



STUDIO GEOTECNICO ITALIANO srl

ingegneria geotecnica - ingegneria sismica - ingegneria ambientale
geologia applicata

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO AI SENSI DEL D.LGS. 231/2001

Revisione Marzo 2021

Emissione 06	G2021-016R01E01	Milano, 30 Marzo 2021
Emissione 05:	G2020-026R01E01	Milano, 12 Marzo 2020
Emissione 04:	G2019-012R01E01	Milano, 25 Marzo 2019
Emissione 03:	G2018-030R01E01	Milano, 26 Marzo 2018
Emissione 02:	G2015-033R01E01	Milano, 30 Aprile 2015
Emissione 01:	G2011-023R01E01	Milano, 13 Giugno 2011



Reg. CH-20504
ISO 9001:2015
ISO 14001:2015
OHSAS 18001:2007

Sede Legale e Uffici: Centro Direzionale Milanofiori - Strada 2 - Palazzo C - Scala C3 - 20057 Assago (MI)
Tel.: +39 02 5220141 - Fax: +39 02 5691845 - Email: info@studiogeotecnico.it - P.E.C.: sgi@legalmail.it
Sito Web: www.studiogeotecnico.it - Capitale Sociale € 1.550.000,00 i.v. - R.E.A. MI 691783
Codice Fiscale e Registro Imprese di Milano Monza Brianza Lodi 00506080019 - Partita IVA IT11261240151



INDICE

PARTE GENERALE

1. DESCRIZIONE DEL QUADRO NORMATIVO

- 1.1 *La responsabilità amministrativa*
- 1.2 *Fattispecie di reato*
- 1.3 *Autori del reato*
- 1.4 *Apparato sanzionatorio*
- 1.5 *Adozione del “modello di organizzazione e gestione” quale possibile esimente*

2. ADOZIONE DEL MODELLO DA PARTE DI SGI

- 2.1 *Obiettivi perseguiti da SGI con l’adozione del Modello*
- 2.2 *Reati rilevanti per SGI*
- 2.3 *Destinatari del Modello*
- 2.4 *Modifiche ed integrazioni del Modello*
- 2.5 *Recepimento del Modello nell’ambito del Gruppo*

3. ORGANISMO DI VIGILANZA

- 3.1 *Individuazione*
- 3.2 *Nomina*
- 3.3 *Funzioni e poteri dell’Organismo di Vigilanza*
- 3.4 *Reporting dell’Organismo di Vigilanza verso il vertice societario*
- 3.5 *Reporting verso l’Organismo di Vigilanza*
- 3.6 *Whistleblowing*
- 3.7 *La procedura di Whistleblowing*
- 3.8 *Il sistema sanzionatorio*
- 3.6 *Raccolta e conservazione delle informazioni*

4. DIFFUSIONE, FORMAZIONE E COMUNICAZIONE

- 4.1 *Diffusione*
- 4.2 *Piano di formazione e comunicazione*

5. STRUTTURA DEL SISTEMA DISCIPLINARE

- 5.1 *Funzione del sistema disciplinare*
- 5.2 *Violazione del Modello*
- 5.3 *Misure nei confronti del personale dipendente*
- 5.4 *Misure specifiche nei confronti dei Dirigenti*
- 5.5 *Misure nei confronti degli Amministratori*
- 5.6 *Misure nei confronti dei Sindaci*

PARTE SPECIALE

PARTE SPECIALE “A”

I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

- 1.A *Potenziali aree a rischio*
- 2.A *Principi di comportamento e controllo nelle principali aree di rischio*
- 3.A *Principi per la prevenzione dei reati contro la Pubblica Amministrazione*



PARTE SPECIALE "B"

I REATI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI E REATI IN MATERIA DI CYBERSECURITY

- 1.B *Potenziali aree a rischio*
- 2.B *Principi di comportamento e controllo nelle principali aree di rischio*
- 3.B *Principi per la prevenzione dei reati informatici, di cybersecurity e di trattamento illecito di dati*

PARTE SPECIALE "C"

I REATI SOCIETARI

- 1.C *Potenziali aree a rischio*
- 2.C *Principi di comportamento e controllo nelle principali aree di rischio*
- 3.C *Principi per la prevenzione dei reati societari*

PARTE SPECIALE "D"

I REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI E GRAVISSIME, COMMESSI CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

- 1.D *Potenziali aree a rischio*
- 2.D *Principi di comportamento e controllo nelle principali aree di rischio*
- 3.D *Principi per la prevenzione dei reati di omicidio colposo e lesioni colpose gravi e gravissime*

PARTE SPECIALE "E"

I REATI DI RICETTAZIONE, RICICLAGGIO E AUTORICICLAGGIO

- 1.E *Potenziali aree a rischio*
- 2.E *Principi di comportamento e controllo nelle principali aree di rischio*
- 3.E *Principi per la prevenzione dei reati di ricettazione e riciclaggio*

PARTE SPECIALE "F"

I DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

- 1.F *Potenziali aree a rischio*
- 2.F *Principi di comportamento e controllo nelle principali aree di rischio*
- 3.F *Principi per la prevenzione dei delitti in materia di violazione del diritto d'autore*

PARTE SPECIALE "G"

I REATI AMBIENTALI

- 1.G *Potenziali aree a rischio*
- 2.G *Principi di comportamento e controllo nelle principali aree di rischio*
- 3.G *Principi per la prevenzione dei reati ambientali*

PARTE SPECIALE "H"

I REATI CONTRO L'AMMINISTRAZIONE DELLA GIUSTIZIA

- 1.G *Potenziali aree a rischio*
- 2.G *Principi di comportamento e controllo nelle principali aree di rischio*
- 3.G *Principi per la prevenzione dei reati contro l'amministrazione della giustizia.*



PARTE SPECIALE "I"

I REATI DI IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE

- 1.I *Potenziali aree a rischio*
- 2.I *Principi di comportamento e controllo nelle principali aree di rischio*
- 3.I *Principi per la prevenzione dei reati di impiego di cittadini di paese terzi il cui soggiorno è irregolare.*

PARTE SPECIALE "L"

I REATI TRIBUTARI

- 1.L *Potenziali aree a rischio*
- 2.L *Principi di comportamento e controllo nelle principali aree di rischio*
- 3.L *Principi per la prevenzione dei reati tributari*

ALLEGATI

Allegato 1 – Reati previsti dal d.lgs. 231/2001



1. DESCRIZIONE DEL QUADRO NORMATIVO

1.1 *La responsabilità amministrativa*

Il decreto legislativo 8 giugno 2001 n. 231 (di seguito, “d.lgs 231/2001”) ha introdotto nell’ordinamento giuridico italiano la disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica (enti). Secondo tale disciplina le società possono essere ritenute responsabili, e conseguentemente sanzionate patrimonialmente, in relazione a taluni reati commessi o tentati *nell'interesse o a vantaggio della società* stessa dagli amministratori o dai dipendenti.

Il d.lgs 231/2001, allineandosi con i sistemi normativi di molti paesi europei, affianca alla responsabilità penale della persona fisica che ha commesso il reato l’autonoma responsabilità amministrativa dell’ente.

L’istituzione della responsabilità amministrativa della società nasce dalla considerazione che frequentemente le condotte illecite commesse all’interno dell’impresa non derivano da un’iniziativa privata del singolo, ma si ricollegano piuttosto a volontà e decisioni di vertice dell’ente medesimo.

1.2 *Fattispecie di reato*

Le fattispecie di reato rilevanti ai sensi del d.lgs. 231/2001 sono quelle espressamente elencate dal legislatore - in ossequio al principio di legalità confermato dall'art. 2 del d.lgs. 231/2001 - e possono essere comprese nelle seguenti principali categorie:

- a) ***delitti contro la pubblica amministrazione*** (quali, indebita percezione di contributi e finanziamenti da parte dello Stato o di altro ente pubblico; truffa ai danni dello Stato e frode informatica ai danni dello Stato; corruzione per un atto d’ufficio o in atti giudiziari; concussione; malversazione a danno dello Stato o di altro ente pubblico; traffico di influenze illecite, frode nelle pubbliche forniture, indicati agli artt. 24 e 25);
- b) ***reati informatici, trattamento illecito di dati e reati in materia di cybersecurity*** (indicati all’art. 24-bis, 25 novies d.lgs. 231/2001);
- c) ***delitti di criminalità organizzata*** (indicati all’art. 24-ter d.lgs. 231/2001);
- d) ***delitti contro la fede pubblica*** (quali falsità in monete/carte di pubblico credito/valori di bollo; delitti contro l’industria e il commercio; indicati agli artt. 25-bis e 25-bis.1);
- e) ***reati societari*** (quali false comunicazioni sociali, falso in prospetto, falsità nelle relazioni o nelle comunicazioni della società di revisione; impedito controllo; illegale ripartizione degli utili e delle riserve; illecite operazioni sulle azioni o quote sociali; operazioni in pregiudizio dei creditori; formazione fittizia del capitale; illecita influenza sull’assemblea; aggio; ostacolo all’esercizio delle



funzioni delle autorità di pubblica vigilanza; corruzione tra privati; indicati all'art. art. 25-ter d.lgs. 231/2001);

- f) **delitti con finalità di terrorismo e di eversione dell'ordine democratico** (ivi incluso il finanziamento ai suddetti fini, indicati all'art. 25-quarter d.lgs. 231/2001);
- g) **delitti contro la personalità individuale** (quali la pratica di mutilazione degli organi genitali femminili, lo sfruttamento della prostituzione, la pornografia minorile, indicati agli artt. 25- quater.1 e 25-quinquies d.lgs. 231/2001);
- h) **reati di abuso di mercato** (indicati all'art. 25-sexies d.lgs. 231/2001);
- i) **reati di lesioni colpose gravi e gravissime e omicidio colposo con violazione di norme antinfortunistiche** (indicati all'art. 25-septies d.lgs. 231/2001);
- j) **reati di ricettazione, riciclaggio e autoriciclaggio** (indicati all'art. 25-octies d.lgs. 231/2001);
- k) **delitti in materia di violazione del diritto d'autore** (indicati all'art. 25-novies d.lgs. 231/200);
- l) **reati contro l'amministrazione della giustizia** (indicati all'art. 25-decies d.lgs. 231/2001)
- m) **reati ambientali** (indicati all'art. 25-undecies d.lgs. 231/2001);
- n) **impiego di cittadini di paesi terzi il cui soggiorno è irregolare** (indicati all'art. 25-duodecies d.lgs. 231/2001);
- o) **reati in materia di razzismo e xenofobia** (indicati dall'art. 25-terdecies d.lgs. n. 231/2001)
- p) **reati transnazionali** (art. 10, Legge 16 Marzo 2006, n.146)
- q) **reati tributari** (art. 25 quinquiesdecies d.lgs. 231/2001).

Si rimanda all'Allegato 1 per l'elenco dettagliato dei reati di cui al d.lgs. 231/2001.

1.3 Autori del reato

Quanto ai soggetti, il d.lgs. 231/2001 (art. 5) prevede la responsabilità dell'ente qualora il reato sia commesso:

- 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 dell'ente stesso"* (c.d. soggetti in posizione apicale o "apicali"; art. 5, comma 1, lett. a), d.lgs. 231/2001);
- b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti in posizione apicale (c.d. soggetti sottoposti altrui direzione; art. 5, comma 1, lett. b), d.lgs. 231/2001).



La società non risponde, per espressa previsione legislativa (art. 5, comma 2, d.lgs. 231/2001), se le persone indicate hanno agito nell'interesse esclusivo proprio o di terzi.

1.4 Apparato sanzionatorio

L'accertamento della responsabilità della società, attribuito al giudice penale, avviene (nell'ambito di un processo *ad hoc* nel quale l'ente viene parificato alla persona fisica imputata) mediante la verifica della sussistenza del reato presupposto per la responsabilità della società, nonché il sindacato di idoneità sui modelli organizzativi adottati.

Il d. lgs 231/2001 prevede un articolato sistema sanzionatorio. Le sanzioni possono essere:

- di **natura pecuniaria** (da Euro 25.000,00 fino ad un massimo di Euro 1.500.000,00 circa)
- di **natura interdittiva** (quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la pubblica amministrazione, l'esclusione o revoca di finanziamenti e contributi), e
- **accessorie**: pubblicazione della sentenza e la confisca del prezzo o profitto del reato.

Nelle ipotesi di commissione, nelle forme del tentativo, dei delitti indicati nel Capo 1 del d.lgs. 231/2001 (artt. da 24 a 25-*quinquies*), le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26).

Secondo l'art. 4 del d.lgs. 231/2001, l'ente può essere chiamato a rispondere in Italia in relazione a reati - contemplati dallo stesso d.lgs. 231/2001 - commessi all'estero. La Relazione illustrativa del d.lgs. 231/2001 sottolinea, infatti, la necessità di non lasciare sfornita di sanzione una situazione criminologica di frequente verifica, anche al fine di evitare facili elusioni dell'intero impianto normativo in oggetto.

1.5 L'adozione del "Modello di Organizzazione e di Gestione" quale possibile esimente

Il d.lgs. 231/2001, nell'introdurre il suddetto regime di responsabilità amministrativa, prevede, tuttavia, una forma specifica di esonero da detta responsabilità qualora l'ente dimostri di aver adottato tutte le misure organizzative e gestionali idonee a prevenire la commissione di reati da parte di soggetti che operino per suo conto.

Il d.lgs. 231/2001 indica quali sono le componenti di un apparato organizzativo efficace ed effettivo (cosiddetto modello di organizzazione e gestione – il Modello) la cui corretta predisposizione porta ad escludere la responsabilità dell'ente.

Il Modello si può definire come un complesso organico di principi, regole, disposizioni, schemi organizzativi, funzionale alla realizzazione ed alla diligente gestione di un sistema di controllo e monitoraggio delle attività sensibili, al fine della prevenzione sulla commissione, anche tentata, dei reati previsti dal d.lgs. 231/2001. La finalità preventiva del Modello si esplica sia nei confronti di soggetti in posizione "apicale" che di soggetti sottoposti all'altrui direzione.



In particolare, il Modello deve:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;
- prevedere, in relazione alla natura ed alla dimensione dell'organizzazione, nonché del 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.

L'adozione di modelli organizzativi, astrattamente idonei a prevenire i reati di cui al d.lgs. 231/2001, deve essere corredata dall'efficace attuazione degli stessi e da una procedura che garantisca il tempestivo aggiornamento e adeguamento.

2. ADOZIONE DEL MODELLO DA PARTE DI SGI

2.1 Obiettivi perseguiti da SGI con l'adozione del Modello

SGI ritiene conforme alle proprie politiche aziendali procedere all'attuazione del modello di organizzazione e gestione previsto dal d.lgs. 231/2001.

SGI si è dotata di un Codice Etico, espressione dei valori e principi sui quali l'attività aziendale si ispira.

È convinzione di SGI che l'adozione del Modello e del Codice Etico, pur non costituendo un obbligo di legge, rappresenti un passo fondamentale per indirizzare e sensibilizzare i comportamenti e le azioni di tutti coloro che agiscono in nome e per conto di SGI, affinché il loro operare sia sempre orientato al rispetto della legge e dei principi di correttezza e trasparenza.

Il Modello è ispirato alle Linee guida per la costruzione dei modelli di Organizzazione, Gestione e Controllo elaborate da Confindustria, approvate il 7 marzo 2002 e come successivamente aggiornate da ultimo nel settembre 2017.

Il Modello, unitamente al Codice Etico qui allegato, è stato adottato all'unanimità, dal Consiglio di Amministrazione di SGI che ha altresì nominato l'Organismo di Vigilanza.

2.2 Reati rilevanti per SGI

Ai sensi dell'art. 6 del d.lgs. 231/2001, che prevede che la società individui le attività nel cui ambito possono essere commessi i reati, SGI ha svolto un'analisi di tutte le attività aziendali, dei processi di formazione delle decisioni, nonché del sistema di controllo interno.



Tale analisi è stata condotta ed aggiornata anche con il supporto di professionisti esterni, tramite l'analisi della documentazione aziendale interna rilevante e l'incontro con i responsabili delle singole aree di attività.

Sulla base dell'analisi di cui sopra e in considerazione della natura e dell'attività di SGI, ai fini del Modello sono considerati rilevanti i reati di cui agli artt. 24, 24-bis, 25, 25-ter, 25-septies, 25-octies, 25-novies, 25 decies 25-undecies, 25-duodecies e 25 quinquiesdecies del d.lgs. 231/2001.

2.3 Destinatari del Modello

Sono destinatari del Modello tutti coloro che operano per il conseguimento dello scopo e degli obiettivi di SGI. Fra i destinatari del Modello è incluso tutto il personale di SGI; le disposizioni contenute nel Modello devono dunque essere rispettate dal personale dirigenziale che opera in nome e per conto di SGI e da tutti i dipendenti.

Gli altri destinatari del Modello sono i componenti degli organi sociali di SGI, i collaboratori, i consulenti esterni, i fornitori con i quali SGI opera (di seguito, congiuntamente, i "Destinatari").

2.4 Modifiche ed integrazioni del Modello

Il Modello è espressione della politica aziendale perseguita dai massimi vertici sociali. Pertanto, il potere di integrare e/o modificare il Modello è demandato al Consiglio di Amministrazione di SGI.

3. ORGANISMO DI VIGILANZA

3.1 Individuazione

L'Organismo di Vigilanza è istituito con delibera del Consiglio di Amministrazione in forma monocratica ovvero collegiale composto sino ad un massimo di tre (3) membri.

L'Organismo di Vigilanza definisce e svolge le attività di competenza ed è dotato ai sensi dell'art. 6, comma 1, lett. b), del d.lgs. 231/2001 di "autonomi poteri di iniziativa e controllo".

Al fine di coadiuvare la definizione e lo svolgimento delle attività di competenza e di consentire la massima adesione ai requisiti e ai compiti di legge, l'Organismo di Vigilanza è autorizzato ad avvalersi di consulenti esterni specializzati.

Per il corretto e regolare esercizio delle sue funzioni l'Organismo di Vigilanza potrà disporre di proprie risorse finanziarie che, su proposta dello stesso, gli saranno accordate dal Consiglio di Amministrazione di SGI, sentito il Collegio Sindacale.

Il Consiglio di Amministrazione, sentito il Collegio Sindacale, nell'atto di nomina o con successiva delibera riconoscerà un compenso all'Organismo di Vigilanza.

3.2 Nomina

I componenti dell'Organismo di Vigilanza sono nominati con delibera del Consiglio di Amministrazione, sentito il parere del Collegio Sindacale.



Costituiscono cause di ineleggibilità e/o di decadenza dell'Organismo di Vigilanza:

- la condanna, con sentenza passata in giudicato, per aver commesso uno dei reati previsti dal d.lgs. 231/2001; ovvero
- la condanna, con sentenza passata in giudicato, a una pena che comporta l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

In casi di particolare gravità, anche prima del giudicato, il Consiglio di Amministrazione di SGI potrà disporre - sentito il parere del Collegio Sindacale - la sospensione dei poteri dell'Organismo di Vigilanza e la nomina di un *interim*.

Fatta salva l'ipotesi di una rivisitazione del ruolo e del posizionamento dell'Organismo di Vigilanza sulla base dell'esperienza di attuazione del Modello, l'eventuale revoca degli specifici poteri propri dell'Organismo di Vigilanza potrà avvenire soltanto per giusta causa, previa delibera del Consiglio di Amministrazione di SGI sentito il parere del Collegio Sindacale.

3.3 Funzioni e poteri dell'Organismo di Vigilanza

I compiti dell'Organismo di Vigilanza sono così definiti:

- vigilanza sull'effettività del Modello;
- disamina dell'adeguatezza del Modello, ossia dell'efficacia nel prevenire i comportamenti illeciti;
- analisi circa il mantenimento, nel tempo, dei requisiti di solidità e funzionalità del Modello;
- promozione dell'aggiornamento ed adeguamento continuo del Modello e del sistema di vigilanza sull'attuazione dello stesso;
- assicurazione dei flussi informativi di competenza;
- supervisionare il sistema di comunicazione interna per consentire la trasmissione di notizie rilevanti ai fini del d.lgs. 231/01 e le segnalazioni in materia di Whistleblowing (si veda successivo articolo 3.6), provenienti da tutti i Destinatari del Modello e dai soggetti terzi, attinenti ad eventuali violazioni delle prescrizioni del Modello, garantendo la tutela e riservatezza del segnalante.

Nello svolgimento dei compiti assegnati, l'Organismo di Vigilanza ha accesso senza limitazioni alle informazioni aziendali per le attività di indagine, analisi e controllo. È fatto obbligo di informazione all'Organismo di Vigilanza, in capo a qualunque funzione aziendale, dipendente e/o componente degli organi sociali di SGI, a fronte di richieste da parte dell'Organismo di Vigilanza o al verificarsi di eventi o circostanze rilevanti.

3.4 Reporting dell'Organismo di Vigilanza verso il vertice societario

L'Organismo di Vigilanza riferisce in merito all'attuazione del Modello, all'emersione di eventuali aspetti critici e comunica l'esito delle attività svolte nell'esercizio dei compiti assegnati. Sono previste le linee di riporto seguenti:



- continuativa, nei confronti del Presidente e dell'Amministratore Delegato di SGI, i quali informano il Consiglio di Amministrazione di SGI;
- annuale, nei confronti del Collegio Sindacale di SGI, predisponendo un rapporto annuale relativo all'attività svolta ed a eventuali innovazioni legislative in materia.

In particolare, alla notizia di una violazione del Modello commessa da parte di uno o più membri del Consiglio di Amministrazione, l'Organismo di Vigilanza informa il Consiglio di Amministrazione ed il Collegio Sindacale. Il Consiglio di Amministrazione procede agli accertamenti necessari e assume, sentito il Collegio Sindacale, i provvedimenti opportuni.

Alla notizia di una violazione del Modello commessa da parte di uno o più Sindaci, l'Organismo di Vigilanza informa il Consiglio di Amministrazione ed il Collegio Sindacale. Il Collegio Sindacale procede agli accertamenti necessari e assume, sentito il Consiglio di Amministrazione, i provvedimenti opportuni.

3.5 Reporting verso l'Organismo di Vigilanza

L'Organismo di Vigilanza deve essere informato, mediante apposite segnalazioni da parte dei soggetti tenuti all'osservanza del Modello, in merito a eventi che potrebbero ingenerare responsabilità della Società ai sensi del d.lgs. 231/2001. Valgono al riguardo le seguenti prescrizioni di carattere generale:

- devono essere raccolte da ciascun responsabile della Società eventuali segnalazioni relative alla commissione, o al ragionevole pericolo di commissione, dei reati contemplati dal d.lgs. 231/2001 o comunque a comportamenti in generale non in linea con le regole di comportamento di cui al Modello e al Codice Etico;
- ciascun dipendente deve segnalare la violazione (o presunta violazione) del Modello contattando il proprio diretto superiore gerarchico e/o l'Organismo di Vigilanza;
- i consulenti, i collaboratori e i partner commerciali, per quanto riguarda la loro attività svolta nei confronti della Società, effettuano la segnalazione direttamente all'Organismo di Vigilanza;

L'Organismo di Vigilanza valuta le segnalazioni ricevute, anche in materia di Whistleblowing, e le attività da porre in essere; gli eventuali provvedimenti conseguenti sono definiti e applicati in conformità a quanto *infra* previsto in ordine al sistema disciplinare. Oltre alle segnalazioni relative a violazioni di carattere generale sopra descritte, devono essere trasmesse all'Organismo di Vigilanza le notizie relative ai procedimenti disciplinari azionati in relazione alla violazione del Modello e del Codice Etico e alle sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

3.6 Whistleblowing

Con la Legge 30 novembre 2017, n. 179 recante le "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" (c.d. legge sul *whistleblowing*) è stato introdotto



nell'ordinamento giuridico italiano un apparato di norme volto a migliorare l'efficacia degli strumenti di contrasto ai fenomeni corruttivi, nonché a tutelare con maggiore intensità gli autori delle segnalazioni incentivando il ricorso allo strumento della denuncia di condotte illecite o di violazione dei Modelli di Organizzazione, Gestione e Controllo gravando il datore di lavoro dell'onere di dimostrare – in occasione di controversie legate all'irrogazione di sanzioni disciplinari, demansionamenti, licenziamenti, trasferimenti o alla sottoposizione del segnalante ad altra misura organizzativa successiva alla presentazione della segnalazione avere effetti negativi, diretti o indiretti, sulla condizione di lavoro – che tali misure risultino fondate su ragioni estranee alla segnalazione stessa (c.d. inversione dell'onere della prova a favore del segnalante).

In particolare, il Legislatore ha introdotto specifiche previsioni per gli enti destinatari del d.lgs. 231/2001, specificando ai sensi del nuovo art. 6 del d.lgs. 231/2001, comma 2bis, 2 ter e 2 quater, che i Modelli di Organizzazione, Gestione e Controllo devono prevedere:

- a. uno o più canali che consentano ai destinatari di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del Decreto e fondate su elementi di fatto precisi e concordanti, ovvero di violazioni del Modello di Organizzazione e Gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;
- b. almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
- c. il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- d. sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

L'art. 6, comma 2 ter, del d.lgs. 231/2001 prevede che l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni può essere denunciata all'ispettorato del Lavoro, per provvedimenti di propria competenza, oltreché dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo. Al comma 2 quater viene altresì disciplinato che il licenziamento ritorsivo o discriminatorio del soggetto segnalante è qualificato come "nullo"; così come nulli devono considerarsi il mutamento di mansioni ai sensi dell'art. 2103 c.c., nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. Il predetto articolo, inoltre, prevede che in caso di controversie legate all'erogazione di sanzioni disciplinari, demansionamenti, licenziamenti, trasferimenti ovvero sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi sulle condizioni di lavoro, spetta al datore di lavoro provare che tali misure siano state adottate sulla base di ragioni estranee alla segnalazione.



3.7 *La procedura di Whistleblowing*

Al fine di garantire l'efficacia del sistema di whistleblowing la Società ha adottato il seguente sistema per la gestione delle segnalazioni di illeciti e irregolarità da parte dei propri dipendenti, amministratori e membri degli organi sociali, nonché terze parti, volto a regolamentare, incentivare e proteggere, chi, nello svolgimento delle proprie mansioni lavorative, venendo a conoscenza di un illecito e/o di un'irregolarità sul luogo di lavoro, rilevanti ai fini del d.lgs. 231/2001, decide di farne segnalazione.

Le segnalazioni possono avere ad oggetto:

- condotte illecite che integrano una o più fattispecie di reato da cui può derivare una responsabilità per l'ente ai sensi del d.lgs. 231/2001;
- condotte, che pur non integrando alcuna fattispecie di reato, sono state poste in essere contravvenendo a regole di condotta, procedure, protocolli o disposizioni contenute all'interno del Modello o dei documenti ad esso allegati.

Non saranno meritevoli di segnalazione, invece, questioni di carattere personale del segnalante, rivendicazioni o istanze attinenti alla disciplina del rapporto di lavoro o rapporti con il superiore gerarchico o con i colleghi.

Le segnalazioni devono fornire elementi utili a consentire ai soggetti preposti di procedere alle dovute e appropriate verifiche ed accertamenti.

Sono altresì disciplinate le segnalazioni anonime, ovvero quelle segnalazioni prive di elementi che consentano di identificare il loro autore. Le segnalazioni anonime non verranno prese in considerazione per quanto attiene la tutela accordata dalla norma al segnalante (art. 6, commi 2 ter e 2 quater, D.lgs. 231/2001). Le predette segnalazioni saranno oggetto di ulteriori verifiche solo ove siano connotate da un contenuto adeguatamente dettagliato e circostanziato e avente ad oggetto illeciti o irregolarità particolarmente gravi.

La Società ha previsto di istituire due canali di comunicazione: un canale tramite posta fisica, mediante l'invio di una busta all'attenzione dell'Amministratore Delegato della Società, presso la sede della Società, contenente al suo interno una seconda busta sigillata indicando sulla stessa la dicitura "all'attenzione dell'OdV" e un canale informatico tramite l'indirizzo di posta elettronica dell'OdV dedicato.

La Società ed i destinatari della segnalazione agiscono in modo da garantire i segnalanti contro qualsiasi forma di ritorsione o comportamenti discriminatori, diretti o indiretti, per motivi collegati, direttamente o indirettamente, alla segnalazione.

La Società al fine di incentivare l'uso dei sistemi interni di segnalazione e di favorire la diffusione di una cultura della legalità illustra al proprio personale dipendente in maniera chiara, precisa e completa il procedimento di segnalazione interna adottato.

3.8 *Il sistema sanzionatorio*

Un sistema di Whistleblowing efficace deve prevedere delle sanzioni nei confronti del segnalante, in caso di abuso dello strumento di segnalazione, nei confronti dei segnalati



in caso di accertamento degli illeciti segnalati e nei confronti di coloro i quali violano la tutela della riservatezza del Segnalante.

Attualmente il sistema di Whistleblowing è stato integrato nel d.Lgs. 231/2001 di conseguenza vengono estese ed applicate in caso di violazioni accertate le sanzioni previste dal sistema descritto al successivo articolo 5.2.

3.9 Raccolta e conservazione delle informazioni

Ogni informazione, segnalazione, *report* previsti nel Modello sono conservati dall'Organismo di Vigilanza in un apposito *data base* informatico e/o cartaceo. I dati e le informazioni così archiviate sono poste a disposizione di soggetti esterni all'Organismo di Vigilanza previa autorizzazione dell'Organismo di Vigilanza stesso.

4. FORMAZIONE E COMUNICAZIONE

4.1 Diffusione

È data ampia diffusione, all'interno ed all'esterno della struttura, dei principi contenuti nel Modello e del Codice Etico.

SGI si impegna a facilitare e promuovere la conoscenza del Modello e del Codice Etico da parte dei dipendenti, con grado di approfondimento diversificato a seconda della posizione e del ruolo, e il loro contributo costruttivo sui suoi contenuti.

4.2 Piano di formazione e comunicazione

Il Modello ed il Codice Etico sono comunicati formalmente dall'Organismo di Vigilanza a ciascun componente degli organi sociali, che li sottoscrive per adesione.

I principi e i contenuti del Modello e del Codice Etico sono comunicati formalmente dall'Organismo di Vigilanza a tutti i dirigenti della Società e ai Responsabili di Divisione, mediante consegna del presente documento.

I principi e i contenuti del Modello e del Codice Etico sono, inoltre, divulgati mediante corsi di formazione ai quali i soggetti sopra individuati sono tenuti a partecipare. La struttura dei corsi di formazione è definita dall'Organismo di Vigilanza in coordinamento con le funzioni aziendali competenti.

Il Modello e il Codice Etico sono affissi nelle bacheche aziendali e i principi e i contenuti del Modello e del Codice Etico sono comunicati a ciascun dipendente.

Il Modello e il Codice Etico sono portati a conoscenza di coloro con i quali SGI intrattiene relazioni d'affari.

5. STRUTTURA DEL SISTEMA DISCIPLINARE

5.1 Funzione del sistema disciplinare

L'art. 6, comma 2, lett. e) e l'art. 7, comma 4, lett. b) del d.lgs. 231/2001 stabiliscono (con riferimento sia ai soggetti in posizione apicale sia ai soggetti sottoposti ad altrui



direzione) la necessaria predisposizione di un “*sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello*”.

La definizione di sanzioni, commisurate alla violazione, applicabili in caso di violazione delle misure contenute nel Modello ha lo scopo di contribuire all’efficacia del Modello stesso ed all’efficacia dell’azione di controllo dell’Organismo di Vigilanza.

L’applicazione del sistema è autonoma rispetto allo svolgimento e all’esito del procedimento penale eventualmente avviato presso l’Autorità giudiziaria competente.

5.2 Violazione del Modello

Ai fini dell’ottemperanza del d.lgs. 231/2001, a titolo esemplificativo, costituisce violazione del Modello:

- la messa in atto di azioni o comportamenti non conformi alle prescrizioni del Modello, ovvero l’omissione di azioni o comportamenti prescritti dal Modello, nell’espletamento di attività nel cui ambito ricorre il rischio di commissione dei reati contemplati dal d.lgs. 231/2001;
- la messa in atto di azioni o comportamenti non conformi alle prescrizioni del Modello, ovvero l’omissione di azioni e comportamenti prescritti dal Modello, che:
 - (a) espongono la Società a una situazione oggettiva di rischio di commissione di uno dei reati contemplati dal d.lgs. 231/2001; e/o
 - (b) siano diretti in modo univoco al compimento di uno o più reati contemplati dal d.lgs. 231/2001; e/o
 - (c) siano tali da determinare l’applicazione a carico della società di sanzioni previste dal d.lgs. 231/2001;
- la messa in atto di azioni o comportamenti non conformi ai principi contenuti nel Codice Etico, ovvero l’omissione di azioni o comportamenti prescritti dal Codice Etico.

5.3 Misure nei confronti del personale dipendente

Alla notizia di una violazione del Modello comunicata da parte dell’Organismo di Vigilanza, corrisponde l’avvio della procedura di accertamento delle mancanze stabilite dal Contratto Collettivo Nazionale del Lavoro applicabile CCNL). Pertanto:

- a ogni notizia di violazione del Modello comunicata da parte dell’Organismo di Vigilanza, è dato impulso da parte del Presidente e/o dell’Amministratore Delegato di SGI alla procedura di accertamento;
- nel caso in cui, a seguito della procedura, sia accertata la violazione del Modello, è individuata dal Presidente e/o dall’Amministratore Delegato di SGI, di intesa con il Responsabile delle Risorse Umane e da quest’ultimo irrogata nei confronti dell’autore della condotta censurata, la sanzione disciplinare prevista dal CCNL;
- la sanzione irrogata è proporzionata alla gravità della violazione.

Le sanzioni disciplinari previste dal CCNL sono:

- rimprovero verbale;
- rimprovero scritto;



- multa;
- sospensione dal lavoro e dalla retribuzione;
- licenziamento per giusta causa.

Il Responsabile delle Risorse Umane comunica l'irrogazione di tale sanzione all'Organismo di Vigilanza.

5.4 Misure specifiche nei confronti di Dirigenti.

Alla notizia di una violazione del Modello comunicata da parte dell'Organismo di Vigilanza, nel caso in cui la violazione del Modello da parte di uno o più dirigenti sia accertata ai sensi del precedente paragrafo 5.3, SGI adotterà nei confronti dell'autore della condotta censurata quanto previsto per legge e per CCNL. Se la violazione del Modello fa venire meno il rapporto di fiducia, la sanzione è individuata nel licenziamento per giusta causa.

5.5 Misure nei confronti degli Amministratori

L'Organismo di Vigilanza informa il Collegio Sindacale e tutti gli Amministratori della notizia di una violazione del Modello commessa da parte di uno o più membri del Consiglio di Amministrazione di SGI. Il Consiglio di Amministrazione di SGI procede agli accertamenti necessari e assume, sentito il Collegio Sindacale, i provvedimenti opportuni.

5.6 Misure nei confronti dei Sindaci

L'Organismo di Vigilanza informa tutti i Sindaci e il Consiglio di Amministrazione di SGI della notizia di una violazione del Modello commessa da parte di uno o più sindaci. Il Collegio Sindacale procede agli accertamenti necessari e assume, sentito il Consiglio di Amministrazione, i provvedimenti opportuni.



PARTE SPECIALE "A"

I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

In questa *parte speciale* sono individuate le aree di attività nel cui ambito possono essere commessi i reati di cui al d.lgs. 231/2001 che riguardano i rapporti con la Pubblica Amministrazione, così come identificati nell'Allegato 1).

1.A Potenziali aree a rischio

In considerazione delle attività svolte dalla Società e della struttura interna adottata, ai sensi dell'art. 6 del d.lgs. 231/2001, sono individuate le seguenti categorie di operazioni ed attività a rischio, nelle quali potrebbero essere commessi i reati previsti dagli artt. 24 e 25, 25 ter e 25 decies del d.lgs. 231/2001:

- a) la partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari ed il loro concreto impiego;
- b) la gestione dei rapporti con soggetti pubblici per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali;
- c) la gestione dei rapporti con i soggetti pubblici per gli aspetti che riguardano la sicurezza e l'igiene sul lavoro;
- d) la gestione dei rapporti con i soggetti pubblici relativi all'assunzione di personale appartenente a categorie protette o la cui assunzione è agevolata;
- e) la gestione di trattamenti previdenziali del personale e/o gestione dei relativi accertamenti/ispezioni;
- f) la richiesta di provvedimenti amministrativi occasionali/ad hoc necessari allo svolgimento di attività strumentali a quelle tipiche aziendali;
- g) la gestione di beni mobili registrati legati all'attività aziendale;
- h) la predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere;
- i) gli adempimenti presso soggetti pubblici, quali comunicazioni, dichiarazioni, deposito atti e documenti, pratiche, ecc. differenti da quelli descritti ai precedenti punti e nelle verifiche/accertamenti/procedimenti sanzionatori che ne derivano;
- j) la gestione di procedimenti giudiziali, arbitrari e/o di conciliazione;
- k) la gestione dei rapporti con le Autorità Pubbliche di Vigilanza.
- l) l'esecuzione dei contratti di fornitura o l'adempimento degli altri obblighi contrattuali che derivano da un contratto di fornitura concluso con lo Stato, o con un altro ente pubblico, ovvero con un'impresa esercente servizi pubblici o di pubblica necessità.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere disposte dall'Organismo di Vigilanza al quale è dato mandato di individuare le relative ipotesi.



2.A Principi di comportamento nelle principali aree di rischio

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 e 25 del d.lgs. 231/2001). Sono altresì proibite le violazioni dei principi e delle procedure aziendali previste nella presente Parte Speciale.

Al fine di evitare il perfezionamento di reati nei confronti della Pubblica Amministrazione, tutti i Destinatari devono attenersi alle seguenti condotte:

- a) osservare rigorosamente tutte le leggi, i regolamenti e le procedure che disciplinano i rapporti e/o i contatti della Società con la Pubblica Amministrazione;
- b) improntare i rapporti con la Pubblica Amministrazione alla massima trasparenza, correttezza ed imparzialità;
- c) verificare, mediante il controllo esercitato dai responsabili delle diverse aree, che qualsiasi rapporto con la Pubblica Amministrazione sia svolto in modo lecito e regolare;
- d) evitare qualsiasi possibile situazione di conflitto di interessi con la Pubblica Amministrazione.

In conformità a tali principi è fatto pertanto divieto di:

- a) usare la propria posizione per ottenere benefici o privilegi per sé o per altri;
- b) effettuare o acconsentire ad elargizioni o promesse di denaro, beni o altre utilità di qualsiasi genere ad esponenti della Pubblica Amministrazione o a soggetti terzi da questi indicati o che abbiano con questi rapporti diretti o indiretti di qualsiasi natura;
- c) distribuire omaggi, regali o prestazioni di qualsiasi natura al di fuori di quanto previsto dalle procedure aziendali (vale a dire, 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 italiani ed esteri 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;
- d) accordare altri vantaggi di qualsiasi natura (promesse di assunzione ecc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze sopra previste;
- e) riconoscere compensi in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;
- f) presentare dichiarazioni non veritiere o incomplete, o comunque indurre in errore, organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;



- g) porre in essere artifici e/o raggiri, tali da indurre in errore e da arrecare un danno allo Stato o ad altro ente pubblico o all'Unione Europea o ad organismi di diritto pubblico internazionale per realizzare un ingiusto profitto;
- h) promettere e/o versare somme, beni in natura e/o altri benefici nei rapporti con i rappresentanti delle forze politiche e/o di associazioni portatrici di interessi, per promuovere o favorire interessi della Società, anche a seguito di illecite pressioni;
- i) destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;
- j) sfruttare relazioni esistenti con un pubblico ufficiale o con un incaricato di un pubblico servizio, fungendo da intermediario "illecito" in cambio di un interesse o vantaggio che possa andare a favore della Società;
- k) accedere senza autorizzazione ai sistemi informatici della Pubblica Amministrazione per ottenere e/o modificare informazioni nell'interesse o a vantaggio della Società.
- l) favorire, nei processi d'acquisto, fornitori e sub-fornitori segnalati dai rappresentanti stessi della Pubblica Amministrazione come *condicio sine qua non* per il futuro svolgimento delle attività (es. affidamento della commessa, concessione del finanziamento agevolato);
- m) commettere frodi nell'esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali che derivano da un contratto di fornitura concluso con lo Stato, o con un altro ente pubblico, ovvero con un'impresa esercente servizi pubblici o di pubblica necessità.

3.A Principi per la prevenzione dei reati contro la Pubblica Amministrazione

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste specifiche procedure; in particolare:

- a) i rapporti nei confronti della Pubblica Amministrazione, per le suddette aree di attività a rischio, devono essere gestiti in modo unitario, procedendo alla nomina di un apposito responsabile per ogni operazione o pluralità di operazioni (in caso di particolare ripetitività delle stesse) svolte nelle aree di attività a rischio;
- b) di ogni operazione a rischio occorre dare debita evidenza per iscritto in modo che siano ricostruibili la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- c) non vi deve essere identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse operazioni i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
- d) i documenti riguardanti l'attività d'impresa devono essere archiviati e conservati, a cura della funzione competente, in conformità alla normativa sulla privacy ed al relativo regolamento aziendale sulla privacy adottato da SGI.



- e) nessuno tipo di pagamento può essere effettuato in contanti o in natura, salva specifica preventiva autorizzazione da parte della funzione Amministrazione Finanza e Controllo per le operazioni di cassa di importo inferiore a *Euro 2.500,00 (duemilacinquecento)*;
- f) la scelta di consulenti esterni deve essere motivata ed avvenire sulla base di requisiti di professionalità, indipendenza, competenza e congruità dei costi;
- g) non devono essere corrisposti compensi, provvigioni o commissioni ad agenti, partners commerciali, collaboratori e/o fornitori in misura non congrua rispetto alle prestazioni rese alla Società e/o comunque non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da tariffe;
- h) i sistemi di remunerazione premianti i dipendenti e collaboratori devono rispondere a obiettivi realistici, misurabili, motivati e coerenti con le mansioni e l'attività svolta e con le responsabilità affidate;
- i) i contratti con collaboratori, agenti, distributori e fornitori devono contenere clausole e condizioni che richiamino alla conoscenza e al rispetto del d.lgs 231/2001 e del Codice Etico di SGI;
- j) le dichiarazioni rese a organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere effettuato, ove previsto, apposito rendiconto;
- k) coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività devono riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.



PARTE SPECIALE “B”

I REATI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI E REATI DI CYBER SECURITY

In questa *parte speciale* sono individuate le aree di attività nel cui ambito possono essere commessi i reati informatici e di cyber security nonché di trattamento illecito di dati, di cui al d.lgs. 231/2001, così come identificati nell'Allegato 1).

1.B Potenziali aree a rischio

In considerazione delle attività svolte dalla Società e della struttura interna adottata, ai sensi dell'art. 6 del d.lgs. 231/2001, sono individuate le seguenti categorie di operazioni ed attività a rischio, nelle quali potrebbero essere commessi i reati previsti dall'art. 24 bis, 25 novies del d.lgs. 231/2001:

- gestione e monitoraggio degli accessi ai sistemi informatici e telematici, con riferimento alle seguenti particolari attività di:
 - a) gestione del profilo utente e del processo di autenticazione;
 - b) gestione e protezione della postazione di lavoro;
 - c) gestione degli accessi verso l'esterno;
 - d) gestione e protezione delle reti;
 - e) gestione degli output di sistema e dei dispositivi di memorizzazione;
 - f) sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.);
 - g) affidamento a terzi di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici dell'azienda.

2.B Principi di comportamento e controllo nelle principali aree di rischio

SGI, conscia dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale, si è posta come obiettivo l'adozione di efficaci politiche di sicurezza informatica e di trattamento dei dati; in particolare, tale sicurezza viene perseguita attraverso la protezione dei sistemi e delle informazioni dai potenziali attacchi (secondo una direttrice organizzativa, mirata alla creazione di una cultura aziendale attenta agli aspetti della sicurezza e a una direttrice tecnologica, attraverso l'utilizzo di strumenti atti prevenire e a reagire a fronte delle diverse tipologie di attacchi) e la garanzia della massima continuità del servizio.

Ciò posto, è vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24 bis del d.lgs. 231/2001). Sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

Al fine di evitare il verificarsi dei reati informatici, previsti dal d.lgs. 231/2001, tutti i Destinatari devono attenersi alle specifiche regole e procedure che sono e saranno predisposte e diffuse dalla Società, così come richiamate nelle dispense informative consegnate dalla Società ai dipendenti.



In particolare, è fatto divieto di:

- a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- b) accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- c) accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e/o cancellare dati e/o informazioni;
- d) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- e) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- f) svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- g) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- h) installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- i) svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- j) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- k) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

3.B Principi per la prevenzione dei reati informatici, di cybersecurity e di trattamento illecito di dati

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate sono previste specifiche procedure; in particolare:

- a) utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
- b) non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi;
- c) in caso di smarrimento o furto, informare tempestivamente i Sistemi Informativi e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;



- d) evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente approvate dall'Area Sistemi Informativi o la cui provenienza sia dubbia;
- e) evitare di trasferire all'esterno dell'Azienda e/o trasmettere *files*, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Azienda stessa o di altra società del Gruppo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
- f) evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc...);
- g) evitare l'utilizzo di *passwords* di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi; qualora l'utente venisse a conoscenza della *password* di altro utente, è tenuto a darne immediata notizia all'amministratore di sistema;
- h) evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- i) utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
- j) rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
- k) impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa;
- l) astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- m) astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- n) osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda;
- o) osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.



PARTE SPECIALE "C"

I REATI SOCIETARI

In questa parte speciale sono individuate le aree di attività nel cui ambito possono essere commessi i reati societari di cui al d.lgs. 231/2001, così come identificati nell'Allegato 1).

1.C Potenziali aree a rischio

In considerazione delle attività svolte dalla Società e dalla struttura interna adottata, ai sensi dell'art. 6 del d.lgs. 231/2001, sono individuate le seguenti categorie di operazioni ed attività a rischio, nelle quali potrebbero essere commessi i reati previsti dall'art. 25 *ter* del d.lgs. 231/2001:

- a) predisposizione di comunicazioni riguardanti la situazione economica, patrimoniale e finanziaria della Società, ivi inclusi i bilanci e le relazioni periodiche;
- b) rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nei bilanci, nelle relazioni e in altri documenti di impresa;
- c) documentazione, archiviazione e conservazione delle informazioni relative all'attività di impresa;
- d) comunicazioni ad autorità pubbliche competenti;
- e) gestione dei rapporti con la società di revisione;
- f) gestione dei rapporti con le Autorità Pubbliche di Vigilanza;
- g) selezione e gestione del personale;
- h) gestione dei rapporti commerciali con i fornitori di acquisti tecnici e servizi;
- i) assegnazione e gestione di incarichi di consulenza e di collaborazione esterna;
- j) gestione delle attività di vendite di servizi;
- k) concessione di erogazioni liberali, sponsorizzazioni, donazione di beni, etc.;
- l) assegnazione e controllo sull'impiego dei *benefit* aziendali (auto aziendali, cellulari, carte di credito, PC, etc.).

2.C Principi di comportamento e controllo nelle principali aree di rischio

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 *ter* del d.lgs. 231/2001). Sono altresì proibite le violazioni dei principi e delle procedure aziendali previste nella presente Parte Speciale.

Al fine di evitare il perfezionamento dei reati societari previsti dal d.lgs. 231/2001, tutti i Destinatari devono attenersi alle seguenti condotte:

- a) agire, ciascuno secondo la propria funzione, in modo corretto, trasparente e conforme alle norme di legge, di regolamento, alle procedure aziendali esistenti, ai principi generalmente riconosciuti di tenuta della contabilità;
- b) mantenere una condotta improntata ai principi di correttezza, trasparenza e collaborazione nello svolgimento delle procedure volte alla formazione del bilancio, delle situazioni contabili periodiche e delle comunicazioni sociali in generale;



- c) mantenere una condotta improntata ai principi di correttezza, trasparenza e collaborazione nell'acquisizione, elaborazione e comunicazione delle informazioni destinate a consentire agli azionisti, alle istituzioni e al pubblico di avere un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
- d) assicurare il regolare funzionamento della Società e degli organi sociali, agevolando e garantendo ogni forma di controllo interno;
- e) osservare tutte le norme poste dalla legge a tutela dell'integrità del capitale sociale;
- f) rispettare, in caso di riduzione del capitale sociale, di fusione e/o di scissione, le norme di legge poste a tutela dei creditori;
- g) effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di controllo da queste esercitate.
- h) verificare, mediante il controllo esercitato dai responsabili delle diverse aree, che la selezione del personale, dei fornitori e dei consulenti sia svolta in modo lecito e regolare.

In conformità a tali principi è fatto pertanto divieto di:

- a) predisporre o comunicare dati falsi o comunque suscettibili di fornire una descrizione non corretta della situazione economica, patrimoniale e finanziaria della Società;
- b) omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;
- c) restituire conferimenti ai soci e esentare i soci dall'effettuarli, al di fuori dei casi specificatamente previsti dalla legge;
- d) ripartire utili non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve che non possono essere ripartite per legge;
- e) effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;
- f) procedere in ogni modo a formazione o aumento fittizi del capitale sociale;
- g) tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del collegio sindacale o della società di revisione;
- h) omettere di effettuare, con la dovuta chiarezza, completezza e tempestività, nei confronti delle autorità competenti, le comunicazioni previste per legge;
- i) porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle autorità pubbliche, anche in sede di ispezioni.



- j) accordare vantaggi di qualsiasi natura (promesse di assunzione, etc.) in favore di rappresentanti di altre società al fine di assicurare un qualsiasi vantaggio per l'azienda;
- k) riconoscere compensi in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere;
- l) promettere e/o versare somme, beni in natura e/o altri benefici nei rapporti con i rappresentanti di altre società, per promuovere o favorire interessi dell'azienda, anche a seguito di illecite promesse;
- m) offrire o promettere denaro o altra utilità non dovuti per ottenere un indebito vantaggio tramite il compimento / l'omissione di un atto in violazione di obblighi d'ufficio o di fedeltà;
- n) compiere / omettere un atto in violazione di obblighi d'ufficio o di fedeltà a fronte di un'offerta o promessa di denaro o altra utilità non dovuti per ottenere un indebito vantaggio.

3.C Principi per la prevenzione dei reati societari

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste specifiche procedure; in particolare:

- a) ogni comunicazione esterna deve essere effettuata per iscritto e per ogni comunicazione obbligatoria per legge occorre poter ricostruire la formazione degli atti e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- b) non vi deve essere identità soggettiva fra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse operazioni i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
- c) i documenti riguardanti l'attività d'impresa devono essere archiviati e conservati, a cura della funzione competente, con modalità tali, ove richiesto dalla legge, da non permetterne la modificazione successiva, se non con apposita evidenza;
- d) nessuno tipo di pagamento può essere effettuato in contanti o in natura, salva specifica preventiva autorizzazione da parte della funzione Amministrazione Finanza e Controllo per le operazioni di cassa di importo inferiore a *Euro 2.500,00 (duemilacinquecento)*;
- e) la scelta dei fornitori e dei consulenti esterni deve essere motivata ed avvenire sulla base di requisiti di professionalità, indipendenza e competenza;
- f) la selezione del personale e le richieste di assunzioni devono essere autorizzate dal responsabile competente secondo le procedure interne;
- g) i sistemi di remunerazione premianti ai dipendenti e collaboratori devono rispondere a obiettivi realistici e coerenti con le mansioni e l'attività svolta e con le responsabilità affidate;



- h) coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività devono porre particolare attenzione in riferimento agli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità;
- i) le concessioni di erogazioni liberali, sponsorizzazioni, donazioni di beni, devono essere direttamente ed esclusivamente connesse all'attività aziendale e devono avere delle soglie di valore massimo prestabilite dalla Società;
- j) l'assegnazione dei *benefits* aziendali sia motivata, in ragione del ruolo e della mansione del personale beneficiario;

L'Organismo di Vigilanza propone le modifiche e le eventuali integrazioni delle prescrizioni di cui sopra e delle relative procedure di attuazione.



PARTE SPECIALE "D"

I REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI E GRAVISSIME, COMMESSI CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

In questa parte speciale sono individuate le aree di attività nel cui ambito possono essere commessi i reati di omicidio colposo e lesioni colpose gravi e gravissime, di cui al d.lgs. 231/2001, così come identificati nell'Allegato 1).

1.D Potenziali aree a rischio

In considerazione delle attività svolte dalla Società e della struttura interna adottata, ai sensi dell'art. 6 del d.lgs. 231/2001, nonché sulla base del documento di valutazione dei rischi, predisposto ai sensi del Decreto Legislativo 9 aprile 2008, n. 81 (Testo Unico Sicurezza), sono individuate le seguenti categorie di operazioni ed attività a rischio, nelle quali potrebbero essere commessi i reati previsti dall'art. 25 septies del d.lgs. 231/2001:

- a) utilizzo di attrezzature non a norma;
- b) mancanza di informazione e formazione sull'attività lavorativa in particolar modo sulle attività lavorative a rischio;
- c) mancata sorveglianza dei presidi antincendio;
- d) inosservanza delle procedure di gestione delle emergenze;
- e) interventi su parti attive di impianti elettrici;
- f) accesso, transito e permanenza nei locali in uso alla Società, nello svolgimento delle sue attività da parte di dipendenti, collaboratori, agenti, fornitori, clienti e/o qualsiasi altro soggetto esterno.

2.D Principi di comportamento e controllo nelle principali aree di rischio

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 septies del d.lgs. 231/2001). Sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

Al fine di evitare il verificarsi dei reati di omicidio colposo e lesioni colpose gravi e gravissime, previsti dal d.lgs. 231/2001, tutti i Destinatari devono attenersi alle specifiche regole e procedure che sono e saranno predisposte e diffuse dalla Società ai sensi del Decreto Legislativo 9 aprile 2008, n. 81 (Testo Unico Sicurezza), nonché alle seguenti condotte:

- a) osservare rigorosamente tutte le leggi e i regolamenti in materia di sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro che disciplinano l'accesso, il transito e lo svolgimento delle attività lavorative presso i locali in uso alla Società;
- b) partecipare ai corsi organizzati dalla Società in materia di sicurezza sul lavoro e sulla tutela dell'igiene e salute sul lavoro e sullo svolgimento delle specifiche mansioni, ai quali sono invitati;



- c) utilizzare i dispositivi di protezione individuali forniti dalla Società ai propri dipendenti, conformemente alle normative vigenti e in funzione delle mansioni svolte;
- d) segnalare alle funzioni competenti (RSPPA – responsabile dei Servizi di Prevenzione e Protezione Aziendale, RLSSA responsabile dei Lavoratori per la Sicurezza, Salute e Ambiente) ed all’Organismo di Vigilanza eventuali inefficienze dei dispositivi di protezione individuali ovvero di altri presidi a tutela della sicurezza sul lavoro e sulla tutela dell’igiene e salute sul lavoro;

In conformità a tali principi è fatto pertanto divieto di:

- a) utilizzare, nello svolgimento delle attività identificate a rischio, attrezzature, strumenti, materiali e dispositivi di protezione individuali non adeguati e non conformi alle normative vigenti per le specifiche operazioni da svolgere;
- b) disattivare o rendere anche parzialmente inefficienti dispositivi individuali o collettivi di protezione;
- c) svolgere attività ed operazioni al di fuori delle aree specificatamente identificate per gli interventi richiesti;
- d) accedere ad aree di lavoro alle quali non si è autorizzati.

3.D Principi per la prevenzione dei reati di omicidio colposo e lesioni colpose gravi e gravissime

Per le attività nell’ambito delle categorie di operazioni a rischio sopra individuate e nell’ambito specifico della gestione della sicurezza sul lavoro e della tutela dell’igiene e salute sul lavoro, nel rispetto di quanto previsto dal Decreto Legislativo 9 aprile 2008, n. 81 (Testo Unico Sicurezza), sono previste nel Documento di valutazione dei rischi specifiche procedure; in particolare:

- a) devono essere periodicamente individuati dalla Società i rischi in materia di sicurezza e tutela dell’igiene e salute sul lavoro, tenendo in adeguata considerazione: la struttura aziendale, la natura delle attività, l’ubicazione dei locali e delle aree di lavoro, l’organizzazione del personale, attrezzature e impianti;
- b) deve essere periodicamente aggiornato il documento di valutazione dei rischi adottato ai sensi del Decreto Legislativo 9 aprile 2008, n. 81 (Testo Unico Sicurezza);
- c) i lavoratori devono essere necessariamente informati circa le procedure adottate dalla Società al fine di ridurre i rischi in materia di sicurezza e tutela dell’igiene e salute sul lavoro;
- d) devono essere periodicamente definiti ed aggiornati il piano di intervento delle azioni di prevenzione e protezione sulla base del risultato della valutazione dei rischi effettuata, nonché i programmi di informazione e formazione dei lavoratori ai fini della sicurezza e della protezione della loro salute;



- e) i dirigenti e i preposti sono tenuti a sorvegliare sull'effettivo rispetto delle procedure proposte e diffuse dalla Società e sulla adozione delle adeguate misure di prevenzione e protezione, comunicando tempestivamente eventuali eccezioni e criticità;
- f) i lavoratori in base agli specifici rischi individuati devono ricevere adeguata informazione e formazione in merito alle misure di prevenzione e protezione da adottare nello svolgimento delle proprie attività e gestione delle emergenze; per ciascun dipendente viene previsto uno specifico piano di addestramento individuale;
- g) alle ispezioni giudiziarie e amministrative devono partecipare i soggetti a ciò espressamente delegati e l'Organismo di Vigilanza dovrà essere prontamente informato sull'inizio di ogni attività ispettiva dalla direzione aziendale interessata.

Infine, in caso di realizzazione di lavori, la Società, nella veste di "committente" ai sensi dell'art. 89 D.Lgs. 81/2008 dà attuazione alle disposizioni del Titolo IV del medesimo decreto e precisamente:

- i) programma, organizza e cura, sotto la propria responsabilità, la corretta applicazione, nell'esecuzione delle attività di cantiere, di quanto espressamente prescritto dalle norme vigenti in materia di prevenzione degli infortuni e di tutela della salute e della sicurezza sui luoghi di lavoro, adottando le necessarie misure;
- ii) affida l'incarico di "responsabile dei lavori" ai sensi dell'art. 89 D.Lgs. 81/2008 a professionista esterno, affinché provveda a dare attuazione agli adempimenti posti a carico del committente o, in casi di nomina, del responsabile dei lavori dagli artt. 90 ss. del decreto stesso;
- iii) tramite il responsabile dei lavori, assicura la conformità del cantiere con la normativa prevenzionistica applicabile, avendo cura che il cantiere sia dotato di tutta la documentazione autorizzativa richiesta dalla legge e delle necessarie dotazioni tecniche e operative prescritte dalle norme di riferimento.



PARTE SPECIALE "E"

I REATI DI RICETTAZIONE, RICICLAGGIO E AUTORICICLAGGIO

In questa *parte speciale* sono individuate le aree di attività nel cui ambito possono essere commessi i reati di ricettazione e riciclaggio, di cui al d.lgs. 231/2001, così come identificati nell'Allegato 1).

1.E Potenziali aree a rischio

In considerazione delle attività svolte dalla Società e della struttura interna adottata, ai sensi dell'art. 6 del d.lgs. 231/2001, sono individuate le seguenti categorie di operazioni ed attività a rischio, nelle quali potrebbero essere commessi i reati previsti dall'art. 25 *octies* del d.lgs. 231/2001:

- a) gestione delle risorse finanziarie (ad es. poteri di disposizione su c/c bancario, emissione assegni, ecc.);
- b) valutazione della clientela;
- c) gestione degli acquisti;
- d) con riguardo al reato di **autoriciclaggio**, in particolare, emerge, quale sensibile area di rischio, quella legata agli adempimenti tributari relativamente al reimpiego del profitto di un eventuale illecito tributario nel business della Società.

2.E Principi di comportamento e controllo nelle principali aree di rischio

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 *octies* del d.lgs. 231/2001). Sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

Al fine di evitare il perfezionamento dei reati di ricettazione, riciclaggio e autoriciclaggio previsti dal d.lgs. 231/2001, tutti i Destinatari devono attenersi alle seguenti condotte:

- a) conservare la documentazione attraverso la quale sia ricostruibile la formazione di un atto e i relativi livelli autorizzativi, a garanzia della trasparenza delle scelte effettuate;
- b) rispettare il principio secondo cui non vi deve essere la sovrapposizione tra coloro che assumono o attuano le decisioni, coloro che devono dare evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
- c) non corrispondere compensi, provvigioni o commissioni a consulenti, collaboratori, agenti o a soggetti pubblici in misura non congrui rispetto alle prestazioni rese alla Società o non conformi all'incarico conferito;
- d) attribuire premi ai dipendenti e collaboratori coerenti con le mansioni e l'attività svolta e con la responsabilità affidate;
- e) informare l'Organismo di Vigilanza in caso di profili di anomalia nei rapporti finanziari con i fornitori e/o i clienti in relazione alle modalità, al luogo o al destinatario di pagamenti;



- f) fissare le condizioni commerciali sulla base di processi decisionali trasparenti e ricostruibili nel tempo, e siano autorizzate esclusivamente da soggetti dotati di idonei poteri secondo un sistema di deleghe e procure coerente con le responsabilità organizzative e gestionali.

In conformità a tali principi è fatto pertanto divieto di:

- a) non effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità Pubbliche;
- b) omettere dati ed informazioni imposti dalla legge sulla normativa antiriciclaggio;
- c) porre in essere comportamenti che impediscano materialmente o che comunque ostacolino lo svolgimento dell'attività di controllo da chiunque sia preposto a tale ruolo (mediamente l'occultamento di documenti o l'uso di altri mezzi fraudolenti);
- d) omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni previste dalle leggi e dalla normativa sul riciclaggio;
- e) porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità Pubbliche.

3.E Principi per la prevenzione dei reati di ricettazione e riciclaggio

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste specifiche procedure; in particolare che:

- a) vi sia separazione dei compiti tra chi autorizza, chi controlla e chi esegue le operazioni;
- b) siano individuati degli indicatori di anomalia per identificare eventuali transazioni "a rischio" o "sospette" con la controparte sulla base di:
 - profilo soggettivo della controparte (ad es. esistenza di precedenti penali, reputazione opinabile, ammissioni o dichiarazioni da parte della controparte in ordine al proprio coinvolgimento in attività criminose);
 - comportamento della controparte (ad es. comportamenti ambigui, mancanza di dati occorrenti per la realizzazione delle transazioni o reticenza a fornirli);
 - dislocazione territoriale della controparte (ad es. transazioni effettuate in paesi off-shore);
 - profilo economico-patrimoniale dell'operazione (ad es. operazioni non usuali per tipologia, frequenza, tempistica, importo, dislocazione geografica);
- c) la scelta e valutazione della controparte avvenga sulla base di requisiti predeterminati dalla Società e dalla stessa rivisti e, se del caso, aggiornati con regolare periodicità;
- d) la scelta e la valutazione dei fornitori e dei clienti italiani ed esteri avvenga attraverso l'analisi di documentazione legale e societaria (ad es. "certificazione antimafia", visura camerale).



PARTE SPECIALE "F"

I DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

In questa *parte speciale* sono individuate le aree di attività nel cui ambito possono essere commessi delitti in materia di violazione del diritto d'autore.

1.F Potenziali aree a rischio

In considerazione delle attività svolte dalla Società e della struttura interna adottata, ai sensi dell'art. 6 del d.lgs. 231/2001, sono individuate le seguenti categorie di operazioni ed attività a rischio, nelle quali potrebbero essere commessi i reati previsti dall'art. 25 *novies* del d.lgs. 231/2001:

- a) acquisto e gestione del sistema informativo e delle licenze software;
- b) acquisto ed utilizzo di opere letterarie, musicali o audiovisive tutelate dal diritto d'autore per attività aziendali (ad es. marketing, training, intranet, etc.).

2.F Principi per la prevenzione dei delitti in materia di violazione del diritto d'autore

Per le operazioni riguardanti l'acquisto e gestione del sistema informativo e delle licenze software, è previsto che:

- a) siano definiti i criteri e le modalità per la gestione dei sistemi software;
- b) siano definiti e attivati criteri e modalità per controllare l'acquisto e l'uso di software;
- c) siano definite le modalità di utilizzo dei personal computer, di installazione e utilizzo di software, di utilizzo di internet.

Per le operazioni riguardanti l'acquisto ed utilizzo di opere letterarie, musicali o audiovisive tutelate dal diritto d'autore per attività aziendali (ad es. marketing, training, intranet, etc.), è previsto che:

- a) siano definiti criteri e modalità per l'accesso da parte degli utenti a siti di download di contenuti;
- b) siano previsti controlli sulle attività che comportano l'utilizzo di opere tutelate dal diritto d'autore.



PARTE SPECIALE "G"

I REATI AMBIENTALI

In questa parte speciale sono individuate le aree di attività nel cui ambito possono essere commessi i reati ambientali di cui al d.lgs. 231/2001, così come identificati nell'Allegato 1).

1.G Potenziali aree a rischio

In considerazione delle attività svolte dalla Società e della struttura interna adottata, ai sensi dell'art. 6 del d.lgs. 231/2001, sono individuate le seguenti categorie di operazioni ed attività a rischio, nelle quali potrebbero essere commessi i reati previsti dall'art. 25-*undecies* del d.lgs. 231/2001:

- a) raccolta, trasporto e smaltimento di rifiuti pericolosi e non pericolosi;
- b) gestione amministrativa e documentale dei processi inerenti la gestione dei rifiuti;

2.G Principi di comportamento e controllo nelle principali aree di rischio

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 *undecies* del d.lgs. 231/2001). Sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

Al fine di evitare il perfezionamento dei reati ambientali previsti dal d.lgs. 231/2001, tutti i Destinatari devono attenersi alle seguenti condotte:

- a) tenere in considerazione, nella selezione dei prodotti e dei servizi da acquistare, anche dell'impatto ambientale e degli oneri di smaltimento degli stessi al termine della loro vita utile;
- b) svolgere l'attività di smaltimento dei rifiuti con il minor impatto ambientale possibile;
- c) svolgere gli adempimenti e la predisposizione della relativa documentazione nei confronti degli Enti della Pubblica Amministrazione preposti al controllo della normativa ambientale nel rispetto delle normative vigenti, nazionali e/o comunitarie;
- d) diffondere ad ogni livello dell'organizzazione la cultura del rispetto dell'ambiente.

In conformità a tali principi è fatto pertanto divieto di

- a) abbandonare o depositare in modo incontrollato i rifiuti;
- b) miscelare categorie diverse di rifiuti pericolosi (oppure rifiuti pericolosi con non pericolosi);
- c) violare gli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari per la gestione dei rifiuti;



- d) falsificare, alterare o compilare i certificati di analisi dei rifiuti, riportando informazioni non corrette sulla natura, composizione e caratteristiche chimico-fisiche dei rifiuti stessi;
- e) impedire l'attività di controllo ai funzionari degli enti competenti, ovvero ostacolarne in qualsiasi modo le relative verifiche o indagini.

3.G Principi per la prevenzione dei reati ambientali

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate, sono previste specifiche procedure; in particolare:

- a) è assicurata la corretta differenziazione dei rifiuti;
- b) deve essere prevenuta ogni miscelazione illecita;
- c) deve essere assicurata la disponibilità della documentazione relativa;
- d) deve essere valutata l'eventuale necessità di autorizzazioni per lo svolgimento delle attività di raccolta e attivate le necessarie procedure per l'ottenimento delle stesse.



PARTE SPECIALE H

I REATI CONTRO L'AMMINISTRAZIONE DELLE GIUSTIZIA

In questa parte speciale sono individuate le aree di attività nel cui ambito può essere commesso il delitto di cui all'art. 377-bis c.p., previsto dall'art. 25-decies D.Lgs. 231/2001, di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

1.H Potenziali aree a rischio

La fattispecie di cui all'art. 377-bis c.p. risulta non essere ricollegabile a specifiche attività d'impresa svolte dalla Società stessa, oltre che non inquadrabile in uno specifico sistema di controlli, posto che astrattamente potrebbe essere commesso ad ogni livello aziendale ed in un numero pressoché infinito di modalità.

2.H Principi di comportamento e di prevenzione

Si ritiene che i principi contenuti nel Codice Etico costituiscano lo strumento più adeguato per prevenire la commissione del delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

Tutti i destinatari del Modello, quindi, al fine di evitare condotte che possano integrare tale delitto, adottano prassi e comportamenti che siano rispettosi del Codice Etico; in particolare, i destinatari del Modello seguono i principi etici della Società relativi ai rapporti con la PA.



PARTE SPECIALE I

REATI DI IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE

In questa parte speciale sono individuate le aree di attività nel cui ambito può essere commesso il reato previsto dall'art. 25-duodecies del d.lgs. 231/2001, così come identificato nell'Allegato 1).

1.1 Potenziali aree a rischio

In considerazione delle attività svolte dalla Società e della struttura interna adottata, ai sensi dell'art. 6 del d.lgs. 231/2001, sono individuate le seguenti categorie di operazioni ed attività a rischio, nelle quali potrebbe essere commesso il reato previsto dall'art. 25-duodecies del d.lgs. 231/2001:

- a. assunzione del personale, con particolare riferimento ai cittadini extracomunitari;
- b. comunicazione dell'assunzione di cittadini extracomunitari agli enti pubblici (Sportello Unico per l'immigrazione, Centro per l'impiego, ecc) in conformità con la normativa vigente;
- c. monitoraggio delle scadenze dei permessi di soggiorno e gestione dei rinnovi;
- d. gestione dei contratti con appaltatori ed altre aziende.

2.1 Principi di comportamento e controllo nelle principali aree di rischio

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare sopra considerate (art. 25-duodecies del d.lgs. 231/2001).

Al fine di evitare il verificarsi del suddetto reato, tutti i Destinatari devono attenersi alle specifiche regole e procedure aziendali, nonché alle seguenti regole di condotta.

È fatto obbligo ai soggetti impegnati nelle aree sensibili rispetto al reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare osservare in modo rigoroso le disposizioni di legge concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, ed in particolare di:

- a) impiegare soltanto lavoratori extracomunitari in possesso di valido permesso di soggiorno;
- b) richiedere ai lavoratori extracomunitari di esibire il permesso di soggiorno all'atto dell'assunzione e a seguito del rinnovo dello stesso;
- c) monitorare le scadenze dei permessi di soggiorno;
- d) inviare comunicazioni ai dipendenti in prossimità della scadenza del permesso di soggiorno;
- e) archiviare correttamente la documentazione relativa al permesso di soggiorno;
- f) inviare le comunicazioni agli enti pubblici competenti, assicurando che le informazioni trasmesse siano veritiere, complete e basate su un'idonea documentazione;



- g) osservare le procedure aziendali interne per garantire il rispetto delle disposizioni legislative vigenti in materia di rapporti di lavoro;
- h) operare nel rispetto delle disposizioni contenute nel presente Modello.

È fatto divieto al datore di lavoro di impiegare lavoratori stranieri del tutto privi di permesso di soggiorno o con un permesso revocato o scaduto, del quale non sia stata presentata domanda di rinnovo, documentata dalla relativa ricevuta postale.

3.1 Principi per la prevenzione del reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare

Per le attività nell'ambito delle categorie di operazioni a rischio sopra individuate sono previste specifiche procedure; in particolare:

- a) l'assunzione dei cittadini extracomunitari deve avvenire nel rispetto delle procedure aziendali previste per l'assunzione del personale;
- b) per favorire i controlli sull'attività in questione ai candidati va espressamente richiesta la presentazione del permesso di soggiorno e, in caso di assunzione, copia del documento permesso di soggiorno dovrà essere archiviata nel dossier personale;
- c) l'assunzione di cittadini extracomunitari va prontamente segnalata all'Organismo di Vigilanza;
- d) nel caso di assunzione di cittadini extracomunitari, la funzione responsabile risorse umane deve comunicare l'instaurazione del rapporto di lavoro agli organi preposti territorialmente competenti, assicurando la correttezza dei dati trasmessi per il lavoratore extracomunitario relativamente a: titolo del permesso di soggiorno; numero del titolo di soggiorno; motivo del soggiorno; scadenza del titolo di soggiorno; questura che ha rilasciato il permesso di soggiorno;
- e) al fine di ridurre il rischio di impiego di dipendenti il cui permesso di soggiorno è scaduto, la funzione responsabile risorse umane effettua le seguenti attività:
 - esegue periodicamente un monitoraggio delle scadenze dei permessi di soggiorno dei lavoratori extracomunitari;
 - invia, con congruo preavviso rispetto alla data di scadenza del permesso di soggiorno, una comunicazione scritta al dipendente, evidenziando l'approssimarsi della data di scadenza del permesso di soggiorno e richiedendo di consegnare all'azienda copia del documento attestante l'avvenuto rinnovo;
 - trasmette in via telematica, anche per il tramite di soggetti esterni, le informazioni relative al rinnovo del permesso di soggiorno al Centro per l'impiego;
- f) nell'ottica di prevenire il rischio che per la Società possa configurarsi, anche soltanto in via indiretta e potenziale, una responsabilità per l'impiego di cittadini extracomunitari



privi del permesso di soggiorno da parte di appaltatori ed altri fornitori, i relativi contratti che ne regolano i rapporti devono contenere specifiche clausole che prevedano l'impegno della controparte di assicurare che, nel caso in cui nell'esecuzione del contratto siano impiegati lavoratori extracomunitari, questi ultimi siano in possesso di regolare permesso di soggiorno e di sollevare la Società da qualsiasi responsabilità che dovesse derivare dal mancato adempimento di tale obbligo; nel caso di contratti di appalto, nell'elenco nominativo dei soggetti da fornire alla Società, per i lavoratori extracomunitari devono essere comunicati gli estremi del permesso di soggiorno (numero del titolo e scadenza).

L'Organismo di Vigilanza cura che le procedure operative aziendali diano effettiva e piena attuazione ai principi e alle misure di prevenzione sopra indicate.



PARTE SPECIALE L

I REATI TRIBUTARI

In questa parte speciale sono individuate le aree di attività nel cui ambito possono essere commessi i reati previsti dall'art. 25-quinquiesdecies del D.lgs. 231/2001. In particolare, ai sensi dell'art. 25-*quinquiesdecies*, sono stati introdotti i seguenti reati tributari:

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, commi 1 e 2-bis, D. lgs. 74/2000);
- dichiarazione fraudolenta mediante altri artifici (art. 3, D. lgs. 74/2000);
- emissione di fatture o altri documenti per operazioni inesistenti (art. 8, commi 1 e 2-bis, D. lgs. 74/2000);
- occultamento o distruzione di documenti contabili (art. 10, D. lgs. 74/2000);
- sottrazione fraudolenta al pagamento delle imposte (art. 11, D. lgs. 74/2000).

Sono altresì stati introdotti dal legislatore con il Decreto Legislativo 14 luglio n. 75/2020 di attuazione della Direttiva PIF (Direttiva (UE) 2017/1371 i seguenti reati tributari:

- dichiarazione infedele in caso di gravi frodi IVA transfrontaliere (art. 4 D.Lgs. 74/200);
- omessa dichiarazione in caso di gravi frodi IVA transfrontaliere (art. 5 D.Lgs. 74/200);
- indebita compensazione in caso di gravi frodi IVA transfrontaliere (art. 10 quater D.Lgs. 74/200).

1. L Potenziali aree a rischio

In considerazione delle attività svolte dalla Società e della struttura interna adottata, ai sensi dell'art. 6 del d.lgs. 231/2001, sono individuate le seguenti categorie di operazioni ed attività a rischio, nelle quali potrebbe essere commesso il reato previsto dall'art. 25-quinquiesdecies del D.lgs. 231/2001:

- a. acquisto di lavori, beni e servizi;
- b. attività che prevedono il ricorso (diretto o indiretto) a manodopera, ad esempio affidamento di appalti;
- c. selezione e monitoraggio dei fornitori;
- d. eventi e sponsorizzazioni;
- e. negoziazione/stipulazione e/o esecuzione di contratti (ivi inclusa la fase di fatturazione) con soggetti pubblici, ai quali si perviene mediante procedure aperte, ristrette o negoziate (affidamento diretto o trattativa privata o gare);
- f. omaggi regali e benefici;
- g. operazioni sul capitale e destinazione dell'utile;
- h. gestione controversie e attività giudiziali;
- i. spese di rappresentanza e spese promozionali;



- j. spese di trasferta e anticipi;
- k. contatto con gli Enti Pubblici per la gestione di rapporti, adempimenti, verifiche, ispezioni concernenti le attività aziendali in materia fiscale;
- l. gestione della tesoreria e delle transazioni finanziarie (anche infragruppo);
- m. gestione fiscale;
- n. tenuta della contabilità e predisposizione dei bilanci o delle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico;
- o. gestione degli accessi da e verso l'esterno;
- p. gestione dei profili utente e del processo di autenticazione;
- q. gestione del processo di creazione, trattamento, archiviazione dei documenti elettronici con valore probatorio.

2.L Principi di comportamento e controllo nelle principali aree di rischio

Di seguito vengono esposte le linee guida di comportamento che devono essere tenute dalla Società al fine di evitare il verificarsi di situazioni favorevoli alla commissione dei reati tributari indicati nel Decreto.

In riferimento all'attività svolta da SGI, le misure generali per la prevenzione dei delitti tributari sono:

- a) astenersi dal porre in essere qualsiasi comportamento volto ad evadere, o consentire ad altri di evadere, le imposte sui redditi o sul valore aggiunto;
- b) astenersi da compiere operazioni simulate o dall'emettere fatture, altri documenti falsi o dall'avvalersi di altri mezzi fraudolenti;
- c) tenere le scritture contabili o i documenti di cui è obbligatoria la conservazione;
- d) presentare le dichiarazioni relative alle imposte sui redditi o sul valore aggiunto.

Inoltre nell'espletamento delle attività considerate a rischio, per i soggetti ai vertici della società (ovvero dirigenti, amministratori, sindaci), nonché i consulenti, in relazione al tipo di rapporto intercorrente con la Società, è vietato:

- a) evadere le imposte sui redditi o sul valore aggiunto;
- b) avvalersi, emettere o rilasciare fatture o altri documenti per operazioni inesistenti;
- c) indicare in fatture o altri documenti relative alle imposte sui redditi o sul valore aggiunto elementi passivi fittizi ovvero elementi attivi per un ammontare inferiore a quello effettivo;
- d) compiere operazioni simulate oggettivamente o soggettivamente, o comunque avvalersi di documenti falsi o di altri mezzi fraudolenti;
- e) consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto;
- f) occultare o distruggere in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione;



- g) alienare simulatamente o compiere altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva;
- h) indicare in una delle dichiarazioni annuali relative alle imposte sui redditi o sul valore aggiunto elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti.

3.L Principi per la prevenzione dei reati tributari

Nel processo di gestione degli adempimenti in materia fiscale, tutti i Destinatari devono attenersi alle regole di seguito indicate:

- a) le operazioni di rilevazione e registrazione delle attività e dei movimenti contabili devono essere effettuate con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza in adempimento delle norme di legge con particolare ma non esclusivo riferimento a quelle tributarie;
- b) tutti i dati e le informazioni che servono alla emissione e gestione delle fatture e degli altri documenti contabili della Società devono essere chiari e completi e rappresentare in modo veritiero la situazione economica, finanziaria e patrimoniale della Società allo scopo di consentire la corretta determinazione delle imposte dirette e indirette della Società;
- c) i dati e le informazioni sono raccolti tempestivamente, sotto la supervisione della direzione amministrativa ed elaborati da soggetti da questa incaricati ai fini della corretta predisposizione di tutti i documenti contabili rilevanti delle dichiarazioni fiscali. A richiesta della suddetta direzione, insieme ai dati e alle informazioni, devono essere trasmessi anche gli eventuali documenti e le fonti da cui sono tratte le informazioni;
- d) prima di porre in essere operazioni di natura societaria, quali ad esempio fusioni e acquisizioni, immobiliari e più in generale di rilevante complessità e/o importo, ovvero di natura non ricorrente, le stesse devono essere dettagliatamente e tempestivamente rappresentate al Consiglio di Amministrazione per consentire i necessari approfondimenti, avvalendosi ove necessario dei consulenti all'uopo preposti, al fine di garantire la piena osservanza della normativa tributaria;
- e) la rilevazione, la trasmissione e l'aggregazione dei dati e delle informazioni contabili utilizzati nel processo di fatturazione deve avvenire con modalità tali (anche per il tramite del sistema informativo aziendale) da assicurare che vi sia sempre evidenza dei passaggi del processo di formazione dei dati, e sia sempre individuabile il soggetto che ha inserito i dati nel sistema. I profili di accesso a tale sistema sono identificati dal responsabile dei sistemi informativi sotto la supervisione della direzione amministrativa.

La Società sanziona, nei limiti e nel rispetto delle disposizioni legislative vigenti applicabili, i comportamenti difforni ai principi sopra riportati, poiché non consentiti dalla legge, dal Modello e dal Codice Etico adottati dalla Società.



STUDIO GEOTECNICO ITALIANO srl

ingegneria geotecnica - ingegneria sismica - ingegneria ambientale
geologia applicata

ALLEGATO N. 1 – ELENCO REATI
MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO
AI SENSI DEL D.LGS. 231/2001

Revisione 30.03.2021



Reg. CH-20504
ISO 9001:2015
ISO 14001:2015
OHSAS 18001:2007

Sede Legale e Uffici: Centro Direzionale Milanofiori - Strada 2 - Palazzo C - Scala C3 - 20057 Assago (MI)
Tel.: +39 02 5220141 - Fax: +39 02 5691845 - Email: info@studiogeotecnico.it - P.E.C.: sgi@legalmail.it
Sito Web: www.studiogeotecnico.it - Capitale Sociale € 1.550.000,00 i.v. - R.E.A. MI 691783
Codice Fiscale e Registro Imprese di Milano Monza Brianza Lodi 00506080019 – Partita IVA IT11261240151



Allegato 1 - I REATI PREVISTI DAL D.LGS. 231/2001

- a) INDEBITA PERCEZIONE DI EROGAZIONI, TRUFFA IN DANNO DELLO STATO O DI UN ENTE PUBBLICO O DELL'UNIONE EUROPEA O PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE E FRODE INFORMATICA IN DANNO DELLO STATO O DI UN ENTE PUBBLICO E FRODE NELLE PUBBLICHE FORNITURE (Art. 24, D. Lgs. n. 231/2001)**
- *Malversazione a danno dello Stato (art. 316-bis c.p.)*
 - *Indebita percezione di erogazione a danno dello Stato (art. 316-ter c.p.)*
 - *Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)*
 - *Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art. 640, 2° comma, n. 1 c.p.)*
 - *Frode informatica (Art. 640-ter c.p.)*
 - *Frode nelle pubbliche forniture (art. 356 c.p.)*
 - *Frode ai danni del Fondo europeo agricolo (art. 2 L. 23/12/1986, n. 898)*
- b) DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (Art. 24-bis, D. Lgs. n. 231/2001)**
- *Accesso abusivo ad un sistema informatico o telematico (art. 615-ter, c.p.);*
 - *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater, c.p.);*
 - *Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies, c.p.);*
 - *Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis, c.p.);*
 - *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.);*
 - *Danneggiamento di sistemi informatici o telematici (art. 635-quater, c.p.);*
 - *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies, c.p.);*
 - *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater, c.p.);*
 - *Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies, c.p.);*
 - *Documenti informatici (art. 491-bis, c.p.);*
 - *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies, c.p.);*
 - *Violazione delle norme in materia di perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)*



c) DELITTI DI CRIMINALITÀ ORGANIZZATA (Art. 24-ter, D. Lgs n. 231/2001)

- *Associazione pe delinquere* (art. 416, c.p.);
- *Associazione di tipo mafioso* (art. 416-bis, c.p.);
- *Scambio elettorale politico-mafioso* (art. 416-ter, c.p.);
- *Sequestro di persona a scopo di rapina o di estorsione* (art. 630, c.p.);
- *Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope* (art. 74, DPR. n. 309/1990);
- *Delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo, escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110* (art. 407, 2° comma, lett. a num. 5, c.p.c.).

d) PECULATO, CONCUSSIONE, INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ, CORRUZIONE E ABUSO D'UFFICIO (Art. 25, D. Lgs. n. 231/2001)

- *Corruzione per l'esercizio della funzione* (art. 318, c.p.);
- *Pene per il corruttore* (art. 321, c.p.);
- *Istigazione alla corruzione* (art. 322, c.p.);
- *Corruzione per un atto contrario ai doveri d'ufficio* (art. 319, c.p.);
- *Corruzione in atti giudiziari* (art. 319-ter, c.p.);
- *ConcuSSIONE* (art. 317, c.p.);
- *Induzione indebita a dare o promettere utilità* (art. 319-quater, c.p.);
- *Corruzione di persona incaricata di un pubblico servizio* (art. 320, c.p.);
- *Istigazione alla corruzione* (art. 322 c.p.)
- *Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri* (art. 322-bis, c.p.);
- *Traffico di influenze illecite*
- *Peculato* (art. 314 c.p.)
- *Peculato mediante profitto dell'errore altrui* (art. 316 c.p.)
- *Abuso d'ufficio* (art. 323 c.p.)

e) FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO (Art. 25-bis, D. Lgs. n. 231/2001)

- *Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate* (art. 453, c.p.);
- *Alterazione di monete* (art. 454, c.p.);
- *Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo* (art. 460, c.p.);



- *Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461, c.p.);*
- *Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455, c.p.);*
- *Spendita di monete falsificate ricevute in buona fede (art. 457, c.p.);*
- *Uso di valori di bollo contraffatti o alterati (art. 464, c.p.);*
- *Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459, c.p.);*
- *Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473, c.p.);*
- *Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474, c.p.).*

f) DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO (Art. 25-bis. 1, D. Lgs. n. 231/2001)

- *Turbata libertà dell'industria e del commercio (art. 513, c.p.);*
- *Frode nell'esercizio del commercio (art. 515, c.p.);*
- *Vendita di sostanze alimentari non genuine come genuine (art. 516, c.p.);*
- *Vendita di prodotti industriali con segni mendaci (art. 517, c.p.);*
- *Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter, c.p.);*
- *Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater, c.p.);*
- *Illecita concorrenza con minaccia o violenza (art. 513-bis, c.p.);*
- *Frodi contro le industrie nazionali (art. 514, c.p.).*

g) REATI SOCIETARI (Art. 25-ter, D. Lgs. n. 231/2001)

- *False comunicazioni sociali (art. 2621, c.c.);*
- *Fatti di lieve entità (art. 2621-bis, c.c.);*
- *False comunicazioni sociali delle società quotate (art. 2622, c.c.);*
- *Falso in prospetto (art. 2623, c.c.);*
- *Impedito controllo (art. 2625, c.c.);*
- *Formazione fittizia del capitale (art. 2632, c.c.);*
- *Indebita restituzione dei conferimenti (art. 2626, c.c.);*
- *Illegale ripartizione degli utili e delle riserve (art. 2627, c.c.);*
- *Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628, c.c.);*
- *Operazioni in pregiudizio dei creditori (art. 2629, c.c.);*
- *Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633, c.c.);*
- *Illecita influenza sull'assemblea (art. 2636, c.c.);*
- *Aggiotaggio (art. 2637, c.c.);*
- *Omessa comunicazione del conflitto d'interessi (art. 2629-bis, c.c.);*
- *Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, c.c.);*
- *Corruzione tra privati (art. 2635, c.c.);*
- *Istigazione alla corruzione tra privati (art. 2635-bis, c.c.);*



- h) DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO (Art. 25-*quater*, D. Lgs. n. 231/2001)**
- *Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270-bis, c.p.).*
- i) PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI (Art. 25-*quater*.1., D. Lgs. n. 231/2001)**
- *Pratiche di mutilazione degli organi genitali femminili (art. 583-bis, c.p.).*
- j) DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE (Art. 25-*quinqües*, D. Lgs. n. 231/2001)**
- *Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);*
 - *Tratta delle persone (art. 601, c.p.);*
 - *Acquisto e alienazione di schiavi (art. 602, c.p.);*
 - *Intermediazione illecita e sfruttamento del lavoro (art. 603-bis, c.p.);*
 - *Prostituzione minorile (art. 600-bis, c.p.);*
 - *Pornografia minorile (600-ter, c.p.);*
 - *Pornografia virtuale (art. 600-*quater*1, c.p.);*
 - *Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-*quinqües* c.p.);*
 - *Detenzione di materiale pornografico (art. 600-*quater*, c.p.);*
 - *Adescamento di minorenni (art. 609-*undecies*, c.p.).*
- k) ABUSI DI MERCATO (Art. 25-*sexies*, D. Lgs. n. 231/2001)**
- Reati di abuso di informazioni privilegiate e di manipolazione del mercato previsti dalla parte V, titolo I-*bis*, capo II, del Testo Unico di cui al D. Lgs. 24 febbraio 1998, n. 58
- *Abuso di informazioni privilegiate (art. 184, TUF);*
 - *Manipolazione del mercato (art. 185, TUF);*
 - *Confisca (art. 187, TUF);*
 - *Abuso di informazioni privilegiate (art. 187-*bis*, TUF);*
 - *Manipolazione del mercato (art. 187-*ter* TUF).*
- l) OMICIDIO COLPOSO O LESIONI GRAVI O GRAVISSIME, COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO (Art. 25-*septies*, D. Lgs. n. 231/2001)**
- *Omicidio colposo (art. 589, c.p.);*
 - *Lesioni personali colpose (art. 590, c.p.).*
- m) RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO (Art. 25-*octies*, D. Lgs. n. 231/2001)**
- *Ricettazione (art. 648, c.p.);*
 - *Riciclaggio (art. 648-*bis*, c.p.);*
 - *Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter*, c.p.);*
 - *Autoriciclaggio (art. 648-*ter*, 1 c.p.).*



- n) DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (Art. 25-novies, D. Lgs. n. 231/2001)**
Delitti previsti dagli articoli 171, primo comma, lettera a-bis, e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies della legge 22 aprile 1941, n. 633 (Legge sul diritto d'autore).
- o) INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (Art. 25-decies, D. Lgs. n. 231/2001)**
- *Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis, c.p.);*
- p) REATI AMBIENTALI (Art. 25-undecies, D. Lgs. n. 231/2001)**
- *Inquinamento ambientale (art. 452-bis, c.p.);*
 - *Disastro ambientale (art. 452-quater, c.p.);*
 - *Delitti colposi contro l'ambiente (art. 452-quinquies, c.p.);*
 - *Delitti associativi aggravati dalle circostanze ex art. 452-octies, c.p.);*
 - *Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies, c.p.)*
 - *Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis, c.p.);*
 - *Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis, c.p.);*
 - *Violazione delle norme in materia di scarico di acque contenenti sostanze inquinanti (art. 137, commi 2-3-5-11-13, D. Lgs n. 152/2006);*
 - *Attività di gestione di rifiuti non autorizzata (art. 256, D. Lgs n. 152/2006);*
 - *Bonifica dei siti (art. 257, D. Lgs n. 152/2006);*
 - *Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258, D. Lgs n. 152/2006);*
 - *Traffico illecito di rifiuti (art. 259, D. Lgs n. 152/2006);*
 - *Attività organizzate per il traffico illecito di rifiuti (art. 260, D. Lgs n. 152/2006);*
 - *Sistema informatico di controllo della tracciabilità dei rifiuti (art. 260-bis, D. Lgs n. 152/2006);*
 - *Superamento dei valori limite di emissione se determina anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa (art. 279, comma 5 D. Lgs n. 152/2006);*
 - *Violazione di quanto previsto dal Regolamento (CE) n. 338/97 del Consiglio del 9 dicembre 1996 (artt. 1, comma1, 2, commi 1 e 2, 6, comma 4, 3-bis, comma 1, Legge n. 150/1992);*
 - *Violazione nel cessare la produzione e l'utilizzazione di sostanze lesive (art. 3, comma 6, D. Lgs. n. 549/1993);*
 - *Inquinamento colposo (art. 9 D. Lgs. n. 202/2007);*
 - *Inquinamento doloso (art. 8 D. Lgs. n. 202/2007).*



- q) IMPIEGO CITTADINI DI PAESI TERZI DI CUI IL SOGGIORNO È IRREGOLARE (Art. 25-duodecies, D. Lgs. n. 231/2001)**
- *Impiego di più di tre lavoratori stranieri con permesso di soggiorno irregolare o che siano minorenni oppure che siano sottoposti a condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'art. 603-bis c.p. (art. 22, comma 12-bis, D. Lgs. n. 286/1998).*
- r) REATI TRANSNAZIONALI COME PREVISTI DALLA LEGGE 16 MARZO 2006 N. 146 DI RATIFICA DELLA CONVENZIONE DI PALERMO SULLA CRIMINALITÀ ORGANIZZATA INTERNAZIONALE**
Art. 10 Legge n. 146/2006, Responsabilità amministrativa degli enti per i seguenti reati:
- *Associazione per delinquere (art. 416 c.p.);*
 - *Associazione per delinquere di tipo mafioso (art. 416 bis c.p.);*
 - *Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291 quater T.U. Leggi doganali);*
 - *Associazione per delinquere finalizzata allo spaccio di stupefacenti (art. 74 T.U. sugli stupefacenti);*
 - *Ricettazione (art. 648 c.p.);*
 - *Riciclaggio (artt. 648-bis e 648-ter c.p.);*
 - *Reati concernenti il traffico di migranti (art. 12, commi 3, 3-bis, 3-ter e 5, del d.lg. 25 luglio 1998, n. 286);*
 - *Reati concernenti l'intralcio alla giustizia (articoli 377-bis e 378 c.p.).*
- s) RAZZISMO E XENOFOBIA (ART. 25-TERDECIES, D.LGS. N. 231/2001)**
- t) FRODE IN COMPETIZIONI SPORTIVE, ESERCIZIO ABUSIVO DI GIOCO O DI SCOMMESSA E GIOCHI D'AZZARDO ESERCITATI A MEZZO DI APPARECCHI VIETATI (ART. 25-QUATERDECIES, D.LGS. N. 231/2001)**
- u) REATI TRIBUTARI (ART. 25-QUINQUESDECIES, D.LGS. N. 231/2001)**
- *Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000)*
 - *Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000)*
 - *Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000)*
 - *Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000)*
 - *Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000)*
 - *Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000) [introdotto dal D.Lgs. n. 75/2020]*
 - *Omessa dichiarazione (art. 5 D.Lgs. n. 74/2000) [introdotto dal D.Lgs. n. 75/2020]*
 - *Indebita compensazione (art. 10-quater D.Lgs. n. 74/2000) [introdotto dal D.Lgs. n. 75/2020]*
- v) CONTRABBANDO (ART. 25-SEXIESDECIES, D.LGS. N. 231/2001)**