilevate con il relativo rinvio agli organismi societari competenti. All'interno della relazione verranno inoltre evidenziate le eventuali carenze riscontrate nel Modello e quindi verranno indicati i correttivi da adottare, con anche l'indicazione delle necessità e delle modalità di aggiornamento.

L'OdV al termine del secondo semestre, in luogo della predetta relazione periodica, redige la relazione annuale da trasmettere al Consiglio di Amministrazione e, per conoscenza, al Sindaco Unico/Collegio Sindacale.

Qualora l'OdV, a seguito di un'istruttoria, rilevi la violazione del Modello o la commissione di uno dei reati previsti dal Decreto, deferisce l'autore alla Divisione Risorse Umane, la quale deciderà in merito ad eventuali provvedimenti disciplinari.

Per lo svolgimento dei propri compiti, l'OdV ha a disposizione un budget annuale stabilito dal Consiglio di Amministrazione, comunque non inferiore ad Euro 10.000,00. Tale somma può essere impiegata, ad esempio, per l'effettuazione di verifiche da parte di terzi e/o per richiedere consulenze

e pareri da parte di soggetti competenti.

I componenti esterni dell'OdV, per lo svolgimento delle loro funzioni e indipendentemente dal numero di presenze registrato, ricevono un compenso stabilito all'atto della nomina da parte del Consiglio di Amministrazione. Il pagamento di detto compenso non costituisce causa di dipendenza.

A.4 Funzione del Modello

Scopo del Modello è la costruzione di un sistema di procedure e di attività di controllo, da svolgersi anche in via preventiva, volto a prevenire la commissione delle diverse tipologie di reati contemplate dal Decreto.

In particolare, mediante l'individuazione delle "aree di attività a rischio" e la loro conseguente proceduralizzazione, il Modello si propone come finalità quelle di:

i. determinare, in tutti coloro che operano all'interno di TSG nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni riportate nel Modello, in un illecito passibile di sanzioni, sul piano penale e amministrativo, non solo nei propri confronti ma anche nei confronti dell'impresa;
ii. ribadire che tali forme di comportamento illecito sono fortemente condannate da TSG in quanto (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etico-sociali cui la Società ed il Gruppo TSG intende attenersi nell'espletamento della propria missione aziendale;
iii. consentire alla Società, grazie a un'azione di monitoraggio sulle "aree di attività a rischio", di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

Punti cardine del Modello sono, oltre ai principi già indicati:

a) l'individuazione delle aree di attività concretamente a rischio dell'azienda, vale a dire delle attività nel cui ambito si ritiene più alta la possibilità che siano commessi i reati;
b) l'attività di sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite (in particolare mediante la formazione);
c) l'attribuzione di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
d) la verifica e documentazione delle operazioni a rischio;
e) la verifica dei comportamenti aziendali, nonché del funzionamento del Modello con conseguente aggiornamento periodico;
f) irrogazione di sanzioni alle persone tramite le quali il reato è stato commesso, oppure le prescrizioni del presente Modello disattese.

A.5 Modifiche e integrazioni del Modello

Essendo il presente Modello un "atto di emanazione dell'organo dirigente" (in conformità alle prescrizioni dell'art. 6 co. I lett. a del Decreto) le successive modifiche e integrazioni di carattere sostanziale del Modello stesso sono rimesse all'approvazione del CdA, anche a seguito delle proposte elaborate dall'OdV.

Il CdA di TSG, con delibera del 19 Settembre 2005, aveva infatti demandato all'Amministratore

Delegato tutte le attività necessarie all'adozione del Modello e la facoltà di apportare allo stesso tutte le modifiche o le integrazioni che si rendessero necessarie.

A distanza di una decina di anni, tenendo conto dei nuovi interventi legislativi, degli orientamenti giurisprudenziali sempre più severi, dell'esperienza all'interno di TSG del sistema di governance successivamente adottato e dello sviluppo della sua attività, si è proceduto ad un aggiornamento del Modello, approvato dal CdA nella riunione del 29 Dicembre 2014.

Successivamente, principalmente per le modifiche intervenute alla disciplina della corruzione tra privati con il Decreto Legislativo 15 marzo 2017 n. 38, pubblicato sulla Gazzetta Ufficiale n. 75 del 30 marzo 2017, ed all'introduzione della disciplina del cosiddetto "whistleblowing", di cui alla Legge n. 179/17, il CdA, con deliberazione del 27 luglio 2018, ha deciso di intervenire nuovamente e di aggiornare il contenuto del Modello, per renderlo più rispondente alla mutata legislazione in vigore.

Infine, a seguito delle ulteriori integrazioni normative ed in considerazione dell'aumento dimensionale subito dalla Società negli ultimi anni, si è proceduto alla presente integrazione del Modello attraverso l'introduzione delle sezioni relative a "Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio" (Art. 25 octies D.Lgs 231/01), ad "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" (Art. 25 decies) ed ai "Reati Tributari" (Art. 25 quinquiesdecies). La presente versione del Modello è stata approvata con deliberazione del Consiglio di Amministrazione del 28/01/2021.

A.6 Individuazione delle Funzioni Direttive ed attribuzione dei compiti di vigilanza sull'attuazione del modello

Posto che l'art. 5 comma 1 lettera a) del Decreto identifica quali "soggetti in posizione apicale" coloro che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente, è possibile individuare tali figure secondo l'attuale struttura della TSG Italia, nelle seguenti posizioni:

- Amministratore Delegato (CEO), Rappresentante Legale della Società;
- Direttore Esecutivo (COO);
- Responsabile Commerciale;
- Responsabile Service;
- Responsabile Risorse Umane – IT;
- Responsabile Amministrazione Finanza e Controllo;

Per contro l'individuazione dei soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti del richiamato comma 1 lettera a dell'art. 5 trova riscontro delle seguenti Funzioni Direttive aziendali, risultanti dall'Organigramma aziendale divulgato alla data di elaborazione del presente Modello:

- Responsabile Sicurezza/Ambiente;
- Responsabile Compliance;
- Responsabile Qualità/PED;
- Responsabile Laboratorio Metrologico;
- Responsabile Acquisti;
- Responsabile Pratiche Amministrative;
- Responsabile Costruzioni;
- Responsabili delle Sedi Operative;
- Responsabile Marketing/R&D;
- Responsabile Agenti;
- Responsabile Accounting & Reporting;

- Responsabile Tesoreria.

E' attribuito alle Funzioni Direttive il compito specifico, sul piano operazionale, di vigilanza sull'efficace e corretto funzionamento delle disposizioni contenute nel Modello e di curarne in via preventiva la divulgazione specifica a tutti coloro posti alle loro dipendenze, coinvolti nell'esecuzione di attività ritenute a rischio e più avanti descritte, avendo cura di riportare formalmente per iscritto all'OdV qualsiasi notizia riguardante comportamenti tenuti in violazione delle norme del Modello.

È compito delle Funzioni Direttive su elencate procedere, se e qualora ritenuto necessario, in collaborazione con il Responsabile Risorse Umane, ad incontri periodici con il personale per sensibilizzarlo all'adozione delle norme contenute nel Modello e monitorarne il grado di consapevolezza.

A.6.1 Destinatari del Modello

Il presente Modello è destinato ai soggetti operanti per TSG quale che sia il rapporto che li lega alla stessa e che:

a) rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società;
b) sono sottoposti alla direzione o alla vigilanza di uno dei soggetti di cui sopra;
c) intrattengono con la Società rapporti di consulenza, appalto, subappalto e fornitura.

A.6.2 Diffusione, comunicazione e formazione

Il Consiglio di Amministrazione, avvalendosi delle strutture aziendali (in particolare delle Funzioni direttive come sopra indicate) provvede ad informare i destinatari dell'esistenza e del contenuto del Modello. La direzione Risorse Umane promuove, coordinandosi con le altre funzioni aziendali, le opportune iniziative per la diffusione e conoscenza del Modello e per la formazione di carattere generale di tutti i destinatari. La formazione è altresì specifica in relazione alla qualifica e funzione dei destinatari, al livello di rischio dell'area in cui operano e viene realizzata, se del caso, per gruppi omogenei di destinatari, anche mediante incontri, dibattiti ed esercitazioni su casi pratici.

A.7 Sistema disciplinare

Aspetto essenziale per l'effettività del Modello è costituito dalla predisposizione di un adeguato sistema sanzionatorio per la violazione delle regole di condotta imposte ai fini della prevenzione dei reati di cui al Decreto e, in generale, delle procedure interne previste dal Modello stesso.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte dall'azienda in piena autonomia indipendentemente dall'illecito che eventuali condotte possano determinare.

A.7.1 Sanzioni per i lavoratori dipendenti

I comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali dettate nel presente Modello sono definiti come illeciti disciplinari.
Con riferimento alle sanzioni irrogabili nei riguardi di detti lavoratori dipendenti il sistema diretto a sanzionare il mancato rispetto delle norme del presente Modello integra, ai sensi dell'art. 2106 c.c. per quanto non previsto e limitatamente alle fattispecie contemplate, le sanzioni previste dal CCNL Sez. 4 Titolo VII, agli artt. 8 "Provvedimenti disciplinari", 9 "Ammonizioni scritte, multe e sospensioni", 10 "Licenziamenti per mancanze", nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) ed eventuali normative speciali

applicabili.

Le sanzioni in concreto previste per la commissione dei fatti descritti sono in relazione alla loro gravità ed agli altri criteri indicati più oltre.

In particolare, si prevede che:

1) Incorre nei provvedimenti di Richiamo verbale o ammonizione scritta il lavoratore che:

   - violi le procedure interne previste dal presente Modello (ad esempio che non osservi le procedure prescritte, ometta di svolgere controlli, ecc.) o adotti, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso, dovendosi ravvisare in tali comportamenti una "non osservanza delle disposizioni portate a conoscenza dalla Società con procedure, norme interne, istruzioni operative, specifiche tecniche od altro comunicato, formalmente divulgato all'interno delle sedi aziendali.

2) Incorre nel provvedimento della Multa il lavoratore che:
   - violi più volte le procedure interne previste dal presente Modello o adotti, più volte, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso, prima ancora che dette mancanze siano state singolarmente accertate e contestate, dovendosi ravvisare in tali comportamenti la ripetuta non osservanza delle disposizioni portate a conoscenza dalla Società con procedure, norme interne, istruzioni operative, specifiche tecniche od altro comunicato, formalmente divulgato all'interno delle sedi aziendali.

3) Incorre nel provvedimento della Sospensione dal lavoro e dalla retribuzione il lavoratore che:
   - nel violare le procedure interne previste dal presente Modello o adottando, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso, nonché compiendo atti contrari all'interesse di TSG arrechi danno alla Società o la esponga a una situazione oggettiva di pericolo per la integrità dei beni dell'azienda, dovendosi ravvisare in tali comportamenti la determinazione di un danno o di una situazione di pericolo per l'integrità dei beni dell'Azienda o il compimento di atti contrari ai suoi interessi.

4) Incorre nei provvedimenti del Licenziamento senza preavviso e con trattamento di fine rapporto il lavoratore che:
   - adotti, nell'espletamento delle attività nelle aree a rischio un comportamento palesemente in violazione alle prescrizioni del presente Modello e diretto in modo univoco al compimento di un reato sanzionato dal Decreto, tale da determinare la concreta applicazione a carico della Società di misure previste dal Decreto, dovendosi ravvisare in tale comportamento la determinazione di un danno notevole o di una situazione di notevole pregiudizio per la Società, oltre al venire meno della fiducia della Società nei suoi confronti.

Il tipo e l'entità di ciascuna delle sanzioni sopra richiamate, saranno applicate in relazione:

- all'intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;
- al comportamento complessivo del lavoratore con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;

- alle mansioni del lavoratore;
- alla posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
- alle altre particolari circostanze che accompagnano la violazione disciplinare.

A.7.2 Misure nei confronti dei dirigenti

In caso di violazione, da parte di dirigenti, delle procedure interne previste dal presente Modello o di adozione, nell'espletamento di attività nelle aree a rischio, di un comportamento non conforme alle prescrizioni del Modello stesso, si provvederà ad applicare nei loro confronti le misure più idonee in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti industriali (artt.21 e. 22),in relazione alla gravità delle inosservanze, tenuto conto della particolare natura fiduciaria del rapporto di lavoro. Esse potranno andare dalla censura scritta, alla revoca della procura se esistente fino al licenziamento senza preavviso, nel rispetto delle procedure previste dall'art.7 della legge 30 maggio 1970, n.300 (Statuto dei lavoratori) ed eventuali normative speciali applicabili.

A.7.3 Vertici aziendali

Le sanzioni indicate sopra al punto A.7.2 potranno essere applicate anche nei confronti del vertice aziendale e cioè il Presidente, l'Amministratore Delegato, gli altri membri del Consiglio di Amministrazione.

A.7.4 Collaboratori, consulenti

Nei confronti di coloro che, in qualità di collaboratori o consulenti della Società e soggetti al coordinamento o vigilanza da parte della stessa, abbiano posto in essere le violazioni alle norme del Modello, potrà essere disposta la risoluzione di diritto del rapporto contrattuale ai sensi dell'art.1456 c.c., salvo restando in ogni caso l'eventuale richiesta da parte della Società del risarcimento dei danni subiti.

A.8 Verifiche periodiche

Il presente Modello sarà soggetto a due tipi di verifiche, la cui effettuazione è delegata all'OdV.

- verifiche sugli atti: annualmente si procederà a una verifica dei principali atti societari e dei contratti di maggior rilevanza conclusi dalla Società in aree di attività a rischio;
- verifiche sulle procedure: annualmente sarà verificato l'effettivo funzionamento del presente Modello con le modalità stabilite dall'OdV. Inoltre, sarà effettuata un'analisi di tutte le segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dai soggetti interessati, degli eventi considerati rischiosi, della consapevolezza del personale rispetto alle ipotesi di reato previste dal Decreto.

Gli esiti delle verifiche saranno ricompresi nelle relazioni redatte con cadenza semestrale dall'OdV, trasmesse al Consiglio di Amministrazione e, per conoscenza, al Sindaco Unico/Collegio Sindacale.

A.9 Modello e Codice etico comportamentale

Le regole di comportamento contenute nel presente Modello si integrano con quelle del vigente Codice etico comportamentale (Documento MSGI – ALL05 – REV 01), pur presentando il Modello, per le finalità che esso intende perseguire in attuazione delle disposizioni riportate nel Decreto, una portata diversa rispetto al Codice stesso.

Sotto tale profilo, infatti:

- il Codice etico comportamentale rappresenta uno strumento adottato in via autonoma e suscettibile di applicazione sul piano generale da parte delle Società del Gruppo TSG allo scopo di esprimere dei principi di "deontologia aziendale" che il Gruppo riconosce come propri e sui quali richiama l'osservanza da parte di tutti i Dipendenti, collaboratori esterni, professionisti e subappaltatori;
- il Modello risponde invece a specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di reati (per fatti che, commessi a vantaggio dell'azienda, possono comportare una responsabilità amministrativa in base alle disposizioni del Decreto medesimo).

In caso di contrasto prevarranno le disposizioni di questo Modello per i destinatari dello stesso.

A.10 Perimetro delle attività di TSG ed aree di reati non pertinenti

Poiché l'art..7.3 D.lgs. 231 dispone che "*Il modello prevede, in relazione alla natura e alla dimensione dell'organizzazione, nonché al tipo di attività svolta misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio*", TSG ha ritenuto superfluo svolgere analisi e verifiche dell'attività aziendale in relazione ai reati di seguito elencati, in quanto l'attività sociale svolta in precedenza, perseguita oggi e presumibilmente in futuro e le sue dimensioni rendono estremamente improbabile la commissione degli stessi:

a) falsità in monete, carte di pubblico credito e valori di bollo
b) delitti con finalità di terrorismo o di eversione dell'ordine democratico
c) delitti contro la personalità individuale
d) associazione per delinquere finalizzata al contrabbando di tabacchi esteri
e) associazione per delinquere finalizzata al traffico illecito di sostanze stupefacenti o psicotrope
f) traffico di migranti
g) pratiche di mutilazione degli organi genitali femminili
h) abusi di mercato
i) delitti in materia di violazione del diritto d'autore
j) reati transnazionali (legge 146/06).

SEZIONE B. REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

B.1 La tipologia dei reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del Decreto)

Si provvede qui di seguito a fornire una breve descrizione dei reati nei rapporti con la P.A., indicati negli artt. 24 e 25 del Decreto.

Malversazione a danno dello Stato o dell'Unione Europea (art. 316-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche parzialmente, la

somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta). Tenuto conto che il momento consumativo del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.

Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (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 mediante l'omissione di informazioni dovute – si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione europea.

In questo caso, contrariamente all'ipotesi delittuosa dell'art. 316-bis, 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 della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

Concussione (art. 317 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della sua posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli. Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal Decreto; in particolare, tale forma di reato potrebbe ravvisarsi, nell'ambito di applicazione del Decreto stesso, nell'ipotesi in cui un dipendente od un agente di una società del Gruppo concorra nel reato del pubblico ufficiale, il quale, approfittando di tale qualità, richieda a terzi prestazioni non dovute (sempre che, da tale comportamento, derivi in qualche modo un vantaggio per la società del Gruppo).

Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318-319 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale riceva, per sé o per altri, denaro o altri vantaggi per compiere, omettere o ritardare atti del suo ufficio (determinando un vantaggio in favore dell'offerente). L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ad esempio: pubblico ufficiale che accetta denaro per garantire l'aggiudicazione di una gara).

Tale 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 o dell'incaricato del pubblico servizio.

Istigazione alla corruzione (art. 322 c.p.)

Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale rifiuti l'offerta illecitamente avanzatagli.

Corruzione in atti giudiziari (art. 319-ter)

Tale ipotesi di reato si configura nel caso in cui una società del Gruppo sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario).

Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea (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 o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea). Tale reato può realizzarsi ad esempio nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta), al fine di ottenere l'aggiudicazione della gara stessa.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche. Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno a terzi. In concreto, può integrarsi il reato in esame qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

Induzione indebita a dare o promettere utilità (art.319 quater)

È l'ipotesi del pubblico ufficiale o dell'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità. Anche in questo caso la Società potrebbe essere coinvolta solo se il suo dipendente concorra con il pubblico ufficiale.

B.2 Aree a rischio

I reati sopra considerati trovano come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione, intesa in senso lato.

Tenuto conto dei reati espressamente richiamati dagli artt. 24 e 25 del Decreto, le aree di attività ritenute più specificamente a rischio sono state circoscritte, ai fini del presente Modello, a quelle relative alla partecipazione a procedure competitive, al conseguimento di finanziamenti o contributi e ai rapporti con gli Uffici metrici ed altri organismi similari di controllo.

In relazione a quanto sopra, ai fini della presente Sezione "B", vengono considerate, come aree di attività a rischio:

1. la partecipazione a procedure di gara o di negoziazione diretta indette da enti pubblici per l'assegnazione di commesse (di appalto, di fornitura o di servizi), di concessioni, od altre operazioni similari caratterizzate comunque dal fatto di essere svolte in un contesto potenzialmente competitivo, intendendosi tale anche un contesto in cui, pur essendoci un solo concorrente in una particolare procedura, l'ente appaltante avrebbe avuto la possibilità di scegliere anche altre imprese presenti sul mercato;
2. la partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da

parte di organismi pubblici italiani o comunitari e il loro concreto impiego;
3. rapporti con uffici metrici provinciali ed altri organismi similari di controllo, coinvolti nelle attività di legalizzazione e rilegalizzazione dei prodotti commercializzati e degli impianti sottoposti alla manutenzione da parte di TSG.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere disposte dal CdA di TSG che potrà individuare le relative ipotesi e definire quali sono le Funzioni Direttive interessate.

B.3 Principi generali di comportamento e di attuazione del processo decisionale nelle aree di attività a rischio

La presente Sezione "B" si riferisce a comportamenti posti in essere da amministratori, dirigenti e dipendenti ("Destinatari") della Società, riconosciuti operanti nelle aree di attività a rischio.

Obiettivo della presente Sezione "B" è che tutti i Destinatari, come sopra individuati, adottino regole di condotta conformi a quanto qui prescritto al fine di impedire il verificarsi dei reati previsti nel Decreto.

La presente Parte speciale prevede l'espresso divieto, a carico dei Destinatari, in via diretta o indiretta, di:

1. porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto);
2. porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Nell'ambito dei suddetti comportamenti (sanciti anche dal Codice etico comportamentale adottato nell'ambito della Società con Documento MSGI – ALL05 – REV 01) è fatto divieto in particolare di:

a) effettuare elargizioni in denaro a pubblici funzionari;
b) distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire, secondo quanto previsto dal Codice etico comportamentale, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici, o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico. I regali offerti – salvo quelli di modico valore – devono essere documentati in modo adeguato per consentire le prescritte verifiche. I regali ricevuti che eccedono il modico valore dovranno essere restituiti;
c) accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al precedente punto b);
d) riconoscere compensi in favore dei collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;
e) presentare dichiarazioni non veritiere ad organismi pubblici al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;

f) destinare somme ricevute da organismi pubblici a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.
g) presentare dichiarazioni e/o certificazioni non veritiere agli Uffici metrici provinciali o all'Ufficio metrico centrale o ad altri organismi di controllo similari, nell'ambito delle attività da esperire per l'ottenimento della legalizzazione su prodotti commercializzati dalla Società o nel corso dell'attività di rilegalizzazione degli impianti in manutenzione.

Ai fini dell'attuazione dei comportamenti di cui sopra:

- nessun tipo di pagamento può esser effettuato in natura. L'effettuazione dei pagamenti deve essere effettuato nello stretto rispetto dei " punti 7) "Rilascio del benestare" e 8) "Autorizzazione al pagamento" della procedura IACQ-01 "Approvvigionamento di beni e servizi – gestione delle fatture passive" e delle procedure IAMM-01, IAMM-02, IAMM-03, IAMM-04, IAMM-05 e IAMM-08, concernenti la gestione della piccola cassa della Sede di Asti e delle altre Unità locali;
- I soggetti posti in posizione apicale e coloro i quali ricoprono Funzioni Direttive Aziendali, come individuate nel paragrafo A.6 del presente Modello, devono vigilare sul rispetto delle Procedure e delle Istruzioni aziendali in vigore, con particolare riferimento all'adozione delle disposizioni contenute nel Manuale del Sistema di Gestione Integrato Qualità e Sicurezza (MSGI) e delle relative Procedure di seguito elencate:

PS01 Gestione delle informazioni documentate
PS02 Monitoraggio e miglioramento
PS03 Gestione delle NC e dei reclami PS04 Strumenti di misura
PS05 Commerciale
PS06 Approvvigionamenti
PS07 Vendita/commercializzazione
PS08 Gestione attrezzature e infrastrutture PS09 Gestione risorse umane
PS10 Service – Manutenzione stazioni di servizio PS11 Service – Costruzioni stazioni di servizio
PS12 Valutazione Del Rischio (VDR)
PS13 Sorveglianza sanitaria PS14 Gestione dei DPI
PS15 Gestione degli infortuni
MORG Manuale Organismo di Ispezione PO01 Gestione contratti
PO02 Verificazioni periodiche PO03 Qualifica degli ispettori
PO04 Non Conformità, Ricorsi, Reclami e Contenziosi PO05 Azioni Correttive e Preventive
PO07 Gestione strumenti e attrezzature

4. le dichiarazioni rese a organismi pubblici ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere predisposto apposito rendiconto;
5. coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità.

Alla data di approvazione del presente aggiornamento del Modello emerge un moderato livello di rischiosità nelle aree di rischio di cui alla presente sezione, insito nei limitati rapporti intercorsi ed intercorrenti tra la Società ed Enti e organismi appartenenti alla Pubblica Amministrazione.

È compito dell'OdV monitorare l'evoluzione dell'attività di business della Società nei confronti della P.A., ed intervenire immediatamente con l'adozione delle opportune modifiche al Modello

organizzativo istituito, al fine di evitare l'insorgenza del rischio di applicazione della responsabilità amministrativa disciplinata dall'art. 25 del Decreto, qualora si verifichino i presupposti.

SEZIONE C. REATI SOCIETARI

C.1 Le tipologie dei reati societari - art. 25 ter del Decreto

Per quanto concerne la presente Sezione "C", di seguito si fornisce una breve descrizione dei reati contemplati nell'art. 25 ter del Decreto.

C.1.1 False comunicazioni sociali – art. 2621 c.c.

Il reato è integrato, fuori dai casi previsti dall'art. 2622 (falsi comunicazioni sociali delle società quotate), dagli amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori, che, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore. Il comma 2 dell'articolo 2621 punisce l'ipotesi in cui le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.

Il delitto di false comunicazioni sociali è stato così modificato dalla Legge n. 69/2015. Nel corpo della norma è stato eliminato il riferimento alla valutazione con riguardo all'esposizione di fatti materiali non rispondenti al vero.

Circa la persistenza della rilevanza penale delle valutazioni, le Sezioni Unite della Corte di cassazione, con la sentenza n. 22474/16 hanno precisato che: "Sussiste il delitto di false comunicazioni sociali, con riguardo all'esposizione o omissione di fatti oggetto di "valutazione", se, in presenza di criteri di valutazione normativamente fissati o di criteri tecnici generalmente accettati, l'agente da tali criteri si discosti consapevolmente e senza darne adeguata informazione giustificativa, in modo concretamente idoneo ad indurre in errore i destinatari delle comunicazioni"; ove sussistano tali requisiti pertanto, l'esposizione o omissione di fatti oggetto di "valutazione" può avere ancora una rilevanza penale.

C.1.2 Fatti di lieve entità – art. 2621 bis c.c.

La norma sanziona con pena più lieve (da sei mesi a tre anni di reclusione anziché da uno a cinque anni), salvo che il fatto non costituisca più grave reato, il delitto di false comunicazioni sociali di cui all'art. 2621 c.c. che sia di lieve entità, in considerazione della natura e delle dimensioni della società, delle modalità o degli effetti della condanna.

Si applica la stessa pena (da sei mesi a tre anni di reclusione), salvo che il fatto costituisca più grave reato, nell'ipotesi in cui il delitto di false comunicazioni sociali sia commesso in società che non superino i limiti previsti dall'art. 1 comma 2 del Regio Decreto n. 267/1942 (cosiddetta Legge Fallimentare). In tale caso poi, il delitto è procedibile a querela della società, dei soci, dei creditori, o degli altri destinatari della comunicazione sociale.

C.1.3 False comunicazioni sociali delle società quotate – art. 2622 c.c.

La norma punisce gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico consapevolmente espongono fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore.

Alle società quotate sono equiparate:

1) le società emittenti strumenti finanziari per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;
2) le società emittenti strumenti finanziari ammessi alla negoziazione in un sistema multilaterale di negoziazione italiano;
3) le società che controllano società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;
4) le società che fanno appello al pubblico risparmio o che comunque lo gestiscono.

Il comma 2 dell'articolo 2622 punisce l'ipotesi in cui le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.

C.1.4 Impedito controllo – art. 2625 II° comma c.c.

La norma punisce gli amministratori che, occultando documenti o con altri idonei artifici, impediscono od ostacolano lo svolgimento di attività di controllo legalmente attribuite ai soci, ad altri organi sociali, qualora da tale condotta derivi un danno ai soci.

C.1.5 Indebita restituzione dei conferimenti – art. 2626 c.c.

La norma punisce gli amministratori che, fuori dai casi in cui si configuri un'ipotesi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli.

C.1.6 Illegale ripartizione degli utili o delle riserve – art. 2627 c.c.

La norma punisce, salvo che il fatto non costituisca più grave reato, gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva ovvero ripartiscano riserve, anche non costituite con utili, che non possono essere distribuite.

La restituzione degli utili o la ricostruzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

C.1.7 Illecite operazioni sulle azioni o quote sociali o della società controllante – art. 2628 c.c.

La fattispecie è integrata nell'ipotesi in cui gli amministratori, al di fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o alle riserve non distribuibili per legge.

Sono altresì puniti in tal senso gli amministratori che, fuori dai casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.

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

C.1.8 Operazioni in pregiudizio dei creditori – art. 2629 c.c.

La norma punisce gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori.

Il reato è punibile a querela di parte; il risarcimento del danno ai creditori prima del giudizio estingue il reato.

C.1.9 Omessa comunicazione del conflitto di interessi – art. 2629 bis c.c.

La norma punisce l'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'art. 116 del testo unico di cui al decreto legislativo 24 febbraio 1998 n. 58, e successive modifiche, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo 1°settembre 1993 n. 385, del citato testo unico di cui al decreto legislativo n. 58 del 1998, del decreto legislativo 7 settembre 2005 n. 209, o del decreto legislativo 21 aprile 1993, n. 124, che viola gli obblighi previsti dall'articolo 2391, primo comma, se dalla violazione siano derivati danni alla società o a terzi.

C.1.10 Formazione fittizia del capitale – art. 2632 c.c.

Tale ipotesi di reato mira a tutelare l'integrità del capitale sociale, punendo gli amministratori ed i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale sociale attraverso l'attribuzione di azioni o quote sociali in misura complessivamente superiore all'ammontare del capitale sociale, la sottoscrizione reciproca di azioni o quote, la sopravvalutazione rilevante dei conferimenti di beni in natura e dei crediti ovvero del patrimonio sociale in caso di trasformazione.

C.1.11 Indebita ripartizione dei beni sociali da parte dei liquidatori – art. 2633 c.c.

La norma punisce i liquidatori che, ripartendo i beni sociali prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, cagionano un danno ai creditori. Il reato è procedibile a querela della persona offesa e si estingue se, prima del giudizio, il danno ai creditori è risarcito.

C.1.12 Corruzione tra privati – art. 2635 c.c.

Sono puniti con la reclusione da uno a tre anni, 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 se' o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.

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

Il delitto è punibile a querela della persona offesa salvo che dal fatto derivi una distorsione della concorrenza nella acquisizione di beni o servizi.

Il Decreto Legislativo n. 38/2017 entrato in vigore il 14 aprile 2017 ha modificato i contenuti del reato di corruzione tra privati di cui all'articolo 2635 c.c..

Le novità di maggior rilievo si rintracciano nella previsione di un nuovo soggetto, "l'interposta persona" e "nell'offerta" del denaro o altra utilità in precedenza solamente promesso o corrisposto. Inoltre, ai sensi del nuovo articolo 2635 ter c.c., alla condanna per il reato di cui all'articolo 2635, primo comma, seguirà l'interdizione temporanea dagli uffici direttivi delle persone giuridiche per coloro che hanno già subito una condanna per il medesimo reato o per quello di cui all'articolo 2635 bis, secondo comma.

Viene altresì punito l'istigatore alla corruzione nel settore privato. Ai sensi del novellato articolo 2635 bis, infatti, 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. Si procede a querela della persona offesa.

È stato contestualmente modificata la lett. s-bis dell'art. 25 ter del D.Lgs n. 231/01, in materia di responsabilità amministrativa degli enti, che nella nuova versione prevede per il delitto di corruzione tra privati, nei casi previsti dal terzo comma dell'art. 2635 c.c., la sanzione pecuniaria da quattrocento a seicento quote e, nei casi di istigazione di cui al primo comma dell'art. 2635 bis c.c., la sanzione pecuniaria da duecento a quattrocento quote. Si applicano altresì le sanzioni interdittive previste dall'articolo 9, comma 2, in precedenza non previste.

C.1.13 Illecita influenza sull'assemblea – art. 2636 c.c.

Tale ipotesi di reato si configura nel caso in cui chiunque, con atti simulati o fraudolenti, determini la maggioranza in assemblea allo scopo di procurare, a sé o ad altri, un ingiusto profitto.

C.1.14 Aggiotaggio – art. 2637 c.c.

La norma punisce chiunque diffonde notizie false, ovvero pone in essere 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 ad incidere in modo significativo sull'affidamento che il pubblico

ripone nella stabilità patrimoniale di banche o di gruppi bancari.

C.1.15 Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza – art. 2638 I e II comma c.c.

La norma punisce gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima.

La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi. È altresì prevista la responsabilità penale degli amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori di società, o enti ed altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolino le funzioni.

Si richiama, per completezza, l'articolo 2639 del codice civile ("Estensione delle qualifiche soggettive") il quale prevede che ai soggetti formalmente investiti della qualifica o titolari delle funzioni previste dalle leggi civili, siano equiparati coloro che sono tenuti a svolgere la stessa funzione, diversamente qualificata nonché coloro che esercitano in modo continuativo e significativo i poteri tipici inerenti la qualifica o la funzione (i cosiddetti "soggetti di fatto").

Al di fuori dei casi in cui siano applicabili le norme riguardanti i delitti dei pubblici ufficiali contro la pubblica amministrazione, le disposizioni sanzionatorie relative agli amministratori si applicano

anche a coloro che sono legalmente incaricati dall'autorità giudiziaria o dall'autorità di pubblica vigilanza di amministrare la società o i beni dalla stessa posseduti o gestiti per conto terzi.

C.2 Aree a rischio

In relazione ai reati e alle condotte criminose sopra elencate, le aree ritenute più specificamente a rischio risultano essere, ai fini della presente Sezione "C" del Modello, le seguenti:

- Predisposizione di comunicazioni dirette al Socio, agli enti appaltanti, pubblici e privati, ovvero al pubblico in generale, in particolare rappresentato da istituti di credito e operatori finanziari, riguardo alla situazione economica, patrimoniale e finanziaria della società;
- Redazione del bilancio d'esercizio e delle relative relazioni accompagnatorie;
- Operazioni societarie che possano incidere sull'integrità del capitale sociale;
- Informative e rapporti con gli organi di informazione e stampa;
- Relativamente al reato di cui all'art. 2627 c.c. (Illegale ripartizione degli utili e delle riserve), tutte le attività riguardanti il processo di distribuzione di utili e/o riserve in conformità agli obblighi di legge;
- Gestione della contabilità e tenuta dei documenti contabili ed extracontabili;
- Gestione del ciclo attivo e passivo, degli approvvigionamenti e dei rapporti contrattuali con fornitori e clienti;
- Gestione dei flussi finanziari e dei fondi della società;

- Rapporti infragruppo, con particolare riferimento ai flussi finanziari;
- Rapporti con società di revisione e organo di controllo legale e contabile;
- Area attinente la "corporate governance" e la direzione generale (ad esempio l'approvazione delle delibere del Consiglio di Amministrazione nonché loro attuazione da parte di soggetti delegati in materia di aumento o riduzione del capitale, conferimenti, ripartizione di utili, fusioni e/o scissioni);
- Gestione delle spese di rappresentanza, omaggi, sponsorizzazioni e liberalità;

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere disposte dal CdA di TSG che potrà individuare le relative ipotesi e definire quali sono le funzioni direttive interessate.

C.3 Principi generali di comportamento e di attuazione

La presente Sezione "C" si riferisce a comportamenti posti in essere da amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci, liquidatori, dirigenti ed i loro dipendenti in linea gerarchica che operino nelle aree di attività a rischio (di seguito i "Destinatari").
Obiettivo della presente Parte speciale è che tutti i Destinatari, come sopra individuati e nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle aree a rischio, si attengano a regole di condotta conformi a quanto qui prescritto al fine di prevenire e impedire il verificarsi dei Reati Societari sopra elencati.

In particolare, la presente Parte speciale ha la funzione di:

a. fornire un elenco dei principi generali e delle istruzioni specifiche, ai quali i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
b. fornire all'OdV gli strumenti per esercitare le attività di controllo, monitoraggio e verifica previste.

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, i Destinatari devono in generale conoscere e rispettare tutte le regole e i principi contenuti nei seguenti documenti:

- il Codice etico comportamentale del Gruppo TSG (MSGI – ALL05 – REV 01);
- il Manuale e le Procedure Contabili del Gruppo TSG, con particolare riferimento alle seguenti Procedure:
- Definizione del Piano dei Conti di Gruppo (Procedure codificate "COA");
- Procedure per la reportistica di Gruppo (Procedure codificate "GRP" e "MAG");
- ogni altra documentazione relativa al sistema di controllo interno in essere nella Società, con particolare riferimento alle Procedure interne:

- IACQ-01 "Approvvigionamento di beni e servizi e gestione delle fatture passive";
- IAMM-06 "Gestione delle Immobilizzazioni Materiali".

In particolare, nell'espletamento delle attività considerate a rischio, i Destinatari dovranno attenersi ai seguenti principi generali di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati Societari;
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 (comportamenti di pericolo);

3. tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e delle altre comunicazioni sociali, al fine di fornire ad enti, pubblici e privati, ai soci ed al pubblico in generale una informazione veritiera e appropriata sulla situazione economica, patrimoniale e finanziaria della Società;
4. assicurare completa tracciabilità (per iscritto su supporto cartaceo e/o informatico) dei processi volti alla selezione dei fornitori/prestatori d'opera ed all'aggiudicazione dei contratti per la fornitura di materiali e/o prestazioni di servizi/subappalto, nel pieno rispetto di quanto definito nelle procedure in precedenza richiamate ed in particolare della procedura interna IACQ-01 "Approvvigionamento di beni e servizi e gestione delle fatture passive";

In ordine a tale punto, è fatto divieto di:

i. predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Società;
ii. omettere di comunicare dati e informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;
iii. non attenersi ai principi e alle prescrizioni contenute nel Manuale Contabile di Gruppo;

5. osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, assicurare il regolare funzionamento della Società e degli organi sociali ed agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei soci, dei creditori e dei terzi. In ordine a tale punto, è fatto divieto di:

    i. restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
    ii. ripartire utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve (anche non costituite con utili) che non possono per legge essere distribuite;
    iii. effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;
    iv. procedere in ogni modo a formazione o aumento fittizi del capitale sociale;
    v. ripartire i beni sociali tra i soci – in fase di liquidazione – prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli.

C.4 Istruzioni e verifiche dell'OdV

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i Reati Societari sono i seguenti:

a) curare l'emanazione e l'aggiornamento delle istruzioni relative ai comportamenti da seguire nell'ambito delle attività a rischio, come individuate nella presente Sezione "C";
b) con riferimento al bilancio, alle relazioni e alle altre comunicazioni sociali previste dalla legge, in ragione anche della circostanza che la situazione contabile di TSG redatta secondo i principi contabili internazionali (IFRS) è sottoposta a verifica di una società di revisione, l'OdV, in collaborazione con il Responsabile Amministrazione, Finanza e Controllo, provvede all'espletamento dei seguenti compiti:

    - monitoraggio sull'efficacia delle procedure interne per la prevenzione del reato di

false comunicazioni sociali;

- esame di eventuali segnalazioni specifiche (anche anonime) provenienti da qualsiasi dipendente ed effettuazione degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute;
- vigilanza sull'effettiva sussistenza delle condizioni per garantire alla società di revisione una concreta autonomia nelle sue funzioni di controllo delle attività aziendali;

c) con riferimento alle altre attività a rischio:

- verifiche periodiche, da effettuarsi con cadenza minima annuale, sul rispetto delle procedure interne;
- monitoraggio sull'efficacia delle verifiche a prevenire la commissione dei reati.

SEZIONE D. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

D.1 Delitti informatici e trattamento illecito di dati: tipologia

La legge 18.3.2008 n. 48 ha ratificato la Convenzione del Consiglio d'Europa sulla criminalità informatica, redatta a Budapest il 23 novembre 2001, avente quale obiettivo la promozione della cooperazione internazionale tra gli Stati firmatari al fine di contrastare il proliferare di reati a danno della riservatezza, dell'integrità e della disponibilità di sistemi, reti e dati informatici.

La Convenzione estende la portata del reato informatico includendo tutti i reati in qualunque modo commessi mediante un sistema informatico, anche nel caso in cui la prova del reato sia sotto forma elettronica.

A seguito della ratifica ed esecuzione della Convenzione suddetta dopo l'art. 24 del D.Lgs. 231/01 è stato inserito l'art. 24 bis "Delitti informatici e trattamento illecito di dati", che lenca la serie dei reati informatici che possono dar luogo alla responsabilità amministrativa degli enti. La citata legge ha modificato anche il codice di procedura penale, essenzialmente al fine di agevolare e regolamentare le indagini e le operazioni di perquisizione e di sequestro dei dati informatici, imponendo all'Autorità procedente di adottare misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

A tal fine si riporta di seguito una descrizione dei reati richiamati dall'art. 24 bis del D.Lgs. 231/01 che possono dar luogo alla responsabilità amministrativa degli enti, in base al quale:

1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635- bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.
2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica la sanzione pecuniaria sino a trecento quote.
3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'art. 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.
4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'art. 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei

delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'art. 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'art. 9, comma 2, lettere c), d) ed e)".

Si riporta di seguito una breve descrizione dei reati contemplati nell'art. 24 bis del Decreto.

D.2 Falsità in un documento informatico pubblico avente efficacia probatoria (art. 491-bis c.p.)

L'art. 491-bis c.p. dispone che ai documenti informatici aventi efficacia probatoria si applichi la medesima disciplina penale prevista per le falsità commesse con riguardo ai tradizionali atti pubblici cartacei, previsti e puniti dagli articoli da 476 a 493 del codice penale. Si citano in particolare i reati di falsità materiale o ideologica commessi da pubblico ufficiale o da privato in atti pubblici, uso di atto falso.

In particolare, si ha "falsità materiale" quando un documento non proviene dalla persona che risulta essere il mittente o da chi risulta dalla firma (contraffazione) ovvero quando il documento è artefatto (alterato) per mezzo di aggiunte o cancellazioni successive alla sua formazione anche da parte dell'autore originario. Si ha invece "falsità ideologica" quando un documento non è veritiero nel senso che, pur non essendo né contraffatto né alterato, contiene dichiarazioni non vere o non fedelmente riportate.

Per "documento informatico" s'intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevati così come riportato dall'art. 1 lettera p) del decreto legislativo n° 82 del 7 marzo 2005 (Codice dell'Amministrazione Digitale).

Il concetto di documento informatico, secondo quanto stabilito dallo stesso Codice dell'Amministrazione Digitale, non è dunque legato al relativo supporto materiale, in quanto l'elemento penalmente determinante ai fini dell'individuazione del documento informatico consiste nella possibilità di attribuire allo stesso di un'efficacia probatoria secondo le norme civilistiche.

In particolare, il Codice dell'Amministrazione Digitale (art. 1 e art. 20) precisa che:

1. un documento informatico non sottoscritto con firma elettronica non ha efficacia probatoria, ma eventualmente soddisfa i requisiti legali che possono equipararlo alla forma scritta;
2. un documento informatico riportante la firma elettronica può non avere efficacia probatoria se non dopo la valutazione della sicurezza, integrità e non modificabilità dello stesso;
3. un documento informatico sottoscritto con firma elettronica qualificata ha l'efficacia prevista dall'articolo 2702 del Codice civile, ovvero a meno della querela di falso.

Tale ipotesi di reato di configura nel caso in cui un rappresentante o un dipendente di TSG Italia falsifichi un documento informatico pubblico avente efficacia probatoria. Ciò potrebbe, in astratto, concretizzarsi ad esempio durante le fasi di trasmissione telematica di documenti o richieste di autorizzazione (modelli fiscali, previdenziali e contributivi, documenti amministrativi societari, legali, ecc.) ai diversi Enti della Pubblica Amministrazione.

D.3 Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)

Tale reato si realizza quando un soggetto si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza. A tal riguardo si sottolinea come il legislatore abbia inteso punire l'accesso abusivo ad un sistema informatico o telematico tout court, e dunque anche

quando ad esempio all'accesso non segua un vero e proprio danneggiamento di dati; si pensi all'ipotesi in cui un soggetto acceda abusivamente ad un sistema informatico e proceda alla stampa di un documento contenuto nell'archivio del personal computer 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 reato è aggravato qualora sia commesso da un pubblico ufficiale o 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 delle qualità di operatore di sistema; se il colpevole per commettere il fatto usa violenza sulle cose o alle persone ovvero se è palesemente armato; se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

La pena è ulteriormente aumentata se i fatti sopra illustrati riguardano sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

La suddetta fattispecie delittuosa si realizza altresì nell'ipotesi in cui il soggetto agente, pur essendo entrato legittimamente in un sistema, vi ci sia trattenuto contro la volontà del titolare del sistema, nonché, secondo il prevalente orientamento giurisprudenziale, qualora il medesimo abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato. Il delitto potrebbe pertanto essere astrattamente configurabile nell'ipotesi in cui un soggetto acceda abusivamente ai sistemi informatici di proprietà di terzi (outsider hacking), per prendere cognizione di dati riservati altrui nell'ambito di una negoziazione commerciale, (per spionaggio industriale, ad esempio), o acceda abusivamente ai sistemi aziendali della società per acquisire informazioni alle quali non avrebbe legittimo accesso in vista del compimento di atti ulteriori nell'interesse della società stessa.

Nel contesto aziendale il reato può essere commesso anche da un dipendente che, pur possedendo le credenziali di accesso al sistema, acceda a parti di esso a lui precluse, oppure acceda, senza esserne legittimato, a banche dati, anche di terzi, mediante l'utilizzo delle credenziali di altri colleghi abilitati per effettuare operazioni che portino un interesse o vantaggio per la società.

D.4 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)

Tale reato si realizza qualora un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso di un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee a raggiungere tale scopo.

Il reato è aggravato se commesso in danno di un sistema informatico o telematico utilizzato dallo stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità nonché se commesso da un pubblico ufficiale o incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio ovvero con abuso della qualità di operatore di sistema.

Il legislatore ha introdotto tale reato al fine di prevenire le ipotesi di accesso abusivo 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 (quali badge o smart card). Tale fattispecie si configura nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (ad esempio un operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi.

L'art. 615-quater c.p., inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

Per questa tipologia di reato, la sua potenziale realizzazione potrebbe avvenire nell'ambito della gestione dei processi informatici e nella gestione degli account. Il reato può essere commesso da soggetti che si procurano codici di accesso ai sistemi informatici al fine di accedere al sistema interno o esterno alla Società ed effettuare operazioni che portino interesse o vantaggio per la Società stessa.

D.5 Diffusione ed installazione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)

Tale reato si realizza qualora qualcuno, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti, o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Tale fattispecie di reato, perseguibile d'ufficio, intende reprimere anche la sola abusiva detenzione o diffusione di credenziali d'accesso o di programmi o dispositivi potenzialmente dannosi indipendentemente dalla messa in atto di altri crimini informatici.

Tale delitto potrebbe ad esempio configurarsi qualora un dipendente si procuri un virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico aziendale in modo da distruggere documenti "sensibili" in relazione ad un procedimento penale a carico della società.

Inoltre, nella valutazione di tale reato potrebbe assumere rilevanza la considerazione del carattere obiettivamente abusivo di trasmissioni di dati, programmi, e-mail, da parte del dipendente che, pur non essendo mosso da specifica finalità di lucro o di determinazione di danno, sia a conoscenza della presenza di virus che potrebbero determinare gli eventi dannosi descritti dalla norma.

D.6 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)

Tale ipotesi di reato si configura qualora un soggetto fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisca o interrompa tali comunicazioni, nonché nel caso in cui, salvo che il fatto costituisca più grave reato, un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione.

Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione dei 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.

L'intercettazione può avvenire sia mediante dispositivi tecnici, sia con l'utilizzo di software. L'impedimento od interruzione delle comunicazioni può anche consistere in un rallentamento delle comunicazioni e può realizzarsi non solo mediante impego di virus informatici, ma anche ad esempio sovraccaricando il sistema con l'immissione di numerose comunicazioni fasulle.

Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, e cioè le condotte commesse in danno di un sistema utilizzato dallo Stato o da altro ente pubblico o da imprese esercenti servizi pubblici o di pubblica necessità, da un pubblico ufficiale o incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio o con abuso della qualità di operatore di sistema e da ultimo le condotte commesse da chi esercita, anche abusivamente, la professione di investigatore privato.

Nell'ambito aziendale l'impedimento o l'interruzione potrebbero essere ad esempio causati dall'installazione non autorizzata di un software da parte di un dipendente.

D.7 Installazione di apparecchiature atte ad 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, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

Il reato è aggravato qualora ricorrano le circostanze aggravanti previste dall'articolo 617 quater sopra menzionate.

La condotta vietata dall'art. 617-quinquies c.p. è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, purché le stesse abbiano una potenzialità lesiva.
Il reato si integra, ad esempio, nel caso in cui un dipendente si introduca fraudolentemente presso un'altra società al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche affinché la società tragga particolari vantaggi.

D.8 Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)

Tale fattispecie di reato si realizza, salvo che il fatto costituisca più grave reato, quando un soggetto distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui.

Il reato è aggravato se commesso con violenza alla persona o minaccia ovvero con abuso della qualità di operatore di sistema.

Il danneggiamento potrebbe essere commesso a vantaggio della società 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 di un fornitore della società o al fine di contestare il corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell'ipotesi in cui vengano danneggiati dei dati aziendali sensibili.

D.9 Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)

Tale reato si realizza, salvo che il fatto costituisca più grave reato, quando un soggetto commetta un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dalla Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. Tale delitto si distingue dal precedente 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 al soddisfacimento di un interesse di natura pubblica.

Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora un dipendente compia atti diretti a distruggere documenti informatici aventi efficacia probatoria registrati presso enti pubblici relativi ad un procedimento penale a carico della società.

Il reato è aggravato se dal fatto derivi la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici ovvero qualora il fatto sia commesso con violenza alla persona o con minaccia o con abuso delle qualità di operatore di sistema.

D.10 Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)

Questo reato si realizza, salvo che il fatto costituisca più grave reato, quando un soggetto mediante le condotte di cui all'art. 635-bis c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informa<ioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento. Pertanto 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 c.p..

Il reato è aggravato se il fatto è commesso con violenza alla persona o con minaccia o con abuso della qualità di operatore di sistema.

D.11 Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)

Questo reato si configura quando la condotta di cui al precedente art. 635-quater c.p. sia diretta a distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità di cui all'art. 635-ter c.p., quel che rileva è in primo luogo che il danneggiamento deve avere ad oggetto un intero sistema e, in secondo luogo, che il sistema sia utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica dello stesso.

La pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero se è commesso con abuso delle qualità di operatore del sistema nonché qualora dal fatto derivi la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo sia reso, in tutto in parte inservibile.

D.12 Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)

Questo reato si configura quando un soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Tale reato è dunque un reato cd "proprio" in quanto può essere commesso solo da parte di certificatori qualificati o, meglio, i soggetti che prestano servizi di certificazione di firma elettronica qualificata.

D.13 Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificamente a rischio risultano essere, ai fini della presente Sezione speciale, quelle proprie di ogni ambito e processo aziendale che utilizza le tecnologie dell'informazione. In particolare:

- tutte le attività aziendali svolte tramite l'utilizzo dei sistemi informativi aziendali, del servizio di posta elettronica e dell'accesso ad internet;
- gestione dei sistemi informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT nonché la sicurezza informatica;
- gestione dei flussi informativi elettronici con la pubblica amministrazione.

Quanto ai reati relativi alla falsificazione materiale/ideologica di documenti informatici pubblici aventi efficacia probatoria si ritiene possano, in astratto, essere commessi in occasione dei collegamenti con la P.A. per la trasmissione di documenti a carattere pubblico.

Per tali fattispecie di reato, TSG Italia ha previsto modalità di connessione alle reti informatiche pubbliche, per l'invio di dati sensibili, che prevedano l'accesso solamente a soggetti muniti di credenziali nominali e di delega garantendo, all'interno del processo di realizzazione di un documento informatico, il principio di segregazione dei ruoli.

In relazione alle valutazioni di cui sopra, sono state individuate a rischio le aree le cui attività prevedono un rapporto con la P.A. e con le autorità attraverso l'impiego di strumenti informatici o reti telematiche.

Nello specifico le aree sensibili individuate sono quelle relative alle attività e ai processi di produzione e trasmissione delle seguenti tipologie di informazioni:

- informazioni societarie, fiscali ed inerenti alle funzioni di verifica metrologica: gli operatori autorizzati, previa autenticazione sui sistemi appositi, inoltrano all'Agenzia delle Entrate e/o alle Camere di Commercio competenti, i dati necessari ai fini fiscali, civilistici e relativi alle attività di verifica metrologica. Si ritiene pertanto che tale tipologia di attività sia sensibile in quanto ad essa sono associabili i presupposti delle falsità materiale ed ideologica;
- informazioni previdenziali e contributive verso la P.A.: gli operatori autorizzati, previa autenticazione sul sistema apposito, caricano il tracciato con i dati oggetto della comunicazione (ad esempio comunicazioni periodiche, comunicazioni relative alle assunzioni, ecc.). Dal momento che la trasmissione è diretta verso la P.A. (ad esempio INPS e INAIL) e riguarda informazioni aventi potenzialmente efficacia probatoria, si ritiene che la relativa attività di produzione e trasmissione presenti i presupposti per il reato di falsificazione materiale ed ideologica;

- informazioni relative alle disposizioni di pagamento: gli operatori autorizzati, previa autenticazione sul sistema apposito, caricano o riportano tramite compilazione i dati sul sistema di remote banking e procedono ad autorizzare l'esecuzione dei relativi flussi finanziari. Si ritiene che questa attività di produzione e trasmissione sia sensibile in quanto ad essa sono associabili i presupposti della falsità materiale ed ideologica.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere disposte dal CdA di TSG che potrà individuare le relative ipotesi e definire quali sono le funzioni direttive interessate.

D.14 Destinatari della parte speciale, principi generali di comportamento e di decisione

La presente parte speciale si applica a tutte le funzioni coinvolte nella gestione e nell'utilizzo dei sistemi informatici e del patrimonio informativo, ed in particolare si riferisce ai comportamenti posti in essere da amministratori, dirigenti e dipendenti della società, organi sociali nonché da partner e collaboratori esterni con essa operanti sulla base di un rapporto contrattuale.

In particolare, devono essere portati a conoscenza dell'OdV, ad opera delle funzioni competenti:

- i processi da seguire e gli obblighi da osservare nello svolgimento delle proprie attività nell'utilizzo dei sistemi informatici con dichiarazione di conformità al D.Lgs. 231/01;
- l'elencazione dei principali adempimenti effettuati nell'espletamento dell'attività di controllo e verifica;
- gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

È compito dei singoli responsabili delle funzioni di Gruppo diffondere a tutti i dipendenti la consapevolezza dei reati che potrebbero commettere e promuovere l'utilizzo delle misure adottate per prevenirli.

Le funzioni e i destinatari della presente parte speciale a qualsiasi titolo, coinvolti nelle attività di gestione e utilizzo di sistemi informatici e del patrimonio informativo, sono tenute ad osservare:

- le disposizioni di legge esistenti in materia;
- la normativa interna nonché le eventuali previsioni del Codice etico e le prescrizioni previste dalle policy e dalle procedure interne di riferimento.

D.15 Principi generali di comportamento

Sulla base degli standard di riferimento internazionali, per sistema aziendale di sicurezza informatica si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità, della tracciabilità dell'informazione e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

Sulla base di tali principi generali, la presente sezione speciale prevede l'espresso divieto di porre in essere / collaborare / dare causa, alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D.Lgs. 231/01 e più in particolare, a titolo meramente esemplificativo e non esaustivo:

- introdursi abusivamente in un sistema informatico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso;
- accedere al sistema informatico, o a parti di esso, ovvero a banche dati della società, o a

parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti software non autorizzati atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- detenere, procurarsi, riprodurre, o diffondere abusivamente codici di accesso o comunque messi idonei all'accesso di un sistema protetto da misure di sicurezza;
- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti.

TSG Italia si impegna a sua volta, a porre in essere, a titolo meramente esemplificativo e non esaustivo, i seguenti adempimenti:

- informare adeguatamente tutti i dipendenti autorizzati all'utilizzo dei sistemi informativi, dell'importanza di mantenere le proprie credenziali confidenziali e di non divulgare le stesse a soggetti terzi nonché dell'importanza del cambio periodico delle password;
- prevedere attività di formazione e addestramento periodico in favore dei dipendenti e diversificate in ragione delle rispettive mansioni;
- implementare sui sistemi informativi politiche che rispettino il principio di separazione dei ruoli, cosiddetto "segregation of duties", definendo e distribuendo diverse responsabilità operative e di gestione evitando sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto, anche in relazione ai processi di formazione dei documenti informatici e compatibilmente con le funzionalità disponibili nei sistemi informativi in dotazione alla società;
- prevedere, per ogni dipendente, un procedimento di autenticazione mediante l'utilizzo di credenziali corrispondenti ad un profilo definito e specifico per il ruolo ricoperto.

D.16 Istruzioni e verifiche dell'OdV

L'OdV può effettuare verifiche a campione sulle attività potenzialmente a rischio, dirette a monitorare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere.

Esso esamina eventuali segnalazioni specifiche ed effettua gli accertamenti ritenuti necessari ed opportuni in relazione alle segnalazioni ricevute.

In ragione dell'attività di vigilanza attribuita all'OdV nel presente Modello, a tale organismo viene garantito in generale libero accesso a tutta la documentazione aziendale che lo stesso ritiene rilevante al fine del monitoraggio dei processi sensibili individuati nella presente sezione speciale.

L'amministratore di sistema (oppure, in alternativa, la funzione competente) deve indirizzare all'OdV report periodici sullo stato di attuazione della presente sezione speciale.

SEZIONE E. REATI IN MATERIA DI SICUREZZA E SALUTE SUL LAVORO

Il Decreto indica questi reati nell'art. 25-septies. Le fattispecie individuate sono due:

1) Omicidio colposo commesso con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 589, c.p.).

L'omicidio colposo sussiste in tutti i casi in cui l'agente, nel tenere un comportamento lecito, compie per negligenza, imprudenza, imperizia o violazione di leggi o regolamenti, un atto da cui deriva la morte di una persona.
Elemento soggettivo è quindi la colpa e, con specifico richiamo all'aggravante di cui all'art. 589, comma 2, c.p. (se il fatto è commesso con violazione delle norme sulla prevenzione degli infortuni sul lavoro), la colpa del datore di lavoro (o del capocantiere, ad esempio) può consistere in un atto puramente omissivo.
Con riferimento all'antinfortunistica, la giurisprudenza ha precisato che essa può configurarsi sia nel caso di violazione di specifiche norme per la prevenzione degli infortuni sul lavoro (negligenza specifica) sia in ipotesi di omissione dell'adozione di misure o accorgimenti per la più efficace tutela della integrità fisica dei lavoratori, in violazione dell'art. 2087 c.c.

2) Lesioni colpose gravi o gravissime commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art.590, comma terzo, c.p.).

Si ha lesione colposa quando si cagiona una lesione personale in conseguenza di negligenza, imprudenza, o violazione di leggi o regolamenti.
La lesione può essere:
- lieve: se da essa deriva una malattia od un'incapacità ad attendere alle ordinarie occupazioni che non superi quaranta giorni;
- grave: se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia od un'incapacità ad attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni, oppure se il fatto produce l'indebolimento permanente di un senso o di un organo o, ancora, se la persona offesa è una donna incinta e dal fatto deriva l'acceleramento del parto;
- 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. Ed ancora, nei casi in cui essa determini la deformazione ovvero lo sfregio permanente del viso o l'aborto della persona offesa.

Il regime sanzionatorio posto dal Decreto a carico dell'ente per i reati in materia di salute e sicurezza sul lavoro è di natura sia pecuniaria che interdittiva. La sanzione pecuniaria è prevista in misura non inferiore a mille quote.

Nel caso di condanna, si applicano all'ente anche le sanzioni interdittive previste dall'art. 9.2 del Decreto per una durata non inferiore a tre mesi e non superiore ad un anno. È esclusa l'applicazione delle misure interdittive in sede cautelare.

Per quanto concerne il sistema di prevenzione e protezione va fatto riferimento al decreto legislativo 9 aprile 2008, n.81 che, fra l'altro, disciplina la gestione della prevenzione nei luoghi di lavoro

dettagliando gli obblighi a carico del datore di lavoro e dei suoi collaboratori (artt.15-54).

E.1 Normativa specifica sul modello

In relazione a questa area di rischio il D.lgs. 9 aprile 2008, n.81, all'art. 30 adatta alla specificità dell'area le norme generali del Decreto sulla responsabilità degli enti, così disponendo:

"Modelli di organizzazione e di gestione

1. *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.*

2. *Il modello organizzativo e gestionale di cui al comma 1 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1*
3. *Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dime nsioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.*
4. *Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.*
5. *In sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti. Agli stessi fini ulteriori modelli di organizzazione e gestione aziendale possono essere indicati dalla Commissione di cui all'articolo 6.*
   5-bis. La commissione consultiva permanente per la salute e sicurezza sul lavoro elabora procedure semplificate per la adozione e la efficace attuazione dei modelli di organizzazione e gestione della sicurezza nelle piccole e medie imprese. Tali procedure sono recepite con decreto del Ministero del lavoro, della salute e delle politiche sociali". (omissis)

E.2 Aree a rischio

Siccome qui le aree di rischio abbracciano potenzialmente tutte le attività della Società in cui sono impiegati, dirigenti e dipendenti è onere dell'OdV e dei vari responsabili delle funzioni indicate sopra al punto A.6 mettere in atto quanto richiesto nell'art. 30 del D.Lgs. 9 aprile 2008, n. 81 qui riportato. In particolare, dovranno essere conferite ai vari responsabili adeguate deleghe e messe a loro disposizione adeguate risorse per le attrezzature di sicurezza e la prevenzione dei rischi.

E.3 Principi generali di comportamento e di attuazione

Destinatari delle norme in materia di sicurezza e salute sul lavoro sono tutti coloro che, nell'ambito dell'attività d'impresa svolta dalla Società, hanno responsabilità, diretta o indiretta, nella tutela della salute e sicurezza nei luoghi di lavoro, a prescindere dal mansionario specifico, e perciò tutti i membri del CdA, i dirigenti del personale, il responsabile del servizio di prevenzione e protezione, i capi reparto.

Al fine di garantire la piena adozione delle norme contenute nella presente Sezione del Modello, la Società ha adottato un Sistema di Gestione per la Salute e la Sicurezza sul Lavoro conforme e certificato in base alla norma UNI ISO 45001:2018, per i servizi di Progettazione e realizzazione di complessi di misura (erogatori di carburanti) e sistemi di gestione pre e post pagamento, costruzione, installazione, manutenzione e ristrutturazione di impianti di distribuzione carburante e commercializzazione dei relativi componenti.

Per effetto dell'implementazione del suddetto Sistema di Gestione per la Salute e la Sicurezza sul Lavoro, sono state adottate procedure per:

a) il rispetto degli standard tecnico-strutturali relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
b) l'attività di valutazione dei rischi e predisposizione delle misure di prevenzione e protezione;
c) l'attività di natura organizzativa, quali emergenze e primo soccorso;
d) l'attività di sorveglianza sanitaria;
e) l'informazione e la formazione dei lavoratori;
f) le procedure e istruzioni per il lavoro in sicurezza;
g) l'acquisizione di documentazioni e certificazioni obbligatorie di legge.

In relazione a questa area di rischio la Società ha elaborato e distribuito a tutto il personale operativo istruzioni dettagliate sulle modalità con le quali eseguire le principali operazioni sui punti vendita, riportate nel documento denominato "JSA – JHA Job Safety Analysis – Job Hazzard Analysis". Anche (ma non solo) in relazione a queste istruzioni i destinatari dovranno:

1. prendersi cura della sicurezza e della salute delle persone presenti sul luogo di lavoro, su cui possono ricadere gli effetti delle loro azioni od omissioni;
2. osservare le disposizioni e le istruzioni impartite dal datore di lavoro ai fini della protezione collettiva ed individuale;
3. utilizzare correttamente i macchinari e le apparecchiature, i mezzi di trasporto e le altre attrezzature di lavoro, come pure i dispositivi di sicurezza e protezione;
4. segnalare senza indugio al datore di lavoro le deficienze dei mezzi e dispositivi di cui al punto 3, nonché le altre eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro conoscenze e disponibilità, per eliminare o ridurre tali deficienze, o pericoli, dandone notizia al rappresentante dei lavoratori

per la sicurezza;
5. non rimuovere o modificare senza autorizzazione o comunque compromettere i dispositivi di sicurezza o di segnalazione o di controllo;
6. non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori.

In particolare, una volta individuato il pericolo, se il rimedio rientra nei mansionari, dovrà darvisi esecuzione senza indugi; in caso contrario, la persona interessata dovrà informarne, sempre senza indugio, il suo referente superiore.
Quanto al sistema di sanzioni si applicheranno le regole stabilite retro al punto A.7.

E.4 Istruzioni e verifiche dell'OdV

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i Reati in materia di tutela della salute e della sicurezza sul lavoro sono in particolare:

- Verificare il sistema di deleghe e procure in vigore (in riferimento al servizio di prevenzione e protezione e comunque in materia di sicurezza) e la loro coerenza con il sistema delle comunicazioni organizzative;
- Svolgere verifiche sul rispetto all'applicazione delle procedure interne previste dal sistema di gestione;
- Esaminare eventuali segnalazioni specifiche ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- Prendere atto degli audit di terza parte effettuati, nell'ambito del sistema di gestione adottato, dalle società di certificazione e seguire l'andamento nel tempo del processo di chiusura degli eventuali rilievi;
- Proporre al datore di lavoro le eventuali integrazioni alle procedure esistenti per rendere più efficaci, ove necessario, le azioni di prevenzione e repressione delle condotte vietate.

SEZIONE F. RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA, AUTORICICLAGGIO (art.25-octies)

F.1 Tipologie di reato

Il Decreto indica questi reati nell'art. 25-octies. Le fattispecie individuate sono le seguenti:

1) Ricettazione (ART. 648 c.p.)

La norma punisce chi, fuori dei casi di concorso nel reato, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare.
La pena è ridotta se il fatto è di particolare tenuità.

Le disposizioni di questo articolo si applicano anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto.

2) Riciclaggio (ART. 648 bis c.p.)

Il delitto è integrato da chi, fuori dei casi di concorso nel reato, sostituisce o trasferisce denaro, beni

o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

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

La pena è 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.

Il reato sussiste anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto.

Il reato di riciclaggio, secondo la più recente giurisprudenza, differisce dalla ricettazione in relazione agli elementi strutturali dell'illecito, quali l'elemento soggettivo, ovvero dolo specifico dello scopo di lucro nella ricettazione e dolo generico nel delitto di riciclaggio; nonché l'elemento materiale, ovvero l'idoneità dell'azione volta a ostacolare l'identificazione della provenienza del bene nel delitto di cui all'art. 648 bis c.p.

3) Impiego di denaro, beni o utilità di provenienza illecita (ART. 648 ter c.p.)

La norma punisce chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita nell'ipotesi di particolare tenuità.
Il reato sussiste anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto.

"Tra il reato di impiego di denaro, beni o utilità di provenienza illecita e quello di riciclaggio, nonché tra quest'ultimo e quello di ricettazione vi è rapporto di specialità, che discende dal diverso elemento soggettivo richiesto dalle tre fattispecie incriminatrici - essendo comune l'elemento materiale della disponibilità di denaro o altra utilità di provenienza illecita: il delitto di cui all'art. 648 cod. pen. richiede una generica finalità di profitto, quello di cui all'art. 648 bis cod. pen. lo scopo ulteriore di far perdere le tracce dell'origine illecita, quello, infine, di cui all'art. 648 ter cod. pen. che tale scopo sia perseguito mediante l'impiego delle risorse in attività economiche o finanziarie". (Cass. Pen. sez. II, sentenza del 14/07/2016, n. 33076).

Molte sono le fattispecie che possono costituire il reato da cui provengono o altri beni: delitti contro il patrimonio (quali il furto, la truffa, la rapina, l'estorsione, l'appropriazione indebita, l'usura) ma anche, a mero titolo esemplificativo, i reati tributari (false od omesse dichiarazioni dei redditi che possono procurare utili illeciti al loro autore), reati societari.

4) Autoriciclaggio (ART.648 ter1 c.p.)

La legge n. 186 del 2014 ha introdotto nel Codice penale il nuovo delitto di autoriciclaggio previsto e punito dall'articolo 648 ter1 ed inserito anche quale reato presupposto per la responsabilità delle Società ai sensi del Decreto 231 nell'articolo 25 octies.
Il nuovo delitto punisce colui che, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative il denaro, i beni o le altre utilità provenienti dal delitto commesso.

Le condotte descritte dalla norma (impiego, sostituzione, trasferimento) devono essere realizzate in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.
È prevista una riduzione di pena qualora il denaro, i beni o le altre utilità provengano dalla commissione di un delitto non colposo punito con la reclusione inferiore nel massimo a cinque anni ed una circostanza aggravante qualora i fatti siano commessi nell'esercizio di un'attività bancaria, finanziaria o di altra attività professionale.
È altresì prevista una riduzione di pena per colui che 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.
Non è invece punibile il soggetto che destini il denaro, i beni o le altre utilità alla mera utilizzazione o al godimento personale.

Con l'introduzione del delitto di autoriciclaggio sono punite le condotte di impiego, sostituzione e trasferimento anche per il soggetto che ha commesso o ha concorso a commettere il delitto non colposo da cui il denaro, i beni o le altre utilità provengono, a differenza delle altre ipotesi (ricettazione, riciclaggio e reimpiego) che si applicano sono a coloro che non hanno commesso o concorso a commettere il delitto a monte.

Sempre con riferimento al delitto di autoriciclaggio, il denaro, i beni o le altre utilità possono innanzitutto provenire da uno dei reati previsti dal Decreto 231 (quali ad esempio i reati societari) e anche, sebbene la questione sia dibattuta nella dottrina specialistica, da altri reati non presupposto della responsabilità prevista dal Decreto 231 (quali ad esempio i reati tributari/fiscali).

F.2 Aree a rischio

- Approvvigionamento/acquisiti (beni/servizi);
- Commerciale/vendita;
- Gestione contabile;
- Gestione flussi finanziari;
- Risorse umane;
- Adempimenti di bilancio;
- Logistica/Magazzino;
- Rapporti con fornitori;
- Gestione adempimenti fiscali;
- Rapporti infragruppo;
- Rapporti con intermediari finanziari;
- Aree/attività/processi a rischio di commissione di reati-presupposto oggetto delle altre parti speciali del Modello 231 della società. dai quali possano generarsi proventi illeciti.

F.3 Destinatari della parte speciale

Sono Destinatari della presente parte speciale gli organi sociali, gli amministratori e i dipendenti che operino nelle aree delle attività individuate come a rischio, oltreché tutti i soggetti che rivestano la qualifica di legale rappresentante.

F.4 Principi generali di gestione

Nella gestione delle attività nelle aree di rischio indicate, la società opera in modo da assicurare:

a. Trasparenza nella gestione dei dati contabili e nella circolazione delle informazioni;
b. Delimitazione dei ruoli e delle attribuzioni delle diverse funzioni attraverso il ricorso a deleghe

e procure che individuano con chiarezza poteri e relative responsabilità dei destinatari delle medesime;

c. Tracciabilità (per iscritto su supporto cartaceo e/o informatico) di tutte le operazioni di natura contabile.

F.5 Regole generali di comportamento

I destinatari della presente parte speciale devono, oltre ad osservare regole e principi codificati nelle altre parti speciali del presente Modello di organizzazione, gestione e controllo, in particolare:

- agire in conformità alla normativa vigente, alle regole previste dal Modello e dal Codice Etico;
- assicurare il pieno rispetto dei requisiti di trasparenza, verificabilità e documentabilità nella gestione delle risorse finanziarie e, più in generale, nell'esercizio dell'attività della Società e nelle transazioni finanziarie;
- garantire la piena corrispondenza tra documentazione e relativi acquisiti/vendite effettuati;
- attenersi alla disciplina prevista nel sistema di gestione della qualità già adottato dalla società ed alle relative procedure operative ed istruzioni di lavoro anche con riferimento alla scelta ed ai rapporti con i fornitori e gestione clienti;
- assicurare la coerenza del prezzo delle transazioni in riferimento ai prezzi di mercato;
- assicurare una trasparente gestione delle risorse finanziare della Società nel rispetto delle competenze e delle procedure interne/istruzioni di lavoro e delle norme di legge;
- effettuare controlli sui flussi finanziari in entrata, tenendo in considerazione alcuni indicatori quali sede legale della controparte (ad esempio "paradisi fiscali", Paesi a rischio terrorismo etc.);
- operare con trasparenza garantendo la tracciabilità di ogni operazione effettuata nell'ambito dei rapporti infragruppo;
- verificare la provenienza delle merci o dei beni in entrata od oggetto di operazioni finanziarie;
- verificare la corrispondenza delle merci/beni acquistati con la documentazione accompagnatoria e gli ordini di acquisto;
- nel processo di assunzione di dipendenti, acquisire le certificazioni del casellario giudiziale nonché le documentazioni attestanti cittadinanza e regolare presenza dello straniero sul territorio italiano;
- assicurare la corretta informazione e formazione sui contenuti del Modello di organizzazione, gestione e controllo e sul relativo sistema disciplinare;
- astenersi dal tenere qualsivoglia condotta da cui possano generarsi proventi illeciti;
- non effettuare operazioni di transfer pricing in violazione dell'art. 110, comma 7, del TUIR;
- assicurare il rispetto degli adempimenti fiscali/tributari alle scadenze previste dalla legge.

È vietata la ricezione ed il trasferimento di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore in euro o valuta estera, effettuato a qualsiasi titolo tra soggetti diversi, quando il valore oggetto di trasferimento, anche se oggetto di frazionamento, è complessivamente pari o superiore ad Euro 3.000. Il trasferimento può tuttavia essere effettuato per il tramite di banche, istituti di moneta elettronica e Poste Italiane spa.
Gli assegni bancari e postali emessi per importi pari o superiori ad Euro 1.000 devono indicare il nome o la ragione sociale del beneficiario e la clausola di non trasferibilità.

Con particolare riferimento alla prevenzione del rischio di commissione del delitto di autoriciclaggio, è vietato ai destinatari della presente parte speciale di:

- indicare nelle dichiarazioni relative alle imposte sui redditi e IVA (non solo le dichiarazioni annuali ma anche, ad esempio, gli elenchi Intrastat e le dichiarazioni di intento) elementi passivi fittizi mediante fatture o altri documenti analoghi aventi efficacia probatoria per

operazioni inesistenti;
- indicare nella dichiarazione dei redditi o nella dichiarazione iva elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, anche attraverso 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;
- indicare nella dichiarazione annuale dei redditi o IVA elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi inesistenti (costi inesistenti o ricavi più bassi);
- omettere di presentare la dichiarazione annuale dei redditi e/o IVA;
- emettere o rilasciare fatture o altri documenti per operazioni inesistenti;
- occultare o distruggere 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;
- omettere il versamento dell'IVA nei termini di legge;
- omettere il versamento delle ritenute d'acconto nei termini previsti;
- alienare simulatamente o compiere altri atti fraudolenti sui beni della Società o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte;
- indicare nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi;
- non versare le somme dovute utilizzando in compensazione crediti non spettanti o inesistenti.

F.6 Istruzioni e verifiche dell'OdV

L'OdV può effettuare verifiche a campione per monitorare l'efficacia delle procedure interne per la prevenzione dei reati ascritti alla presente Parte Speciale con particolare riferimento al Codice Etico, ed esaminare eventuali segnalazioni in arrivo, disponendo gli accertamenti ritenuti necessari.

Sono inviati all'Odv, da parte dei responsabili delle funzioni interessate, report periodici aventi ad oggetto la gestione degli adempimenti della presente parte speciale e fatte in ogni caso salve le comunicazioni urgenti che si rendessero necessarie.

SEZIONE G. INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA (art.25-decies)

G.1 La tipologia dei reati contro l'Amministrazione della Giustizia (Legge 3 Agosto 2009, n. 116)

La presente fattispecie si riferisce al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, richiamato dalla disposizione di cui all'art. 25-decies del D.lgs. 231/2001.

Tale norma, introdotta nel Decreto legislativo con Legge 3 agosto 2009, n. 116, testualmente prevede: "in relazione alla commissione del delitto di cui all'articolo 377-bis del Codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote".

La citata disposizione normativa, a sua volta, stabilisce: Art. 377-bis c.p. - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria - "Salvo che il fatto costituisca

più grave reato, 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, è punito con la reclusione da due a sei anni".

La norma richiamata mira a tutelare le possibili strumentalizzazioni della facoltà di tacere concessa agli indagati ed agli imputati, nonché ai cd. indagati/imputati in procedimenti connessi, al fine di tutelare il corretto svolgimento dell'attività processuale contro tutte le indebite interferenze.

Possono, pertanto, risultare destinatari della condotta gli indagati e gli imputati (anche in procedimento connesso o in un reato collegato) che potrebbero essere indotti dalla Società a "non rispondere" o a rispondere falsamente all'Autorità giudiziaria (giudice, pubblico ministero).

Il reato in oggetto può quindi assumere rilevanza all'interno della Società nell'ipotesi in cui possa verificarsi un processo penale a carico di un qualsiasi soggetto della Società, amministratore, consigliere e/o sindaco, responsabile e/o dirigente, dipendente e/o operaio, e altro soggetto della Società stessa ponga in essere la condotta descritta nel reato di cui all'art. 377 bis c.p., finalizzata a non far rendere dichiarazioni o a rendere dichiarazioni mendaci nel processo penale.

G.2 Aree ed Attività a rischio

I processi che la società ha individuato al proprio interno come sensibili nell'ambito dei reati contro l'amministrazione della giustizia riguardano la gestione dei rapporti con l'Autorità giudiziaria.

G.3 Destinatari della parte speciale, principi generali di comportamento e di decisione

Obiettivo della presente Parte Speciale è che tutti i Destinatari, come individuati nella Parte Generale, adottino regole di condotta conformi a quanto prescritto nella presente sezione del Modello, al fine di prevenire il verificarsi dei reati in essa considerata.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- indicare i principi di comportamento a cui i Dipendenti, gli Organi Sociali, i Consulenti e Partner della Società devono attenersi;
- fornire all'Organismo di Vigilanza, e ai responsabili delle altre funzioni aziendali che cooperano con esso, i principi cui devono ispirarsi e necessari per esercitare le attività di controllo, monitoraggio e verifica.

Si indicano di seguito i criteri procedurali, che tutti i Destinatari sono tenuti a rispettare:

- nei rapporti con l'Autorità giudiziaria, i Destinatari sono tenuti a prestare una fattiva collaborazione ed a rendere dichiarazioni veritiere, trasparenti ed esaustivamente rappresentative dei fatti;
- nei rapporti con l'Autorità giudiziaria, i Destinatari e, segnatamente, coloro i quali dovessero risultare indagati o imputati in un procedimento penale, anche connesso, inerente all'attività lavorativa prestata, sono tenuti ad esprimere liberamente le proprie rappresentazioni dei fatti od a esercitare la facoltà di non rispondere accordata dalla legge;
- tutti i Destinatari devono tempestivamente avvertire, attraverso gli strumenti di comunicazione esistenti all'interno della Società (oppure con qualsivoglia strumento di comunicazione, purché nel rispetto del principio di tracciabilità), l'Organismo di Vigilanza di ogni atto, citazione a testimoniare e procedimento giudiziario (civile, penale o amministrativo) che li veda coinvolti, sotto qualsiasi profilo, in rapporto all'attività lavorativa prestata o comunque ad essa attinente;

- l'Odv può acquisire gli atti del processo ed eventualmente chiedere informazioni al difensore dell'indagato o imputato che deve essere sentito dall'Autorità Giudiziaria.

G.4 Procedimento di formazione ed attuazione della volontà decisionale nelle aree di attività a rischio di commissione dei reati

G.4.1 Criteri ai quali uniformare il processo decisionale afferente le aree di attività a rischio di commissione dei reati

Nell'espletamento di tutte le operazioni attinenti alla gestione dei rapporti con l'Autorità giudiziaria, oltre alle regole di cui al presente Modello e, in particolare, a quelle indicate nel successivo paragrafo G.4.2, tutti i dipendenti e gli Organi Sociali della società, nonché i suoi consulenti e partner devono conoscere e rispettare:

- il Codice Etico del presente Modello;
- l'organigramma aziendale e la documentazione e le disposizioni inerenti alla struttura gerarchico;
- funzionale aziendale e organizzativa del Gruppo, nel rispetto del sistema dei poteri e deleghe esistente;
- il principio di separazione dei ruoli e responsabilità nelle fasi dei processi aziendali;
- il sistema disciplinare di cui al CCNL ed al presente Modello.

G.4.2 Principi di comportamento in riferimento ad attività a rischio di commissione di reati

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, la fattispecie di reato sopra richiamata; sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti, i quali, sebbene risultino tali da non costituire di per sé reato, possano potenzialmente diventarlo.

In particolare:

- la Società vieta espressamente a chiunque di coartare od indurre, in qualsiasi forma e con qualsiasi modalità, nel malinteso interesse della società, la volontà dei Destinatari di rispondere all'Autorità giudiziaria o di avvalersi della facoltà di non rispondere;
- nei rapporti con l'Autorità giudiziaria, ai Destinatari non è consentito accettare denaro o altra utilità, anche attraverso consulenti della Società medesima;
- nei rapporti con l'Autorità giudiziaria è vietata ogni forma di condizionamento che induca il Destinatario a rendere dichiarazioni non veritiere;
- tutti i Destinatari devono tempestivamente avvertire l'Organismo di Vigilanza di ogni violenza o minaccia, pressione, offerta o promessa di danaro o altra utilità, ricevuta al fine di alterare le dichiarazioni da non rendere all'Autorità giudiziaria.

G.5 Organismo di Vigilanza

L'OdV effettua controlli a campione sulle attività potenzialmente a rischio, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere.

Esso esamina eventuali segnalazioni specifiche ed effettua gli accertamenti ritenuti necessari ed

opportuni in relazione alle segnalazioni ricevute.

In ragione dell'attività di vigilanza attribuita all'OdV nel presente Modello, a tale organismo viene garantito in generale libero accesso a tutta la documentazione aziendale che lo stesso ritiene rilevante al fine del monitoraggio dei processi sensibili individuati nella presente Parte Speciale.

SEZIONE H. IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (art.25-duodecies)

Compie questo reato il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dall' articolo 22 D.lgs.25 luglio 1998, n.286 (sull'assunzione di lavoratori subordinati stranieri a tempo determinato ed indeterminato), ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato.

H.1 Area a rischio ed obblighi da osservare

L'area di rischio rientra fra le competenze del Responsabile risorse umane, il quale dovrà accertare, prima dell'impiego di tali lavoratori, che tutti i permessi e le condizioni di cui all'art.22 del D.lgs. 25 luglio 1998, n.286 come pure che le condizioni dettate dallo Sportello Unico per l'Immigrazione siano rispettate. Per impiego si devono intendere tutte le forme giuridiche o di fatto attraverso le quali la società si avvale della collaborazione di dipendenti.

SEZIONE I. REATI AMBIENTALI

I reati ambientali, per la cui commissione è prevista la responsabilità amministrativa dell'ente, sono disciplinati nell'art. 25-undecies del Decreto che comprende la violazione di varie norme del Codice penale (dall'elenco abbiamo tolto alcuni reati, tra i quali quelli di cui all'art.727 "Abbandono di animali" e all'art.727 bis "Uccisione di animali" perché non entrano nel perimetro dell'attività della Società), del D. Lgs 3 aprile 2006, n.152 (Codice dell'ambiente), della Legge 7 febbraio 1992, n.150 , della Legge 28 dicembre 1993, n. 549, del D.L. 6 novembre 2007, n. 2002.

I principali reati sanzionati sono i seguenti:

a) **Distruzione o deterioramento di habitat** all'interno di un sito protetto (art. 733-bis c.p.) ovvero una zona classificata a tutela speciale ai sensi dell'art. 4, commi 1 e 2 della Direttiva 2009/147/CE, oppure un habitat naturale designato come zona speciale di conservazione ai sensi dell'art. 4, paragrafo 4 della Direttiva 92/43/CE.
b) **Apertura di nuovi scarichi e scarico di acque reflue industriali contenenti sostanze pericolose** effettuato senza autorizzazione o quando essa sia stata revocata o sospesa o utilizzazione agronomica di effluenti di allevamento, acque di vegetazione di frantoi oleari, acque reflue di aziende agricole e piccole aziende agroalimentari al di fuori dei casi e delle procedure previste (art. 137, comma 3, D.Lgs. 3 aprile 2006, n. 152 contenente Norme in materia ambientale).
c) Reati in materia di **attività di gestione dei rifiuti non autorizzata** (art. 256 D.lgs.3 aprile 2006 n.152 Codice dell'ambiente) **bonifica dei siti** (art. 257), **violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari per la tracciabilità dei rifiuti (SISTRI)** (art. 258), delle attività organizzate per il **traffico illecito di rifiuti** (art. 260), del **sistema informatico di controllo della tracciabilità dei rifiuti** (art. 260-bis).
d) L' art. 279 D. lgs. 3 aprile 2006, n. 152, sanziona **l'installazione o la modifica di un impianto**

o di una attività senza autorizzazione o perché scaduta, sospesa, revocata, o in violazione dell'ordine di chiusura dell'impianto o di cessazione dell'attività, disattendendo i valori limite di emissione e le prescrizioni stabilite.

e) La Legge 28 dicembre 1993, n. 549, art. 3, disciplina l'attuazione delle norme in materia di cessazione e riduzione **dell'impiego di sostanze lesive dell'ozono atmosferico e dannose per l'ambiente**, in particolare controllando la produzione, il consumo, l'importazione, l'esportazione, la detenzione e la commercializzazione di sostanze lesive (omissis).

f) Il D.L. n.136 del 2013 ha introdotto nel Codice dell'ambiente l'art.256 bis che istituisce il reato di **combustione illecita dei rifiuti**.

g) Nel caso della commissione dei reati di attività organizzata per il **traffico illecito di rifiuti** (art. 260, D.lgs. 3 aprile 2006, n. 152) o di **inquinamento doloso causato da navi** (art. 8, D.Lgs. 6 novembre 2007, n. 202) si applica all'ente la sanzione dell'interdizione definitiva dall'esercizio dell'attività (art. 16.3 Decreto).

I reati possono essere compiuti con dolo o con colpa anche lieve., che include la semplice imprudenza o imperizia. Le sanzioni pecuniarie applicabili a tali reati vanno da 150 a 500 quote, le pene detentive da uno a tre anni.

L'interdizione definitiva può essere disposta se l'ente ha tratto dal reato un profitto di rilevante entità oppure è già stato condannato almeno 3 volte negli ultimi 7 anni all'interdizione temporanea dall'esercizio dell'attività.

I.1 Aree a rischio

I processi che la Società ha individuato al proprio interno come sensibili nell'ambito dei reati ambientali riguardano:

- Lo smaltimento di rifiuti urbani e altri rifiuti speciali (ad es. toner, neon, etc..);
- l'attività svolta nell'ambito della manutenzione e controllo delle stazioni di servizio, degli erogatori di carburanti e di tutte le apparecchiature ivi installate, nonché per lo smantellamento e/o dismissione delle stesse.

La Società ha adottato un Sistema di Gestione Ambientale conforme e certificato ENI EN ISO 14001:2015 per i servizi di Progettazione e realizzazione di complessi di misura (erogatori di carburante) e sistemi di gestione pre e post pagamento, costruzione, installazione, manutenzione e ristrutturazione di impianti di distribuzione carburante e commercializzazione dei relativi componenti.
Nell'ambito del predetto sistema sono previste una mappatura ed un'analisi dei rischi, un organigramma ed una verifica delle deleghe/funzioni, oltre ad una serie di procedure e protocolli, che coinvolgono vari soggetti interessati.

Le funzioni e le procedure ivi contenute sono oggetto di audit e di aggiornamento periodico.

I.2 Principi generali di comportamento e di attuazione

Oltre ai vertici aziendali, i destinatari del Modello per evitare i reati ambientali di cui sopra sono soprattutto coloro che coordinano le attività sopra indicate e pertanto in primis i responsabili della Manutenzione delle Sedi Operative, i quali dovranno:

1) monitorare l'attività svolta dai tecnici posti sotto la propria responsabilità presso le stazioni di servizio;
2) individuare le singole attività che, pur non avendo ancora causato gli eventi puniti come reato, hanno la potenzialità di causarli;

3) intervenire direttamente per eliminare il pericolo oppure, se ciò non rientra nelle competenze, avvisare senza indugio i responsabili competenti di cui al punto A.6;
4) seguire puntualmente le disposizioni che sono emanate in linea generale o di volta in volta dalla Società relativamente allo svolgimento delle attività sopra indicate.

A tal proposito, e nel rispetto di quanto previsto dal predetto Sistema di Gestione Ambientale ISO 14001:2015, sarà opportuno che le relative deleghe o gli ordini di servizio comprendano i poteri non solo di monitorare i lavoratori addetti a tali attività, e le operazioni da essi compiute ma anche dare precise istruzioni atte a prevenire i reati, con facoltà di intervento immediato appena sorgesse un fatto che potrebbe dar luogo all'evento (inquinamento).

SEZIONE L. DISCIPLINA DEL WHISTLEBLOWING

L.1 PRIMA PARTE – PRINCIPI GENERALI

Il 29 dicembre 2017 era entrata in vigore la legge n. 179 recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato" (pubblicata sulla Gazzetta Ufficiale, Serie Generale n. 291 del 14 dicembre 2017).

La legge introduceva una disciplina specifica sul fenomeno del c.d. whistleblowing, perseguendo lo scopo di incentivare la collaborazione dei lavoratori per favorire l'emersione dei reati o pratiche illegali o irregolarità commessi all'interno di enti pubblici o privati.

La legge contemplava specifici meccanismi di protezione del dipendente che segnalava illeciti, distinguendo la disciplina del settore pubblico da quella del settore privato.

Nel settore privato l'art. 2 della Legge 179/2017 aveva modificato l'articolo 6 del d.lgs. 231/2001 introducendo il comma 2bis, 2ter e 2 quater.

TSG Italia s.r.l. si era, perciò, dotata di una specifica procedura in materia di whistleblowing in attuazione delle previsioni normative introdotte dall'art. 2 della Legge 179/2017.

Il 30 marzo 2023 è entrato in vigore il Decreto Legislativo 10 marzo 2023, n. 24, con il quale il Legislatore italiano ha dato attuazione della Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali (Gazzetta Ufficiale n. 63 del 15 marzo 2023).

La procedura in materia di whistleblowing adottata da TSG Italia s.r.l. è stata, quindi, rivista.

Nei paragrafi che seguono (i) si illustrerà cos'è il whistleblowing, (ii) si esporranno, in sintesi, i principi rilevanti contenuti nel Decreto Legislativo 10 marzo 2023, n. 24 ("d.lgs. 24/2023") e (iii) si descriverà la nuova procedura adottata dalla Società in conformità al d.lgs. 24/2023.

COS'É IL WHISTLEBLOWING

Per whistleblowing si intende l'azione di denuncia compiuta dal whistleblower.

Whistleblower è la persona che, lavorando all'interno di un'organizzazione, di un'azienda pubblica o

privata, si trova ad essere testimone di un comportamento illecito o irregolare e decide di segnalarlo all'azienda a cui appartiene o a soggetti terzi (ad esempio l'Autorità Giudiziaria), per porre fine a quel comportamento.

PRINCIPI GENERALI

1. Elementi di novità introdotti dal d.lgs. 24/2023

L'obiettivo della direttiva europea (attuata con il d.lgs. 24/2023) è quello di disciplinare la protezione dei whistleblowers, introducendo norme minime comuni per garantire la protezione delle persone che segnalano illeciti o irregolarità, creando canali di comunicazione sicuri, sia all'interno delle organizzazioni che all'esterno.

Il d.lgs. 24/2023 raccoglie in un unico testo normativo la disciplina del whistleblowing (chi può denunciare, quando e cosa), dei canali di segnalazione da utilizzare e delle tutele riconosciute ai segnalanti sia del settore pubblico che privato.

L'obiettivo è quello di incentivare l'effettuazione di segnalazioni di illeciti, per favorirne l'emersione. La trattazione che segue avrà ad oggetto una sintesi dei principi generali sanciti dal d.lgs. 24/2023 con riferimento alle società di diritto privato, qual è TSG Italia s.r.l.

2. Ambito soggettivo: i soggetti che possono segnalare

Sono legittimati a segnalare le persone che operano nel contesto lavorativo della Società:
- lavoratori dipendenti;
- lavoratori autonomi;
- collaboratori, liberi professionisti e consulenti;
- volontari e tirocinanti, retribuiti e non retribuiti;
- soci e persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto.

La disciplina normativa (con le relative tutele) si applica anche a segnalazioni che riguardano violazioni avvenute nell'ambito di un rapporto di lavoro poi terminato; nonché a coloro il cui rapporto non sia ancora iniziato, qualora le informazioni sulle violazioni siano state acquisite durante la selezione o in altre fasi precontrattuali o durante il periodo di prova.

3. Ambito oggettivo: l'oggetto della segnalazione

Possono essere segnalati tutti i comportamenti, gli atti o le omissioni che violano le disposizioni nazionali e dell'Unione Europea, che ledono l'interesse pubblico o l'integrità dell'ente privato, di cui i segnalanti siano venuti a conoscenza nel contesto lavorativo. In particolare, possono essere segnalati:
- le violazioni di disposizioni normative nazionali e, quindi, gli illeciti amministrativi, contabili, civili o penali, nonché le condotte rilevanti ai sensi del d.lgs. 8 giugno 2001, n. 231;
- le violazioni dei Modelli di Organizzazione e Gestione della Società e del Codice Etico comportamentale della Società;
- il mobbing, le molestie a sfondo sessuale, le molestie psicologiche, le discriminazioni in materia di parità di genere e qualsiasi violazione dei principi e delle regole poste a tutela dell'integrità e della dignità delle persone
- le violazioni di disposizioni normative europee in materia di appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo;

sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi; atti o omissioni che ledono gli interessi finanziari dell'Unione; atti o omissioni riguardanti il mercato interno (es. violazioni in materia di concorrenza e di aiuti di Stato); atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione.

-

Vengono in considerazione, quindi, condotte aventi rilevanza penale o che incidono sugli interessi strategici comunitari, ma anche condotte che si assumono poste in essere in violazione degli standard etici a cui la Società aderisce.

Sono, invece, escluse (i) le contestazioni, rivendicazioni o richieste legate a un interesse personale del segnalante o che attengono a rapporti individuali di lavoro o (ii) le violazioni la cui segnalazione è oggetto di procedure specifiche.

Con riferimento al punto (i) che precede, si evidenzia che il fatto segnalato deve attenere a pericoli o rischi che minacciano la Società nel suo complesso.

4. Contenuto della segnalazione

Le segnalazioni devono essere fondate su elementi di fatto precisi e concordanti.

La segnalazione può anche avere ad oggetto (i) le informazioni relative alle condotte volte ad occultare le violazioni sopra indicate e (ii) le attività illecite non ancora compiute ma che il segnalante ritenga ragionevolmente possano verificarsi, in presenza di elementi concreti, precisi e concordanti.

5. I canali di segnalazione

Le segnalazioni possono essere trasmesse attraverso:

a) il canale di segnalazione interno alla Società;
b) il canale esterno gestito dall'ANAC (Autorità Nazionale Anti-Corruzione);
c) la divulgazione pubblica tramite la stampa, o mezzi elettronici, o mezzi di diffusione in grado di raggiungere un numero elevato di persone;
d) la denuncia all'autorità giudiziaria o contabile.

La scelta del canale di segnalazione non è rimessa alla discrezione del whistleblower in quanto in via prioritaria viene favorito l'utilizzo del canale interno per tutte le segnalazioni.

Solo al ricorrere di determinate condizioni, è possibile effettuare una segnalazione all'ANAC o procedere con la divulgazione pubblica.

La denuncia all'autorità giudiziaria o contabile è, invece, ovviamente, sempre possibile, per i fatti che possono essere oggetto di denuncia.

A. Canale interno

Il canale interno di segnalazione è quello di cui la Società deve dotarsi (come, in effetti, si è dotata e come si vedrà nel paragrafo che segue "PROCEDURA DI GESTIONE DELLE SEGNALAZIONI: IL CANALE INTERNO").

Il canale interno può essere utilizzato per segnalare tutti gli illeciti o le irregolarità indicate al punto 3 che precede.

Il d.lgs. 24/2023 detta alcuni specifici principi in relazione alla gestione del canale interno di segnalazione:

- i soggetti del privato devono attivare canali di segnalazione, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione. Tali canali devono essere previsti nei modelli di organizzazione e gestione ex d.lgs. 231/2001;
- la gestione del canale di segnalazione deve essere affidata a una persona o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione, oppure ad un soggetto esterno, anch'esso autonomo e con personale specificamente formato;
- le segnalazioni possono essere effettuate in forma scritta, anche con modalità informatiche, oppure orale attraverso linee telefoniche o sistemi di messaggistica vocale o, su richiesta del segnalante, con un incontro diretto fissato entro un termine ragionevole;
- qualora la segnalazione sia presentata ad un soggetto diverso da quello indicato dalla procedura adottata dalla Società, essa dovrà essere trasmessa, entro sette giorni dal suo ricevimento, al soggetto competente, dando contestuale notizia della trasmissione alla persona segnalante.

Il d.lgs. 24/2023 individua, inoltre, una serie di regole che devono essere osservate per quanto concerne la gestione del canale interno da parte dell'ente.

La persona o l'ufficio a cui è affidata la gestione del canale di segnalazione interna devono:

a) rilasciare alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;
b) mantenere le interlocuzioni con la persona segnalante e possono richiedere a quest'ultima, se necessario, integrazioni;
c) dare diligente seguito alle segnalazioni ricevute;
d) fornire riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione;
e) mettere a disposizione informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni esterne. Le suddette informazioni sono esposte e rese facilmente visibili nei luoghi di lavoro, nonché accessibili alle persone che, pur non frequentando i luoghi di lavoro, intrattengono uno dei rapporti indicati al punto 2. Gli enti dotati di un proprio sito internet pubblicano le informazioni anche in una sezione dedicata del suddetto sito.

Il d.lgs. 24/2023, ferma l'applicazione del regolamento (UE) 2016/679, del decreto legislativo 30 giugno 2003, n. 196 e del decreto legislativo 18maggio 2018, n. 51, stabilisce alcune regole specifiche per la conservazione e il trattamento dei dati personali inerenti alla segnalazione, tra cui:

- i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente;
- devono essere adottate misure tecniche e organizzative da parte dei gestori dei canali di segnalazione idonei a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti di dati personali effettuati;
- le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a

decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione;

- se per la segnalazione si utilizza una linea telefonica registrata o un altro sistema di messaggistica vocale registrato, la segnalazione, previo consenso della persona segnalante, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante trascrizione integrale. In caso di trascrizione, la persona segnalante può verificare, rettificare o confermare il contenuto della trascrizione mediante la propria sottoscrizione.

Se per la segnalazione si utilizza una linea telefonica non registrata o un altro sistema di messaggistica vocale non registrato la segnalazione è documentata per iscritto mediante resoconto dettagliato della conversazione a cura del personale addetto. La persona segnalante può verificare, rettificare e confermare il contenuto della trascrizione mediante la propria sottoscrizione;

- quando, su richiesta della persona segnalante, la segnalazione è effettuata oralmente nel corso di un incontro con il personale addetto, essa, previo consenso della persona segnalante, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale. In caso di verbale, la persona segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione.

B. <u>Canale esterno – ANAC</u>

Il segnalante può effettuare una segnalazione all'ANAC quando ricorra una delle seguenti condizioni:

- nell'ambito del suo contesto lavorativo, non è stato attivato il canale di segnalazione interno oppure, anche se attivato, non è conforme;
- il segnalante ha già effettuato una segnalazione interna e non ha avuto seguito;
- il segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna alla Società, non sarebbe dato efficace seguito o determinerebbe condotte ritorsive;
- il segnalante ha fondati motivi di ritenere che la violazione possa costituire un pericolo imminente o palese per l'interesse pubblico.

La gestione e il funzionamento del canale esterno di segnalazione tramite ANAC è disciplinata nel d.lgs. 24/2023 e nei relativi provvedimenti attuativi.

C. <u>Canale esterno – Divulgazione pubblica</u>

Il segnalante può effettuare una divulgazione pubblica, alle seguenti condizioni:

- ha già effettuato una segnalazione interna ed esterna, ovvero direttamente esterna, e non è stato dato riscontro nei termini in merito alle misure previste o adottate per darvi seguito;
- ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per l'interesse pubblico;
- ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o non avere efficace seguito in ragione delle circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove, oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella stessa.

D. <u>Canale esterno – Denuncia all'Autorità Giudiziaria</u>

La denuncia all'Autorità Giudiziaria (o contabile) è sempre possibile, per i fatti che possono essere oggetto di denuncia (es. per tutti i reati è sempre possibile procedere con la denuncia all'Autorità Giudiziaria).

6. Tutele per il segnalante

Il d.lgs. 24/2023 prevede specifiche tutele per il soggetto che effettua le segnalazioni:

a) Tutela della riservatezza: Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.

   L'identità del segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.

   La riservatezza del segnalante è protetta (con determinati limiti) anche nel procedimento penale, nel procedimento dinnanzi alla Corte dei Conti e nel procedimento disciplinare avviato in relazione al fatto oggetto della segnalazione.

   Quando, in ogni caso, la rivelazione dell'identità del segnalante è indispensabile, è previsto che sia dato avviso alla persona segnalante.

b) Ritorsioni: È vietata ogni forma di ritorsione anche solo tentata o minacciata nei confronti del segnalante (ivi incluso il licenziamento, il demansionamento, il trasferimento di sede e ogni altra azione che comporti effetti negativi sui contratti di lavoro, quali sono, ad esempio, la mancata promozione, la retrocessione di grado, la sospensione della formazione, il mancato rinnovo del contratto in scadenza, nonché una serie di altre condotte afflittive, come la richiesta di sottoposizione ad accertamenti medici o psichiatrici, e azioni discriminatorie dalle quali conseguano pregiudizi economici o finanziari). Il segnalante può comunicare all'ANAC le ritorsioni che ritiene di avere subito. Gli atti di ritorsione sono nulli.

c) Inversioni dell'onere probatorio: sono previste specifiche regole processuali a tutela del soggetto segnalante nei procedimenti giudiziari, amministrativi, disciplinari in cui sia coinvolto;

d) è prevista l'istituzione presso l'ANAC di un elenco di enti che forniscono alle persone segnalanti misure di sostegno (informazioni, assistenza e consulenze a titolo gratuito sulle modalità di segnalazione e sulla protezione dalle ritorsioni);

e) sono previste specifiche cause di non punibilità in ambito penale, civile e amministrativo in favore del segnalante.

A determinate condizioni, è prevista l'estensione delle misure di protezione anche (i) ai facilitatori (ossia, una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata), (ii) alle persone del medesimo contesto lavorativo della persona segnalante e che sono legate ad essa da uno stabile legame affettivo o di parentela entro il quarto grado, (iii) ai colleghi di lavoro della persona segnalante che operano nel suo contesto lavorativo e che hanno con lui un rapporto abituale e corrente, (iv) nonché agli enti di proprietà del segnalante o per i quali le stesse persone lavorano nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

Il segnalante, nel rispetto della riservatezza, può essere sentito, anche mediante procedimento cartolare, attraverso l'acquisizione di osservazioni scritte e documenti.

7. **Perdita delle tutele per il segnalante**

Salve le cause di non punibilità specificamente previste dal d.lgs. 24/2023, quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave, le tutele non sono garantite e alla persona segnalante o denunciante è irrogata una sanzione disciplinare

8. **Sanzioni**

È prevista l'applicazione di sanzioni amministrative pecuniarie da parte dell'ANAC in relazione a specifiche fattispecie, come ad esempio, quando vengono commesse ritorsioni nei confronti del segnalante, quando è stato violato l'obbligo di riservatezza, quando non sono stati istituiti canali di segnalazione o in caso di omessa analisi delle segnalazioni.

9. **Segnalazioni anonime e dei fornitori/clienti**

Il d.lgs. 24/2023 non prevede alcuna disciplina con riferimento alla gestione delle segnalazioni anonime.

Parimenti non è prevista una disciplina specifica per eventuali segnalazioni di fornitori o clienti della Società. È, ovviamente, sempre possibile per gli enti pubblici o privati prevedere la facoltà per fornitori o clienti di effettuare segnalazioni tramite canali interni. Tuttavia, il fornitore o il cliente non potrà invocare – a suo favore – le tutele contemplate dal d.lgs. 24/2023.

L.2 PROCEDURA DI GESTIONE DELLE SEGNALAZIONI: IL CANALE INTERNO

1. **Premessa**

TSG Italia s.r.l. si è dotata di una specifica procedura di gestione delle segnalazioni in conformità a quanto previsto dal d.lgs. 24/2023 e all'art. 6, comma 2bis d.lgs. 231/2001 (ancora in vigore).

La Società nei prossimi paragrafi illustrerà, quindi, il funzionamento del canale interno da utilizzare per le segnalazioni e come queste ultime vengono gestite.

2. **Chi può attivare il canale interno di segnalazione**

Il canale interno di segnalazione può essere attivato:
- da tutti i soggetti indicati al punto 2 del paragrafo "PRINCIPI GENERALI";
- dai fornitori della Società;
- dai clienti della Società.

La Società intende incentivare anche i propri fornitori e clienti a segnalare gli illeciti e irregolarità riscontrate, così come identificate al punto 3 del paragrafo "PRINCIPI GENERALI".

La Società accetta anche le segnalazioni anonime. Le segnalazioni anonime determineranno l'apertura dell'istruttoria esclusivamente nell'ipotesi in cui il loro contenuto sia conforme a quanto indicato nel punto 6 che segue (con la sola esclusione di quanto indicato alla lettera a.). In caso di

segnalazione anonima, ovviamente non sarà possibile inviare la conferma di ricezione della segnalazione né tantomeno aggiornare il segnalante sulla gestione e sull'esito della segnalazione.

3. **Quando può essere attivato il canale interno di segnalazione**

Il canale interno di segnalazione può essere attivato allorché ricorrano i presupposti indicati al punto 3 del paragrafo "PRINCIPI GENERALI" e si disponga delle informazioni di cui al punto 4 del paragrafo "PRINCIPI GENERALI".

4. **Il Gestore della segnalazione**

Ci sono due soggetti preposti alla ricezione e alla disamina delle segnalazioni in TSG Italia:
(i) l'Organismo di Vigilanza ("ODV");
(ii) il Comitato Segnalazioni che è un Comitato interno al Comitato per la Parità di Genere ("Comitato Segnalazioni") ed è composto da un Consulente Legale Interno e dal Responsabile dell'Ufficio Risorse Umane.

Nel seguito ODV e Comitato Segnalazioni sono definiti anche come "Gestore Interno".

Qualora la segnalazione sia presentata ad un soggetto diverso dal Gestore Interno, essa verrà trasmessa, entro (7) sette giorni lavorativi dal suo ricevimento, all'ODV, dando contestuale notizia della trasmissione alla persona segnalante.
Come si dirà infra, è, inoltre, attivabile tramite Internet il canale di segnalazione messo a disposizione dal Gruppo TSG, che segue una procedura e regole specifiche sotto descritte.

5. **Mezzi: come può avvenire la segnalazione**

La Società si è dotata dei seguenti canali di comunicazione della segnalazione, idonei a preservare la riservatezza del soggetto segnalante:

Segnalazione scritta:

- Canale e-mail:
  È possibile inviare una segnalazione tramite e-mail a uno dei seguenti indirizzi:
  1. tsgitalia.odv@tsg-solutions.com;
  2. segnalazioni.paritadigenere@tsg-solutions.com.

La segnalazione deve essere inviata a uno solo degli indirizzi e-mail sopra indicati.

- Canale telematico:
  E' possibile inviare una segnalazione compilando i campi dell'apposito format presente nel sito internet della società, accessibile tramite il seguente link : https://www.tsg-solutions.com/it/whistleblowing-tsg/

  Nel compilare il format l'utente deve scegliere se inviare la segnalazione all'ODV o al Comitato Segnalazioni.

  Nel primo caso, la segnalazione verrà inviata e gestita dall'ODV.
  Nel secondo caso, la segnalazione verrà inviata e gestita dal Comitato Segnalazioni.

Segnalazione telefonica:

è possibile registrare un messaggio vocale al seguente numero di telefono: 01411881526.

La gestione dei messaggi vocali registrati sul numero di telefono avverrà ad opera del Comitato

Segnalazioni.

Il segnalante dovrà indicare nel messaggio vocale anche il suo nome e cognome e l'indirizzo e-mail di contatto. Il numero di telefono da cui viene effettuata la chiamata viene registrato.

Se la segnalazione non è anonima, il Comitato Segnalazioni trascriverà il messaggio vocale e lo invierà all'indirizzo e-mail del segnalante per avere conferma della correttezza della trascrizione.

Richiesta di fissare un incontro

Il segnalante può anche chiedere, avvalendosi dei suddetti canali di comunicazione (portale, e-mail o recapito telefonico), la fissazione di un incontro.

In tal caso, il segnalante indicherà se vuole fissare l'incontro con l'ODV o con il Comitato Segnalazioni.

L'incontro potrà essere organizzato presso la sede legale della Società oppure all'esterno, a seconda di quanto preferito dal segnalante.

Previo consenso del segnalante, il contenuto dell'incontro sarà verbalizzato. Il segnalante potrà verificare, rettificare e confermare il verbale dell'incontro.

Qualora il segnalante non autorizzi la trascrizione su verbale, non potrà essere garantita la corretta comprensione delle informazioni da parte del Gestore Interno.

Il canale del Gruppo TSG

È, inoltre, attivabile tramite Internet il canale telematico messo a disposizione dal Gruppo TSG per la gestione delle segnalazioni.

Le segnalazioni possono essere inviate tramite il "Portale per la segnalazione della corruzione nelle società del gruppo TSG", accessibile al seguente link: https://whistleblowing_italia.tsg-solutions.com.

Dopo la compilazione, il modulo verrà inviato al seguente indirizzo e-mail: whistleblowing@tsg-solutions.com.

Le segnalazioni saranno gestite dai Direttori del dipartimento legale e finanziario del Gruppo TSG, che saranno gli unici destinatari delle segnalazioni inviate.

6. **Contenuto**
   La segnalazione deve avere il contenuto indicato al punto 4 del paragrafo "PRINCIPI GENERALI".

   Occorrerà descrivere in modo dettagliato e minuzioso il fatto o l'omissione che si intende segnalare.

   Occorrerà, in particolare, indicare:
   a) le generalità di chi effettua la segnalazione, la qualifica professionale e i recapiti telefonici ed e-mail;
   b) luogo, data e orario, in cui si è verificato il fatto;
   c) generalità e qualifica professionale dei soggetti che hanno posto in essere i fatti

segnalati;

d) generalità e recapiti telefonici e/o e-mail dei soggetti che possono riferire sui fatti oggetto di segnalazione;
e) chiara e completa descrizione dei fatti oggetto di segnalazione e delle modalità con le quali si è venuto a conoscenza degli stessi;
f) ogni ulteriore informazione che possa fornire riscontro e conferma circa la sussistenza dei fatti segnalati.

Alla segnalazione occorrerà allegare tutta la documentazione comprovante l'illecito o l'irregolarità riscontrata. È possibile trasmettere file con estensione .jpg, .png e .pdf.

Le segnalazioni che non siano precise e circostanziate verranno archiviate e non daranno avvio al procedimento.

7. Procedimento di gestione della segnalazione

La segnalazione ricevuta dai canali di segnalazione sopra indicata viene gestita come segue:

Apertura del fascicolo

- Entro 7 (sette) giorni dalla ricezione della segnalazione, viene confermata al segnalante (se non anonimo) l'avvenuta ricezione della segnalazione.
- Il Gestore Interno assegnerà alla segnalazione un numero di riferimento e aprirà (i) un fascicolo cartaceo, che sarà conservato in armadio ad uso riservato del Gestore Interno e (ii) un fascicolo telematico che sarà conservato su apposito hard disk esterno conservato in armadio ad uso riservato del Gestore Interno.
- Entro 10 (dieci) giorni lavorativi dalla ricezione della segnalazione, si procede alla convocazione dei componenti dell'organo collegiale.
- Viene, quindi, comunicato al segnalante il numero assegnato al procedimento e vengono richieste al segnalante eventuali informazioni o documentazione integrativa.

Mancata integrazione e archiviazione

- Qualora la richiesta di integrazione documentale trasmessa dal Gestore Interno al segnalante rimanga senza riscontro, decorsi 20 (venti) giorni lavorativi, il Gestore Interno valuterà se i dati o le informazioni fornite siano sufficienti a consentire comunque una sommaria istruttoria. In difetto, procederà all'archiviazione della segnalazione.
- L'archiviazione della segnalazione per mancata integrazione verrà comunicata al segnalante. Il segnalante potrà in qualunque momento comunicare al Gestore Interno le informazioni e i documenti integrativi richiesti. L'integrazione comporterà l'apertura di una nuova pratica di segnalazione.

Istruttoria

- L'organo ricevente la segnalazione svolge direttamente tutte le attività volte alla verifica dei fatti oggetto della segnalazione. Può anche avvalersi del supporto e della collaborazione di strutture o funzioni aziendali o consulenti incaricati, quando per la loro natura, il luogo o la complessità risulti necessario un loro coinvolgimento.
- In conformità ai principi di imparzialità, il Gestore Interno effettua ogni attività ritenuta opportuna, inclusa l'audizione personale del segnalante, del segnalato e di eventuali altri soggetti che possono riferire sui fatti. Di tali incontri redige verbali da conservare nel fascicolo della procedura.

Chiusura del procedimento

- Entro 3 (tre) mesi dall'invio dell'avviso di ricevimento, il Gestore Interno trasmette al

segnalante un report sintetico contenente la descrizione delle attività compiute e l'esito.

- Il Gestore interno elabora, inoltre, una relazione dettagliata in ordine a tutte le attività svolte, allegando copia di tutti i verbali (nel rispetto dei doveri di riservatezza). Tale relazione deve essere inviata all'organo amministrativo. Qualora la segnalazione riguardi l'organo amministrativo, la segnalazione viene inviata all'organo di controllo (sindaco o collegio sindacale).

Conservazione dati

I dati acquisiti verranno conservati a cura della Società per 5 (cinque) anni dalla comunicazione dell'esito finale del procedimento o, in caso di procedura giudiziaria, sino all'esaurirsi dei rimedi giuridici esperibili avverso il giudicato.

8. Riservatezza

Il canale interno di segnalazione garantisce la riservatezza, in conformità a quanto indicato al punto 6 del paragrafo "PRINCIPI GENERALI" e a quanto previsto dal d.lgs. 24/2023.

La riservatezza del soggetto segnalante, dei soggetti menzionati e degli elementi di segnalazione viene garantita nel corso dell'istruttoria dal Gestore Interno, anche se la riservatezza non è stata espressamente richiesta dal soggetto segnalante.

La Società si impegna a garantire la riservatezza del soggetto segnalante che sia fornitore o cliente della Società per tutta la durata dell'istruttoria, salvo che i fatti segnalati debbano essere denunciati all'Autorità giudiziaria o contabile.

9. Divieto di atti ritorsivi

La Società si conforma a quanto previsto al punto 6 del paragrafo "PRINCIPI GENERALI" e al d.lgs. 24/2023 in relazione al divieto di applicazione di misure ritorsive.

Qualora il segnalante subisca l'applicazione di atti ritorsivi, dovrà informare tempestivamente il Gestore Interno.

10. Diffusione delle informazioni

La Società si è dotata di meccanismi di diffusione delle informazioni sulle procedure e sui presupposti per effettuare le segnalazioni interne ed esterne.

11. Sanzioni disciplinari

Potranno essere adottate, avuto riguardo alla gravità della condotta, sanzioni disciplinari nei confronti dei seguenti soggetti:

- soggetti segnalanti, quando sia pronuncia sentenza passata in giudicato per una delle fattispecie per le quali il d.lgs. 24/2023 prevede la perdita delle tutele;
- soggetti che pongono in essere atti ritorsivi nei confronti del soggetto segnalante, per motivi collegati, direttamente o indirettamente, alla segnalazione;
- soggetti che violano gli obblighi di riservatezza di cui al punto 6 del paragrafo "PRINCIPI GENERALI" e contemplati dal d.lgs. 24/2023.

SEZIONE M. REATI TRIBUTARI

M.1 I reati tributari (art. 25 quinquiesdecies) – Tipologia e caratteristiche

La Legge n. 157 del 2019, che ha convertito con alcune modifiche il Decreto legge n. 124 del 2019, ha introdotto nel catalogo dei reati presupposto previsti dal Decreto 231 alcune ipotesi di reati tri butari disciplinati dal Decreto legislativo n. 74 del 2000 (contenente la "Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto a norma dell'articolo 9 della legge 25 giugno 1999, n. 205").

L'introduzione dei nuovi reati presupposto trova giustificazione nell'esigenza manifestata sia dal legislatore nazionale che da quello comunitario di prevedere strumenti efficaci di contrasto all'evasione fiscale e, più in generale, alle frodi fiscali.

Considerate le particolarità dei reati introdotti e le conseguenze sanzionatorie, anche in via meramente cautelare, che possono derivarne, è innanzitutto necessario esplicitare con chiarezza tipologie e contenuti dei reati introdotti nonché precisare le aree/processi aziendali potenzialmente a rischio di commissione dei suddetti, prevedendo idonee ed efficaci misure di prevenzione e di controllo.

Il nuovo articolo 25 quinquiesdecies del Decreto prevede le seguenti ipotesi di reati tributari:

M.1.1 Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (articolo 2 commi 1 e 2 bis del D.LGS. n. 74/2000).

La norma punisce con la reclusione da quattro a otto anni chi, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative alle imposte sui redditi o sul valore aggiunto elementi passivi fittizi.
È prevista una circostanza attenuante se l'ammontare degli elementi passivi fittizi è inferiore ad euro 100.000; in tale ipotesi la pena è da un anno e sei mesi a sei anni di reclusione.

Il fatto di reato si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando essi sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria (ipotesi, quest'ultima, che non parrebbe riguardare i soggetti tenuti alle scritture contabili poiché l'omessa registrazione del documento impedisce la deduzione dell'elemento passivo dallo stesso attestato.)

Si ricorda che l'articolo 21 del D.P.R. n. 633/1972 stabilisce che, per ciascuna operazione imponibile, il soggetto che effettua la cessione del bene o la prestazione del servizio deve emettere fattura (anche elettronica), anche sotto forma di nota, conto, parcella e simili o, ferma restando la sua responsabilità, assicurare che la stessa sia emessa, per suo conto, dal cessionario o dal committente ovvero da un terzo.

Sono considerati rilevanti dall'articolo 2 del D.Lgs. n. 74/2000 anche gli altri documenti che, oltre alle fatture, hanno rilievo probatorio analogo alle medesime, in base alle norme tributarie (quali, a titolo meramente esemplificativo: le ricevute fiscali, gli scontrini fiscali, le note di credito e di addebito, i documenti che integrano o sostituiscono la fattura, la scheda carburante, i documenti di trasporto).

Tutti i documenti sopra evidenziati, perché possa sussistere il reato, debbono essere emessi per

operazioni inesistenti: a fronte cioè di operazioni che non siano state realmente effettuate in tutto o in parte, che indichino i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, ovvero che riferiscano l'operazione a soggetti diversi da quelli effettivi (art. 1, lett. a D.Lgs. n. 74/2000).

Pertanto, si distingue tra:

- inesistenza oggettiva: concerne operazioni (da intendersi come qualunque rapporto avente un contenuto economicamente rilevante) in tutto o in parte mai effettuate. Ad esempio, fattura emessa per consulenze/servizi mai prestati che consente alla Società di imputare il costo e abbassare il reddito dichiarato al fisco.
  L'inesistenza oggettiva può anche essere parziale come nell'ipotesi di sovrafatturazione e cioè di aumento fittizio di passività esistenti (tipico il caso delle cosiddette "fatture gonfiate").
- inesistenza soggettiva: è relativa ad operazioni, realmente effettuate, concluse tra soggetti in tutto o in parte diversi da quelli tra cui l'operazione avrebbe dovuto tenersi.

L'inesistenza soggettiva potrebbe sussistere, ad esempio, in un caso di appalto di lavori conferito a società, che procede a fatturare i lavori effettuati, ove poi risulti che la società non era operativa ed effettivamente esistente ed i lavoratori dalla stessa formalmente impiegati erano in realtà autonomi.

La Società appaltante, nell'esempio citato, può avere imputato dei costi e portato in detrazione l'IVA quando non avrebbe potuto farlo o avrebbe dovuto farlo a condizioni ed in quantità differente, ciò poiché la differenza soggettiva può incidere sulla misura dell'aliquota e, conseguentemente, sull'entità dell'imposta che il cessionario/committente può legittimamente detrarre.

Più in generale: "oggetto della repressione penale è ogni tipo di divergenza tra la realtà commerciale e la sua espressione documentale" (Cass. Pen., Sez. III, sentenza n. 28352 del 21.05.2013).

La condotta del reato ha struttura bifasica per la sua consumazione:

1. utilizzo di fatture o altri documenti per operazioni inesistenti;
2. indicazione di elementi passivi fittizi nelle dichiarazioni relative alle imposte sui redditi o sul valore aggiunto.

Per elementi passivi si intendono le componenti, espresse in cifra, che concorrono, in senso negativo, alla determinazione del reddito o delle basi imponibili rilevanti ai fini dell'applicazione delle imposte sui redditi o sul valore aggiunto e le componenti che incidono sulla determinazione dell'imposta dovuta (art. 1 lett. b) D.Lgs. n. 74/2000).

Per dichiarazioni si intendono anche le dichiarazioni presentate in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche o di sostituto d'imposta, nei casi previsti dalla legge (art. 1 lett. c) D.Lgs. n. 74/2000).

L'elemento soggettivo del reato è costituito dal dolo specifico: oltre alla consapevolezza e volontà di tenere le condotte sopra descritte è necessario il fine di evadere le imposte sui redditi o sul valore aggiunto (in tale dolo specifico, per espressa previsione normativa, rientra anche il fine di conseguire un indebito rimborso o di conseguire il riconoscimento di un inesistente credito di imposta come previsto dall'articolo 1 lett. d) del D.Lgs. n. 74/2000).

Riguardo ai fatti commessi da chi agisce in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche, il "fine di evadere le imposte" ed il "fine di sottrarsi al pagamento" si intendono riferiti alla società, all'ente o alla persona fisica per conto della quale si agisce (art. 1 lett. e) del D.Lgs n. 74/2000).

Il reato ha natura istantanea e si perfeziona con la presentazione della dichiarazione relativa alle imposte o sul valore aggiunto contenente elementi passivi fittizi. Per espressa previsione normativa (articolo 6 del D.Lgs. n. 74/2000) non è punibile il tentativo.

Per la Società, l'articolo 25 quinquiesdecies del Decreto prevede le seguenti sanzioni:

- sanzione pecuniaria da 100 a 500 quote;
- sanzione pecuniaria da 100 a 400 quote per l'ipotesi attenuata di cui al comma 2 bis dell'articolo 2 del D.Lgs. n. 74/2000 (se l'ammontare degli elementi passivi fittizi è inferiore ad euro 100.000).

Qualora la Società abbia conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

È altresì prevista la possibilità di applicare le sanzioni interdittive di:

- divieto di contrattare con la pubblica amministrazione, salvo che per ottenere prestazioni di un pubblico servizio;
- esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi.

Si applica, da ultimo, la confisca del prezzo o del profitto del reato, che può consistere anche in risparmio di spesa. La confisca può essere preceduta dal sequestro preventivo, anche per equivalente, ai sensi degli articoli 19 e 53 del Decreto. Il sequestro per equivalente ha ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato (si veda il successivo paragrafo 1.1).

M.1.2 Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000)

Il reato in questione punisce con la reclusione da tre a otto anni chi, al di fuori delle ipotesi previste dall'articolo 2 (quindi al di fuori dei casi di utilizzo di fatture o altri documenti per operazioni in tutto o in parte inesistenti) 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, indica in una delle dichiarazioni relative alle imposte sui redditi o sul valore aggiunto elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi.

Perché la condotta evidenziata possa assumere rilevanza penale, devono sussistere, congiuntamente, le seguenti condizioni:

a) l'imposta evasa deve essere superiore, con riferimento a taluna delle singole imposte, a Euro 30.000;
b) poi, l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, deve essere superiore al 5% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, superiore a Euro 1.500.000, ovvero l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta deve essere superiore al 5% dell'ammontare dell'imposta medesima o comunque a Euro 30.000.

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 (ipotesi, quest'ultima, che non riguarderebbe i soggetti tenuti alle scritture contabili

poiché l'omessa registrazione del documento impedisce la deduzione dell'elemento passivo dallo stesso attestato.)

La condotta penalmente rilevante si articola in due fasi.

La prima fase consiste nella condotta fraudolenta che, a sua volta può concretizzarsi nel:

1. compiere operazioni simulate oggettivamente o soggettivamente;
2. utilizzare documenti falsi;
3. impiegare mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria.

La seconda fase della condotta consiste poi, per effetto di quanto sopra, nell'indicare elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, con l'ulteriore precisazione che debbono altresì sussistere i requisiti quantitativi sopra elencati.

Per operazioni simulate oggettivamente o soggettivamente devono intendersi quelle operazioni apparenti poste in essere con la volontà di non realizzarle in tutto o in parte (simulazione oggettiva) ovvero operazioni riferite a soggetti fittiziamente interposti (simulazione soggettiva).
Da tali operazioni sono espressamente escluse quelle previste dall'articolo 10 bis della Legge 212 del 2000 (il cosiddetto "Statuto del Contribuente") in materia di abuso del diritto ed elusione fiscale: sono cioè escluse dalla rilevanza penale quelle operazioni prive di sostanza economica che, pur nel rispetto formale delle norme fiscali, realizzano essenzialmente vantaggi fiscali indebiti e sono prive di connotazione fraudolenta e più in generale decettiva (art. 1 lett. gbis del D.Lgs. n. 74/2000).

Per meglio comprendere la differenza, si richiama quanto statuito dalla Corte di cassazione, Sez. III, con la sentenza n. 38016 del 21.04.2017: "In tema di violazioni finanziarie, l'istituto dell'abuso del diritto di cui all'art. 10-bis l. n. 212 del 2000 – che, per effetto della modifica introdotta dall'art. 1 del d.lg. n. 128 del 2015, esclude ormai la rilevanza penale delle condotte ad esso riconducibili – ha applicazione solo residuale rispetto alle disposizioni concernenti comportamenti fraudolenti, simulatori o comunque finalizzati alla creazione e all'utilizzo di documentazione falsa di cui al d.lg. n. 74 del 2000, cosicché esso non viene mai in rilievo quando i fatti in contestazione integrino le fattispecie penali connotate da tali elementi costitutivi."; e da Cass. Pen., Sez. III, sentenza n. 40272 del 1.10.2015: "In tema di violazioni finanziarie, l'istituto dell'abuso del diritto di cui all'art. 10-bis l. 27 luglio 2000, n. 212, che, per effetto della modifica introdotta dall'art. 1 del d.lg. 5 agosto 2015, n. 128, esclude ormai la rilevanza penale delle condotte ad esso riconducibili, ha applicazione solo residuale rispetto alle disposizioni concernenti comportamenti fraudolenti, simulatori o comunque finalizzati alla creazione e all'utilizzo di documentazione falsa di cui al d.lg. 10 marzo 2000, n. 74, cosicché esso non viene mai in rilievo quando i fatti in contestazione integrino le fattispecie penali connotate da tali elementi costitutivi.".

Per altri mezzi fraudolenti (art. 1 lett. g ter del D.Lgs. n. 74/2000) si devono intendere condotte artificiose attive nonché omissive realizzate in violazione di uno specifico obbligo giuridico, che determinano una falsa rappresentazione della realtà (rientrano in tale categoria, ad esempio, la simulazione di negozi giuridici, l'utilizzazione di un magazzino occulto).

L'articolo 3 del D. Lgs. n. 74/2000 prevede espressamente che non costituiscono mezzi fraudolenti, rilevanti per la fattispecie penale, 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, proprio perché caratterizzati da assenza di connotazioni fraudolente e potenzialmente riconducibili a mere violazioni di carattere formale.

Si ricorda che i mezzi fraudolenti debbono essere idonei ad ostacolare l'accertamento e ad indurre

in errore l'amministrazione finanziaria.

L'elemento psicologico del reato è costituito dal dolo specifico, cioè la consapevolezza e volontà di tenere le condotte descritte dalla norma oltre al fine di evadere le imposte sui redditi o sul valore aggiunto (in tale dolo specifico, per espressa previsione normativa, rientra anche il fine di conseguire un indebito rimborso o di conseguire il riconoscimento di un inesistente credito di imposta come previsto dall'articolo 1 lett. d) del D.Lgs. n. 74/2000).

Oggetto del dolo, secondo parte della dottrina e della giurisprudenza, devono essere anche le soglie di punibilità previste dalla norma: chi agisce deve cioè rappresentarsi e volere, anche solo a livello di accettazione del rischio, il superamento delle stesse.

Per espressa previsione normativa (articolo 6 del D.Lgs. n. 74/2000), il delitto non è punibile a titolo di tentativo.

La sanzione pecuniaria per la Società, in caso di commissione del reato oggetto di esame, è da 100 a 500 quote.

Se la Società ha acquisito un profitto di rilevante entità, la pena è aumentata di un terzo.

È altresì prevista la possibilità di applicare le sanzioni interdittive di:

- divieto di contrattare con la pubblica amministrazione, salvo che per ottenere prestazioni di un pubblico servizio;
- esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi.

Si applica, da ultimo, la confisca del prezzo o del profitto del reato, che può consistere anche in un risparmio di spesa. La confisca può essere preceduta dal sequestro preventivo, anche per equivalente, ai sensi degli articoli 19 e 53 del Decreto. Il sequestro per equivalente ha ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato (si veda il successivo paragrafo 1.1).

M.1.3 Emissione di fatture o altri documenti per operazioni inesistenti (articolo 8, commi 1 e 2 bis del D.Lgs. n. 74/2000)

Il delitto in questione si ravvisa nella condotta di chi, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

L'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso dello stesso periodo di imposta si considera come un solo reato.

Il delitto è punito con la reclusione da quattro a otto anni.

È prevista una ipotesi attenuata (pena della reclusione da un anno e sei mesi a sei anni) se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a Euro 100.000.

Quanto alle definizioni rilevanti per la fattispecie di reato di cui all'articolo 8, si rimanda alla descrizione del delitto previsto dall'articolo 2 del D.Lgs. n. 74/2000 poiché la fattispecie in questione costituisce l'ipotesi speculare rispetto a quella di utilizzo di fatture o altri documenti per operazioni

inesistenti.

Si precisa che il termine emissione concerne le fatture mentre il termine rilascio riguarda gli altri documenti quali ricevute fiscali etc.

Perché si possa ritenere realizzata la condotta di reato è comunque indispensabile che il documento esca dalla sfera di fatto e di diritto del cedente mediante consegna o spedizione al terzo, potenziale utilizzatore che non abbia partecipato alla perpetrazione del falso.

Il dolo è specifico, è cioè necessaria la consapevolezza e volontà della condotta descritta ed il fine di consentire a terzi l'evasione delle imposte o del valore aggiunto (in tale dolo specifico, per espressa previsione normativa, rientra anche il fine di conseguire un indebito rimborso o di conseguire il riconoscimento di un inesistente credito di imposta come previsto dall'articolo 1 lett. d) del D.Lgs. n. 74/2000).

In relazione a tale fattispecie di reato, è da evidenziare come il fine di evasione richiesto per l'integrazione del medesimo non debba essere esclusivo ma si possa conciliare con altri scopi che possono qualificare, nei fatti, l'interesse e/o il vantaggio per la Società emittente quale presupposto della responsabilità d'impresa.
Si pensi al caso in cui l'emissione di fatture per operazioni inesistenti sia ricollegabile all'accordo con cui il ricevente rimborsi, almeno in parte, quanto l'emittente ha versato a titolo di imposta sul valore aggiunto o, in generale, a pagare un corrispettivo per l'emissione della fattura stessa.

Si ricorda che, ai sensi dell'articolo 9 del D.Lgs. n. 74/2000, è escluso il concorso di persone tra l'emittente di fatture punito ai sensi dell'articolo 8 e chi si avvale di fatture per operazioni inesistenti punito dall'articolo 2.

La sanzione per la società è da 100 a 500 quote e per l'ipotesi attenuata (se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a Euro 100.000), da 100 a 400 quote.

Se la Società ha acquisito un profitto di rilevante entità, la pena è aumentata di un terzo.

È altresì prevista la possibilità di applicare le sanzioni interdittive di:

- divieto di contrattare con la pubblica amministrazione, salvo che per ottenere prestazioni di un pubblico servizio;
- esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi.

Si applica, da ultimo, la confisca del prezzo o del profitto del reato, che può consistere anche in un risparmio di spesa. La confisca può essere preceduta dal sequestro preventivo, anche per equivalente, ai sensi degli articoli 19 e 53 del Decreto. Il sequestro per equivalente ha ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato (si veda il successivo paragrafo 1.1).

M.1.4 Distruzione od occultamento di documenti contabili (articolo 10 D.Lgs. n 74/2000)

Il delitto in questione punisce con la reclusione da tre a sette anni, salvo che non sia configurabile un'ipotesi di reato più grave, chi al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire a terzi l'evasione, occulta, distrugge 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 d'affari.

La condotta di occultamento o di distruzione non è però sufficiente perché possa ritenersi integrato il reato. È infatti necessario che tale condotta abbia impedito la ricostruzione dei redditi o del volume d'affari.

Secondo l'orientamento prevalente della giurisprudenza, recentemente ribadito dalla sentenza della Corte di cassazione, Sezione III, n. 37348 del 12/03/2019, il reato disaminato sussiste anche nell'ipotesi in cui sia stato possibile egualmente ricostruire le operazioni effettuate dal contribuente, poiché è sufficiente che la condotta abbia reso, se non impossibile, solamente più difficoltosa l'attività di verifica fiscale.

Il dolo è specifico: devono cioè sussistere la rappresentazione e volizione di occultare o distruggere le scritture o i documenti di cui è obbligatoria la conservazione ed il fine di evadere le imposte sui redditi o sul valore aggiunto (in tale dolo specifico, per espressa previsione normativa, rientra anche il fine di conseguire un indebito rimborso o di conseguire il riconoscimento di un inesistente credito di imposta come previsto dall'articolo 1 lett. d) del D.Lgs. n. 74/2000) oppure di consentire a terzi l'evasione.

La Società è punita con la sanzione pecuniaria da 100 a 400 quote.

Se la Società ha acquisito un profitto di rilevante entità, la pena è aumentata di un terzo.

È altresì prevista la possibilità di applicare le sanzioni interdittive di:
- divieto di contrattare con la pubblica amministrazione, salvo che per ottenere prestazioni di un pubblico servizio;
- esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi.

Si applica, da ultimo, la confisca del prezzo o del profitto del reato, che può consistere anche in un risparmio di spesa. La confisca può essere preceduta dal sequestro preventivo, anche per equivalente, ai sensi degli articoli 19 e 53 del Decreto. Il sequestro per equivalente ha ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato (si veda il successivo paragrafo 1.1).

M.1.5 Sottrazione fraudolenta al pagamento delle imposte (art. 11 D.Lgs. n. 74/2000)

L'articolo 11 del D.Lgs. 74/2000 prevede due differenti ipotesi di reato.

In primo luogo è punito con la reclusione da sei mesi a quattro anni chi, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovverosia di interessi o sanzioni amministrative relativi alle suddette imposte di ammontare complessivo (cioè per imposte, interessi e sanzioni amministrative) superiore a Euro 50.000, aliena simulatamente o compie altri atti fraudolenti sui propri o altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva.

La pena è aumentata se l'ammontare delle imposte, sanzioni ed interessi è superiore ad Euro 200.000. Perché sussista il delitto in questione non è necessario che vi sia una procedura di riscossione in atto ma è sufficiente che vengano posti in essere gli atti indicati nella norma al fine

di sottrarsi al pagamento.

La valutazione della idoneità della condotta a rendere in tutto o in parte inefficace la procedura di riscossione coattiva deve essere effettuata ex ante, riportandosi cioè al momento in cui è realizzata la condotta stessa e senza che sia necessario il verificarsi dell'evento (inefficacia della procedura di riscossione coattiva).

La condotta può estrinsecarsi in una alienazione simulata o in altri atti fraudolenti sui propri beni o su quelli altrui.

Si tratta di atti che, quand'anche effettuati con negozi giuridici legittimi, comportano un fittizio impoverimento e riduzione del patrimonio del debitore-contribuente, allo scopo di sottrarsi al pagamento delle imposte dovute.

Si possono indicare, a titolo di esempio: contratti simulati di affitto d'azienda o di cessione di crediti, intestazioni fiduciarie di beni, costituzione di un trust; cessione simulata di avviamento commerciale; pluralità di trasferimenti immobiliari in rapida successione; messa in atto di più operazioni di cessioni di aziende e di scissioni societarie simulate finalizzate a conferire i beni ai nuovi soggetti societari.

Il dolo è specifico: consapevolezza dell'esistenza di un debito nei confronti dell'erario complessivamente superiore ad Euro 50.000 e coscienza e volontà di realizzare le condotte descritte, unitamente alla rappresentazione della concreta idoneità di pregiudicare la procedura di riscossione coattiva e finalità di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovverosia di interessi o sanzioni amministrative relativi alle suddette imposte per l'importo complessivo superiore ad Euro 50.000.

L'articolo 11, al comma 2, punisce altresì con la reclusione da sei mesi a quattro anni, chi, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della transazione fiscale, elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad Euro 50.000.

Anche in tale caso la pena è aumentata se l'ammontare complessivo è superiore ad Euro 200.000.

La seconda ipotesi prevista dal citato articolo 11 concerne il caso della transazione fiscale nell'ambito della crisi d'impresa e individua appunto, quale soggetto attivo della condotta, l'imprenditore in stato di crisi o l'amministratore di una società in crisi che sottoscrive la proposta di transazione fiscale (si vedano in particolare gli articoli 63 e 88 del D.Lgs. n. 14/2019 "Codice della crisi d'impresa").

Si tratta di un reato tramite il quale il soggetto, rappresentando passivi inferiori a quelli reali, tende ad indurre in errore l'Amministrazione finanziaria spingendola a scelte transattive cui altrimenti non avrebbe aderito.

Anche in tale caso l'elemento soggettivo è costituito dal dolo specifico, dovendo sussistere non solo la consapevolezza e volontà di porre in essere la condotta evidenziata ma altresì lo scopo, che non deve necessariamente concretizzarsi, di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori.

In entrambi i casi, la sanzione pecuniaria per la Società è modulata da 100 a 400 quote.

Se il profitto derivante alla Società dal reato è di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

È altresì prevista la possibilità di applicare le sanzioni interdittive di:

- divieto di contrattare con la pubblica amministrazione, salvo che per ottenere prestazioni di un pubblico servizio;
- esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi.

Si applica, da ultimo, la confisca del prezzo o del profitto del reato, che può consistere anche in un risparmio di spesa. La confisca può essere preceduta dal sequestro preventivo, anche per equivalente, ai sensi degli articoli 19 e 53 del Decreto. Il sequestro per equivalente ha ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato (si veda il successivo paragrafo M.2).

M.2 La confisca del prezzo o del profitto del reato

In tutte le ipotesi di reato presupposto indicate nell'articolo 25 quinquiesdecies del Decreto sopra esaminate è altresì prevista l'applicazione della confisca del prezzo o del profitto del reato.

La nozione di prezzo del reato (da intendersi come il compenso o il corrispettivo ricevuto o promesso per indurre, determinare o istigare qualcuno a commettere un reato) è di difficile applicazione ai reati tributari. Può sussistere tale categoria, ad esempio e secondo la dottrina, nell'ipotesi del reato di distruzione od occultamento di scritture contabili, quando sia commesso per consentire a terzi l'evasione dietro corrispettivo, oppure nel caso di emissione di fatture per operazioni inesistenti sempre al fine di consentire a terzi l'evasione e vi sia un corrispettivo per la realizzazione di tali condotte.
Ben più evidente è la rilevanza della locuzione profitto del reato, da intendersi quale vantaggio di natura economica o, più in generale, nel beneficio aggiuntivo di natura patrimoniale che si ricava per effetto della commissione del reato.

Nella nozione di profitto deve essere ricompreso anche il cosiddetto risparmio di spesa dovuto al mancato pagamento dell'imposta dovuta, mancato pagamento che si traduce in un risparmio o in un arricchimento futuro nella forma di indebito rimborso.

Secondo quanto previsto dall'articolo 19 del Decreto 231, la confisca può avere ad oggetto anche somme di denaro, beni o altre utilità di valore equivalente al profitto o la prezzo del reato qualora non sia possibile procedere alla confisca del medesimo: si tratta della confisca per equivalente.

Prima dell'accertamento definitivo del reato e, di conseguenza, dell'applicazione della confisca, l'autorità giudiziaria può procedere ad applicare la misura cautelare reale del sequestro preventivo finalizzato alla confisca che può operare anche per equivalente e cioè sui beni, denaro o altre utilità di valore equivalente al prezzo o al profitto del reato qualora questo non sia direttamente sequestrabile.

È pertanto evidente come la puntuale mappatura delle aree a rischio di commissione di uno o più dei reati tributari nonché la predisposizione di efficaci misure di prevenzione del rischio di commissione dei medesimi, costituiscano adempimenti imprescindibili anche per evitare l'applicazione in via cautelare di misure, interdittive e/o patrimoniali, che possono avere un impatto di vasta portata sulla realtà societaria.

M.3 La Direttiva dell'Unione Europea sulla protezione degli interessi finanziari

La Direttiva dell'Unione Europea n. 1371 del 2017 stabilisce che gli Stati membri debbono adottare misure per sanzionare penalmente le frodi che ledano gli interessi finanziari dell'Unione Europea. In particolare, nel nostro ordinamento è prevista l'introduzione della responsabilità degli Enti e delle Società per ulteriori reati tributari (dichiarazione infedele, omessa dichiarazione, indebita compensazione) commessi anche in parte sul territorio di un altro Stato membro al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore ad Euro 10.000.000.

In relazione ai delitti previsti dagli articoli 2, 3 e 4 del D.Lgs. n. 74/2000 è prevista l'introduzione della punibilità del tentativo, quando cioè gli atti diretti a commetterli siano compiuti anche nel territorio di un altro Stato membro dell'Unione Europea, al fine di evadere l'imposta sul valore aggiunto per un valore complessivo non inferiore ad Euro 10.000.000.

Le regole di comportamento ed i presidi di prevenzione e controllo elaborati e richiamati nella presente parte speciale tengono già in considerazione i futuri profili normativi sopra evidenziati.

M.4 Aree potenzialmente a rischio di commissione dei reati di cui all'Articolo 25 quinquiesdecies Decreto 231

L'attività di mappatura delle aree/processi aziendali potenzialmente a rischio di commissione di uno o più dei reati presupposto di cui all'articolo 25 quinquiesdecies del Decreto 231 ha tenuto nella debita considerazione la circostanza che le modalità di realizzazione e gli effetti dei suddetti possono interessare numerosi settori, processi ed attività della Società, non essendo possibile circoscriverli in un settore unico e specifico.

Le aree potenzialmente a rischio di commissione dei reati della presente parte speciale sono anche quelle ricomprese in altre parti speciali del presente Modello (come quelle previste in relazione alle parti speciali finalizzate alla prevenzione dei delitti contro la Pubblica Amministrazione, in materia di reati societari e prevenzione della ricettazione, riciclaggio e autoriciclaggio) e i presidi ed i controlli ivi predisposti ben possono dispiegare i propri virtuosi effetti preventivi anche in relazione alle fattispecie tributarie di recente introduzione.

Di seguito vengono indicate le aree ed i processi aziendali potenzialmente a rischio di commissione dei reati presupposto previsti dall'articolo 25 quinquiesdecies del Decreto 231, tenuto conto che debbono ricomprendersi anche le attività/processi di supporto alle stesse:

- Supply chain e Approvvigionamento/acquisti (beni/servizi);
- Marketing e Vendita;
- Gestione rapporti con clienti;
- Determinazione e gestione listino prezzi;
- Scelta e monitoraggio fornitori;
- Rapporti con fornitori;
- Gestione appalti;
- Gestione contabile ed adempimenti societari (attività di registrazione, conservazione e controllo dei documenti contabili; controllo di gestione; redazione del bilancio, delle relazioni e delle comunicazioni rivolte ai soci, alla società di revisione e/o a terzi e riguardanti la situazione patrimoniale, finanziaria ed economica della Società);
- Adempimenti di bilancio;
- Gestione adempimenti fiscali;

- Ciclo passivo ed attivo;
- Gestione flussi finanziari;
- Gestione fondi della Società;
- Risorse umane;
- Rapporti infragruppo (flussi finanziari, rapporti giuridici);
- Area attinente alla corporate governance ed alla direzione generale (ad esempio l'approvazione delle delibere del Consiglio di Amministrazione nonché la loro attuazione da parte dei soggetti incaricati, in conformità allo statuto e alle norme vigenti nonché nel rispetto del Codice etico e del Modello di organizzazione e gestione nonché delle procedure ed istruzioni operative da questo richiamate);
- Rapporti con intermediari finanziari;
- Omaggi, Spese di rappresentanza;
- Rapporti con società di revisione e collegio sindacale;
- Trasferte;
- Sponsorizzazioni (se previste);
- Rapporti contrattuali con terzi e eventuali accordi transattivi;
- Atti di liberalità.

M.5 I destinatari della parte speciale

Sono Destinatari della presente parte speciale gli organi sociali, gli amministratori, il direttore generale, i dirigenti, i dipendenti e tutti coloro che operano nelle aree delle attività/processi a rischio, oltre ai soggetti che rivestono la qualifica di legale rappresentante nonché i professionisti eventualmente incaricati e che operino nelle medesime aree/processi aziendali.
I "Responsabili delle aree/attività a rischio di reato" sono i soggetti Responsabili delle funzioni all'interno delle quali vengono svolte operazioni potenzialmente a rischio di reato.

Sono, altresì, destinatari della presente parte speciale le figure specificamente individuate nelle procedure e istruzioni di lavoro contenute nei sistemi di gestione adottati dalla Società e integralmente richiamati dal presente Modello.

M.6 Principi generali di gestione

Nella gestione delle attività nelle aree/processi a rischio evidenziati, la società opera in modo da assicurare:

a. piena trasparenza nella gestione dei dati contabili e nella circolazione delle informazioni;
b. chiara attribuzione di ruoli a persone con adeguate esperienze e competenze attraverso il ricorso a deleghe e procure che individuano con chiarezza poteri e relative responsabilità dei destinatari delle medesime;
c. tracciabilità e archiviazione puntuale (per iscritto su supporto cartaceo e/o informatico) di tutte le operazioni effettuate nelle aree/processi a rischio (ad esempio documenti a supporto di beni/servizi acquistati e/o venduti; gestione del magazzino e delle giacenze ivi presenti; adempimenti di natura fiscale);
d. trasparenza e correttezza nella selezione dei contraenti, nel rispetto delle procedure operative e delle istruzioni di lavoro già esistenti, con raffronto dei preventivi di spesa, fatti salvi casi specificamente previsti e motivati, sottoposti dai potenziali contraenti e valutazione, con particolare riferimento alla fornitura di servizi, di tutti gli elementi posti a giustificazione dell'offerta e che ne qualifichino la natura in rapporto alle esigenze concrete;
e. trasparenza e verificabilità dei prezzi applicati a beni/servizi mediante ricorso a listini o a

verifiche del prezzo medio applicato nel settore di riferimento, con giustificazione e documentazione di eventuali scostamenti da tali parametri di riferimento;

f. predisposizione di adeguati meccanismi di controllo e di verifica, anche a campione, sul corretto adempimento degli obblighi di legge e della gestione delle attività/processi a rischio di commissione dei reati (ad esempio mediante la verifica dei prezzi applicati, la presenza della documentazione prevista a supporto delle operazioni effettuate, della documentazione attestante l'adempimento degli obblighi di natura fiscale).

Tutte le entrate e le uscite di cassa e di banca debbono essere giustificate da idonea documentazione, a fronte di beni e servizi realmente erogati o ricevuti, con la raccolta della documentazione attestante l'avvenuta ricezione del bene/servizio e di fattura emessa dal fornitore.

Le assunzioni di personale debbono essere effettuate sulla base di specifiche esigenze ed autorizzate secondo i vigenti poteri di rappresentanza e di firma sociale. Mediante il ricorso alle modalità indicate nella parte Speciale H (relativa alla prevenzione dei reati afferenti l'impiego di cittadini di Paesi terzi il cui soggiorno è irregolare) è garantita la verifica della regolarità dell'assunzione di cittadini extra comunitari in possesso di documenti di soggiorno in corso di validità.

Le consulenze e gli incarichi professionali debbono essere assegnati a fronte di specifiche esigenze ed autorizzate secondo i vigenti poteri di rappresentanza e di firma.

I rapporti intrattenuti con gli Istituti bancari, con i clienti, i fornitori e le altre società del Gruppo debbono essere verificati attraverso lo svolgimento di periodiche riconciliazioni.

In materia di appalti e, più in generale, di rapporti contrattuali con soggetti terzi la verifica dell'esistenza effettiva del soggetto appaltatore o del terzo contraente avviene anche in conformità alle procedure previste nel sistema di gestione della tutela della salute e sicurezza nei luoghi di lavoro e del sistema di gestione ambientale (gestione appalti e verifica dell'idoneità tecnico professionale, gestione rifiuti).

M.7 Il transfer pricing

Particolare attenzione deve essere prestata al cosiddetto meccanismo del "transfer pricing" e cioè all'operazione infragruppo (ad esempio se realizzata tra società ubicate in Stati diversi con differente regime fiscale) caratterizzata da transazioni commerciali di cessioni di beni o servizi.

Al fine di impedire comportamenti illeciti e distorsivi, quali ad esempio l'applicazione di un prezzo di trasferimento differente da quello praticato tra soggetti del tutto indipendenti nel mercato libero, l'articolo 110 comma 7del D.P.R. n. 917 del 1986 prevede che: " I componenti del reddito derivanti da operazioni con società non residenti nel territorio dello Stato, che direttamente o indirettamente controllano l'impresa, ne sono controllate o sono controllate dalla stessa società che controlla l'impresa, sono determinati con riferimento alle condizioni e ai prezzi che sarebbero stati pattuiti tra soggetti indipendenti operanti in condizioni di libera concorrenza e in circostanze comparabili, se ne deriva un aumento del reddito".

Se, invece, derivi una diminuzione del reddito, il parametro di riferimento deve essere il "prezzo secondo condizioni ed ai prezzi che sarebbero stati pattuiti tra soggetti indipendenti operanti in condizioni di libera concorrenza e in circostanze comparabili" quando ricorra una delle seguenti condizioni:

- in esecuzione degli accordi conclusi con le autorità competenti degli Stati esteri a seguito delle procedure amichevoli previste dalle convenzioni internazionali contro le doppie

imposizioni sui redditi o dalla Convenzione relativa all'eliminazione delle doppie imposizioni in caso di rettifica degli utili di imprese associate, con atto finale e dichiarazioni, fatta a Bruxelles il 23 luglio 1990, resa esecutiva con legge 22 marzo 1993, n. 99;
- a conclusione dei controlli effettuati nell'ambito di attività di cooperazione internazionale i cui esiti siano condivisi dagli Stati partecipanti;
- a seguito di istanza da parte del contribuente, a fronte di una rettifica in aumento che:
    1. sia stata resa definitiva;
    2. sia stata operata nel rispetto del principio di libera concorrenza;
    3. sia stata esercitata da uno Stato con il quale è in vigore una Convenzione contro le doppie imposizioni che preveda un adeguato scambio di informazioni.

La Società assicura il rispetto del parametro normativo per il transfer pricing, costituito dalle "condizioni e dai prezzi che sarebbero stati pattuiti tra soggetti indipendenti operanti in condizioni di libera concorrenza e in circostanze comparabili", osservando il dettato della disciplina di riferimento nazionale e comunitaria ed ispirandosi alle Linee Guida dell'OCSE sui prezzi di trasferimento.

Le aree di interesse per le transazioni infragruppo sono, in particolare:
- vendita di beni;
- acquisto di beni per la distribuzione in Italia;
- servizi infragruppo;
- transazioni residuali (afferenti, ad esempio, il riaddebito di specifiche spese sostenute per conto di altre società del Gruppo).

La Società, per ciascun ambito, provvede alla archiviazione di tutta la documentazione relativa che è a disposizione degli organi societari e degli enti/autorità competenti per i controlli che si rendessero necessari.

M.8 Il cash pooling

La società è parte di un accordo di cash pooling stipulato a livello di Gruppo.
Come noto, il contratto di cash pooling consiste nell'accentrare in capo ad un unico soggetto giuridico la gestione delle disponibilità finanziarie di un gruppo societario, allo scopo di gestire la tesoreria aziendale in riferimento ai rapporti tra le società aderenti al gruppo e gli istituti di credito ed ha la finalità di evitare squilibri finanziari per le singole società attraverso una gestione unitaria della situazione finanziaria del gruppo.
Il contratto stipulato dalla Società disciplina con trasparenza i rapporti intercorrenti tra le parti definendone rispettive competenze e poteri con il fine di regolamentare e giustificare i movimenti di liquidità dai conti correnti delle singole società al conto corrente accentrato.

M.9 Principi di comportamento

I Destinatari della presente parte speciale, nello svolgimento di attività nelle aree/processi a rischio di commissione dei reati previsti dalla presente Parte speciale devono:
- agire in conformità alla normativa vigente, alle regole previste dal Modello di gestione, organizzazione e controllo e dal Codice Etico e dalle procedure operative e istruzioni di lavoro;
- assicurare il pieno rispetto dei requisiti di trasparenza, verificabilità e documentabilità nella gestione delle risorse finanziarie e, più in generale, nell'esercizio dell'attività della Società e nelle transazioni finanziarie, garantendo la piena corrispondenza tra documentazione e

relativi acquisiti/vendite effettuati e l'effettiva esistenza delle consulenze e, più in generale, dei servizi acquistati o forniti;
- rispettare il principio di segregazione delle funzioni tra chi autorizza e gestisce le operazioni, chi effettua i pagamenti, chi procede alla registrazione contabile delle suddette operazioni ed alla conseguente archiviazione della documentazione;
- rispettare la suddivisione dei poteri conferiti con deleghe e procure;
- attenersi alla disciplina prevista nel sistema integrato di gestione della qualità e nei sistemi di gestione in materia di salute e sicurezza nei luoghi di lavoro e di tutela dell'ambiente già adottati dalla Società ed alle relative procedure operative ed istruzioni di lavoro anche con riferimento alla scelta ed ai rapporti con i fornitori e gestione clienti;
- assicurare la coerenza del prezzo delle transazioni, anche infragruppo, in riferimento ai prezzi di mercato;
- effettuare controlli sui flussi finanziari in entrata, tenendo in considerazione alcuni indicatori quali sede legale della controparte (ad esempio "paradisi fiscali", Paesi a rischio terrorismo etc.);
- operare con trasparenza garantendo la tracciabilità e verificabilità di ogni operazione effettuata nell'ambito dei rapporti infragruppo;
- verificare la provenienza delle merci o dei beni in entrata od oggetto di operazioni finanziarie;
- verificare la corrispondenza delle merci/beni/servizi acquistati/venduti con la documentazione accompagnatoria e gli ordini di acquisto/vendita;
- nel processo di assunzione di dipendenti, acquisire le certificazioni del casellario giudiziale nonché le documentazioni attestanti cittadinanza e regolare presenza dello straniero sul territorio italiano;
- assicurare la corretta informazione e formazione sui contenuti del modello di organizzazione, gestione e controllo e sul relativo sistema disciplinare;
- astenersi dal tenere qualsivoglia condotta da cui possano generarsi proventi illeciti;
- rispettare la normativa vigente in relazione ad operazioni intercorse con paesi elencati nella cosiddetta "black list";
- effettuare/ricevere pagamenti facendo ricorso al canale bancario;
- non effettuare operazioni in violazione dell'art. 110, comma 7, del TUIR;
- assicurare il rispetto degli adempimenti fiscali/tributari alle scadenze previste dalla legge.

È espressamente vietato:

- indicare nelle dichiarazioni relative alle imposte sui redditi e Iva (non solo le dichiarazioni annuali ma anche, ad esempio, gli elenchi Intrastat e le dichiarazioni di intento) elementi passivi fittizi mediante fatture o altri documenti analoghi aventi efficacia probatoria per operazioni inesistenti;
- indicare nella dichiarazione dei redditi o nella dichiarazione Iva elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, anche attraverso 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;
- indicare nella dichiarazione annuale dei redditi o Iva elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi inesistenti (costi inesistenti o ricavi più bassi);
- omettere di presentare la dichiarazione annuale dei redditi e/o Iva;
- emettere o rilasciare fatture o altri documenti per operazioni inesistenti;
- occultare o distruggere 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;
- omettere il versamento dell'Iva nei termini di legge;
- omettere il versamento delle ritenute d'acconto nei termini previsti;

- alienare simulatamente o compiere altri atti fraudolenti sui beni della Società o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte;
- non versare le somme dovute utilizzando in compensazione crediti non spettanti o inesistenti.

M.10 Procedure e istruzioni di lavoro

La società assicura la concreta applicazione ed attuazione dei principi e delle regole sopra esposti mediante:

1. le specifiche procedure di gestione e istruzioni di lavoro adottate nell'ambito del Sistema Integrato di Gestione per la Qualità ISO 9001:2015;
2. le specifiche procedure di gestione e istruzioni di lavoro adottate nell'ambito del Sistema di Gestione per la Salute e la Sicurezza sul Lavoro ISO 45001:2018;
3. le specifiche procedure di gestione e istruzioni di lavoro adottate nell'ambito del Sistema di Gestione Ambientale ISO 14001:2015;
4. il Codice Etico Comportamentale;
5. le disposizioni previste nella procedura IACQ-01 "Approvvigionamento di beni e servizi – gestione delle fatture passive", con particolare riferimento alle modalità di effettuazione dei pagamenti previsti nei punti 7) "Rilascio del benestare" e 8) "Autorizzazione al pagamento" della predetta procedura;
6. le disposizioni previste nella procedura IAMM-06 "Gestione delle Immobilizzazioni Materiali";
7. le specifiche procedure emesse per la gestione della piccola cassa delle varie Sedi aziendali;
8. le procedure di Gruppo FT/PRO-0001 "Bank Authorisation and Treasury Management" e FT/PRO- 0002 "Financial Issues/Anomalies Reporting (Materiality Thresholds and Timings);
9. le disposizioni contenute nel Manuale del Sistema di Gestione Integrato Qualità e Sicurezza (MSGI) e delle relative Procedure, come elencate nel paragrafo B.3 del presente Modello;
10. le disposizioni previste nella procedura IAMM-09 "Modalità' di Computo delle Imposte Dirette e Indirette dell'Esercizio e dei Contributi Previdenziali e Assistenziali – Versamenti e Verifica dei Relativi Adempimenti di Legge".

Le procedure e le istruzioni di lavoro sopra richiamate costituiscono parte integrante del presente Modello di Organizzazione, Gestione e controllo.

Poiché, come già evidenziato, le possibili modalità di realizzazione dei reati tributari oggetto della presente Parte speciale possono interessare molteplici aree/processi di rischio nonché sovrapporsi con condotte integranti altre fattispecie di reato (ad esempio corruzione, autoriciclaggio, reati societari), sono operativi e concretamente applicabili anche i presidi di controllo ed i principi formulati nelle altre Parti speciali del presente Modello organizzativo che si intendono qui integralmente richiamati nonché le procedure/istruzioni di lavoro di riferimento.

I rapporti con le Società del Gruppo sono improntati a trasparenza e verificabilità dei flussi finanziari sulla scorta di criteri predeterminati e conformi alla normativa e alle regole di mercato.

M.11 Flussi di comunicazione all'OdV

È inviato all'Odv, da parte dei "Responsabili delle aree/attività a rischio di reato", report trimestrale avente ad oggetto la gestione degli adempimenti della presente parte speciale, e fatte in ogni caso salve le comunicazioni urgenti che si rendessero necessarie.

Le comunicazioni periodiche inviate all'Organismo di Vigilanza ai sensi del presente paragrafo concernono i contenuti delle attività e delle procedure richiamate nella presente Parte speciale, il rispetto delle stesse e le eventuali anomalie/criticità riscontrate ad una verifica di primo livello effettuata dai Responsabili di funzione.

M.12 Compiti dell'OdV

Nello svolgimento dei propri compiti l'OdV dovrà verificare periodicamente il funzionamento del Modello
di organizzazione e gestione e delle procedure/istruzioni di lavoro adottate.

L'OdV deve esaminare eventuali segnalazioni in arrivo e disporre gli accertamenti ritenuti necessari.

Devono essere tempestivamente comunicati all'OdV gli esiti di eventuali ispezioni e/o accertamenti da parte delle autorità competenti nonché l'instaurazione di procedimenti, di natura civile, amministrativa e/o penale, per violazione delle norme direttamente e/o indirettamente richiamate dall'articolo 25 quinquiesdecies del Decreto 231.