

Allegato 2 alla Delibera del CdA n. 1 del 25 gennaio 2018

**PIANO TRIENNALE DI PREVENZIONE DELLA CORRUZIONE E TRASPARENZA AI SENSI DELLA
L. 190/12**

INDICE

2. Ambito normativo di riferimento per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione	6
3. Soggetti interni coinvolti nel processo di predisposizione e adozione del PTPC	7
3.1 Organi di indirizzo	7
3.2 Il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT)	7
3.3 I Referenti per la prevenzione	9
4. Trasparenza.....	10
6. Analisi di contesto	12
7. Casi giudiziari, episodi di corruzione	12
8. Formazione	12
8. Gestione del rischio	12
8.1 Mappatura dei processi e valutazione del rischio.....	12
8.2 Trattamento del rischio.....	14
9. MISURE DI PREVENZIONE E CONTROLLO.....	14
9.1 Attribuzione degli incarichi e nomina Commissioni – verifica dei precedenti penali.....	14
9.2 Rotazione del personale.....	14
9.3 Tutela del segnalante (c.d. whistleblower)	14
1.1 Programmazione.....	16
1.2 Progettazione della gara	16
1.3 Selezione del contraente	17
1.4 Verifica dell'aggiudicazione e stipula del contratto	17
1.5 Esecuzione del contratto	17
1.6 Rendicontazione del contratto	18
2. ACQUISIZIONE E GESTIONE DEL PERSONALE	18
3. NOMINA DEGLI ORGANI DI INDIRIZZO POLITICO E CONFERIMENTO DI INCARICHI DIRIGENZIALI	18

5. AUTORIZZAZIONI E CONCESSIONI	20
Sezione "B": art. 25 ter D. Lgs. 231/01	22
Reati societari	22
1. Reati e modalità di commissione	22
2. Aree sensibili e processi a rischio	25
3. Presidi interni	25
3.1 Presidio degli amministratori	25
3.2 Presidio del collegio dei revisori	25
3.3 Doveri e responsabilità delle direzioni e funzioni interne	26
3.4 Ulteriori presidi	27
Sezione "C": art. 25 septies D. Lgs. 231/01	29
Reati in violazione delle norme sulla tutela della salute e della sicurezza sul lavoro	29
1. Reati	29
2. Ruoli e responsabilità in materia di sicurezza	29
2.1 Datore di lavoro	29
2.2 Datore di lavoro e dirigenti	30
2.3 Preposto	31
2.4 RSPP e addetti al Servizio di Prevenzione e Protezione	31
2.5 Lavoratori incaricati della gestione delle emergenze	32
2.6 RLS	32
2.7 Medico competente	32
2.8 Lavoratori	32
3. Misure adottate nei luoghi di lavoro	33
4. Archivio della documentazione rilevante	34
5. Flussi informativi tra OdV e soggetti del SPP	34
Sezione "D": art. 24 bis D. Lgs. 231/01	36
Delitti di criminalità informatica e trattamento illecito dei dati	36
1. Reati e modalità di commissione	36
2. Aree sensibili	39
3. Protocolli di prevenzione	39
4. Flussi informativi verso l'OdV	43
Sezione "E": art. 25 undecies D. Lgs. 231/01	44
Reati ambientali	44
1. Reati inerenti alla gestione dei rifiuti	44

2. Ruoli e responsabilità a presidio	45
3. Aree sensibili e protocolli di prevenzione	45
Sezione “F”: art. 25 decies	46
Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria	46
1. Reati	46
2. Aree a rischio.....	46
3. Principi di comportamento.....	46
Sezione “H”: art. 25 octies D. Lgs. 231/01	51
Reati di ricettazione, riciclaggio e impiego di denaro, beni e utilità di provenienza illecita	51
SISTEMA DISCIPLINARE	52

PIANO TRIENNALE DI PREVENZIONE DELLA CORRUZIONE - PARTE GENERALE

Come indicato nel Piano Nazionale Anticorruzione per la prevenzione del fenomeno corruttivo non si deve solo far riferimento alla definizione di corruzione ai sensi del codice penale¹, bensì al concetto di *maladministration*, intesa quale assunzione di decisioni devianti dall'interesse generale a causa del condizionamento improprio da parte di interessi particolari.

Essa riguarda atti e comportamenti che, sebbene non costituiscano specifici reati, contrastano con la cura dell'interesse pubblico e pregiudicano l'affidamento dei cittadini nella imparzialità delle Pubbliche Amministrazioni e dei soggetti che svolgono attività di pubblico interesse.

Il presente Piano Triennale di Prevenzione della Corruzione e Trasparenza (PTPCT) per gli esercizi 2018/20 è stato predisposto all'esito delle seguenti Delibere ANAC e decreti:

1. Delibera n. 1134 recante «*Nuove linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici*»
2. Delibera n. 831 del 3 Agosto 2016 *Aggiornamento del Piano Nazionale Anticorruzione 2016*, pubblicata sulla GU n. 197 del 24 agosto 2016. il D. Lgs. 25 maggio 2016 n. 97 *Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della Legge 190/12 e del D. Lgs. 33/13, ai sensi della legge 124/2015 in materia di riorganizzazione delle amministrazioni pubbliche*
3. Determinazione ANAC n. 8 *Linee guida per l'attuazione della normativa in materia di prevenzione degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici* del 17 giugno 2015
4. Linee Guida ANAC per *l'attuazione dell'accesso civico generalizzato* (c.d. FOIA, ex D. Lgs. 33/2013 art. 5, come modificato dal D. Lgs. 97/2016) approvate il 28 dicembre 2016.
5. D. Lgs. 33/13 Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni
6. D. Lgs. 39/13 Disposizioni in materia di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti di diritto privato in controllo pubblico.

La Legge 190/12 prevede che l'organo di indirizzo politico su proposta del Responsabile PCT, entro il 31 gennaio di ogni anno, adotti il Piano Triennale di prevenzione della corruzione e trasparenza, curandone la pubblicazione.

Il Piano deve rispondere alle seguenti esigenze:

- a) individuare le attività nel cui ambito è più elevato il rischio di corruzione, anche raccogliendo le proposte dei dirigenti, elaborate nell'esercizio delle competenze previste dall'art. 16 comma 1 lett. a bis) del D. Lgs. 30 marzo 2001 n. 165
- b) prevedere, per le attività individuate ai sensi della lettera a), meccanismi di formazione, attuazione e controllo delle decisioni idonei a prevenire il rischio di corruzione
- c) prevedere, con particolare riguardo alle attività individuate ai sensi della lettera a), obblighi di informazione nei confronti del RPCT
- d) monitorare il rispetto dei termini, previsti dalla legge o dai regolamenti, per la conclusione dei procedimenti
- e) monitorare i rapporti tra l'amministrazione e i soggetti che con la stessa stipulano contratto o che sono interessati a procedimenti di autorizzazione, concessione o erogazione di vantaggi economici di qualunque genere, anche verificando eventuali relazioni di parentela o affinità sussistenti tra titolari, amministratori, soci, dipendenti degli stessi soggetti e dipendenti dell'amministrazione
- f) individuare specifici obblighi di trasparenza ulteriori rispetto a quelli previsti dalle disposizioni di legge.

¹ Cfr. Sezione A del Modello – Reati contro la Pubblica Amministrazione

2. Ambito normativo di riferimento per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione

Per superare alcune incertezze interpretative dopo le modifiche intervenute nella normativa sull'ambito soggettivo di applicazione delle disposizioni, l'Autorità con la Determinazione n. 8 del 17 giugno 2015 "*Linee guida per l'attuazione della normativa in materia di prevenzione degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici*" ha integrato le disposizioni nei confronti degli enti pubblici economici, degli enti di diritto privato in controllo pubblico (assimilabili come chiarito dall'ANAC alle Fondazioni) e delle società a partecipazione pubblica.

La Legge 190/2012 all'art. 1 co. 60 prevede tra i destinatari della normativa anticorruzione e sulla trasparenza i soggetti di diritto privato partecipati da pubbliche amministrazioni o in controllo pubblico e gli enti pubblici economici.

Ai sensi dell'art. 1 co. 2 lettera c) del D. Lgs. 39/13 per *enti di diritto privato in controllo pubblico* si intendono "le società e gli altri enti di diritto privato che esercitano funzioni amministrative, attività di produzione di beni e servizi a favore delle amministrazioni pubbliche o di gestione di servizi pubblici, sottoposti a controllo ai sensi dell'art. 2359 c.c. da parte di amministrazioni pubbliche, oppure gli enti nei quali siano riconosciuti alle pubbliche amministrazioni, anche in assenza di partecipazione azionaria, poteri di nomina dei vertici o dei componenti degli organi".

Nel PNA in merito alle modalità di applicazione della normativa anticorruzione ai soggetti in controllo pubblico e agli enti di diritto privato in controllo pubblico (assimilabili come detto alle Fondazioni) si fa riferimento alle disposizioni di cui al d. lgs. 231/01. Com'è noto gli ambiti di applicazione della Legge 190/2012 e del D. Lgs. 231/01 non coincidono:

a) il d. lgs. 231/01 contempla reati che sono commessi *nell'interesse o vantaggio della società*; diversamente la Legge 190 è volta a prevenire anche i reati commessi *a danno della società*.

b) il d. lgs. 231/01 in relazione al reato di corruzione contempla anche quelli di concussione, induzione indebita a dare o promettere utilità, corruzione tra privati; la Legge 190 fa riferimento a un concetto più ampio di corruzione, considerando anche le situazioni di "cattiva amministrazione" che comprendono i casi di deviazione significativa dei comportamenti e delle decisioni dalla cura dell'interesse pubblico.

Alla luce di quanto sopra e secondo le indicazioni contenute nel PNA le società sono tenute a integrare i contenuti del Modello organizzativo 231/01 con le misure idonee a prevenire anche i fenomeni di corruzione e di illegalità in coerenza con le finalità della Legge 190. Tali misure devono essere ricondotte in un unico documento che tenga conto del Piano di prevenzione della corruzione adottato dalle società.

Le misure volte alla prevenzione della corruzione ex Legge 190 sono elaborate dal RPC in stretto coordinamento con l'OdV e sono adottate dal Consiglio di Amministrazione.

Di seguito sono richiamati i contenuti minimi delle misure di prevenzione da adottare: **a) Individuazione e gestione dei rischi di corruzione:** in coerenza con quanto previsto dall'art. 1 co. 9 della Legge 190 e dall'art. 6 co. 2 del d. lgs. 231/01 le società effettuano un'analisi di contesto e una mappatura per individuare i processi a rischio. Tra le attività esposte al rischio di corruzione vanno annoverate quelle previste dalla Legge 190 (autorizzazioni e concessioni, appalti e contratti, sovvenzioni e finanziamenti, selezione e gestione del personale), cui si aggiungono ulteriori aree individuate in base alle proprie caratteristiche organizzative **b) Sistema dei controlli:** la definizione del sistema di gestione del rischio prevista dalla Legge 190 si completa con la valutazione del sistema di controllo interno previsto dal decreto 231. Il coordinamento tra i controlli deve essere assicurato anche tramite le funzioni del RPC e dell'OdV **c) Codice di comportamento:** le società integrano il proprio codice di comportamento (codice etico) approvato ai sensi del D. Lgs. 231 con i comportamenti da osservarsi ai fini della prevenzione della corruzione **d) Trasparenza e) Inconferibilità e incompatibilità degli incarichi:** le società adottano misure necessarie a inserire nelle lettere di attribuzione degli incarichi tutte le clausole di inconferibilità e incompatibilità contenute nei D. Lgs. 33/2013 e 39/2013 **f) Attività successiva alla cessazione del rapporto di lavoro dei dipendenti pubblici:** le società adottano misure per evitare l'assunzione di dipendenti pubblici che negli ultimi tre anni abbiano esercitati poteri autorizzativi o negoziali nelle PA. **g) Formazione:** i moduli formativi sulla corruzione vanno integrati con quelli sul decreto 231/01 e sul relativo Modello **h) Tutela del dipendente che segnala illeciti:** come previsto dalle Linee Guida emanate dall'ANAC con la

Determinazione n. 6 del 28 aprile 2015 le società adottano misure per incoraggiare il dipendente che segnala illeciti garantendo la riservatezza della sua identità **i) Rotazione e misure alternative:** le società adottano sistemi di turnover dei dipendenti preposti alla gestione dei processi più esposti a rischio di corruzione **l) Monitoraggio:** le società adottano sistemi di monitoraggio sull'attuazione delle misure di prevenzione della corruzione e sul loro aggiornamento, specificando i ruoli e le responsabilità dei soggetti chiamati a svolgere tali attività.

3. Soggetti interni coinvolti nel processo di predisposizione e adozione del PTPC

3.1 Organi di indirizzo

Tra gli obiettivi strategici fissati dall'Organo di indirizzo per il triennio in materia di prevenzione della corruzione e di trasparenza rilevano:

- 1) la promozione di maggiori livelli di trasparenza attraverso la pubblicazione dei dati richiesti dalla legge. In merito il RPCT promuove la richiesta ai singoli uffici dei dati e delle informazioni da pubblicare nella sezione Amministrazione Trasparente
- 2) l'adozione di misure organizzative interne che favoriscano lo scambio di informazioni tra il RPCT e il personale aziendale. In particolare deve essere assicurato un costante flusso informativo da e verso il RPCT attraverso un sistema di reportistica sistematico e strutturato in merito a eventi a rischio, la cui rilevazione costituisca il punto dal quale possono originarsi azioni di riscontro e approfondimento degli organi di vertice su eventuali situazioni anomale a rischio di reato.
- 3) il coinvolgimento degli stakeholder attraverso comunicati mirati in una logica di sensibilizzazione dei cittadini alla cultura della legalità.
- 4) la creazione di una struttura organizzativa di supporto al RPCT.

Il CdA riceve la relazione annuale del RPCT e può chiamare quest'ultimo a riferire sull'attività e riceve dallo stesso segnalazioni su eventuali disfunzioni riscontrate inerenti all'attuazione delle misure di prevenzione e di trasparenza.

3.2 Il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT)

L'organo d'indirizzo politico (a cui la Legge 190/12 all'art. 1 comma 7 aveva demandato la nomina del Responsabile della prevenzione della corruzione) nomina il RPCT. L'atto di nomina del RPCT è accompagnato da un comunicato con cui si invitano tutti i dirigenti e il personale a dare allo stesso la necessaria collaborazione.

Al riguardo si ricorda che l'art. 8 del DPR 62/2013 prevede un dovere di collaborazione dei dipendenti nei confronti del RPCT, dovere la cui violazione è sanzionabile disciplinarmente.

Come specificato anche nella Determinazione n. 8 *"Linee guida per l'attuazione della normativa in materia di prevenzione degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici"* il RPCT deve essere scelto preferibilmente tra i dirigenti in servizio che non operano nelle aree particolarmente esposte al rischio di corruzione. Solo nelle ipotesi in cui la società sia priva di dirigenti, il RPCT può essere scelto senza un profilo dirigenziale purché garantisca idonee competenze. In questo caso il Consiglio di Amministrazione è tenuto a esercitare su questi un'attività di vigilanza periodica.

Nelle società di piccole dimensioni dove l'OdV è monocratico, è possibile nominare il RPCT quale OdV. In merito alle responsabilità del RPCT, restano invariate quelle dirigenziali e quelle dei dipendenti proprie di ciascuna tipologia di società. Si aggiungono a queste quelle derivanti dall'omessa vigilanza sul funzionamento e sull'osservanza delle misure poste a prevenzione della corruzione, da indicarsi nella lettera di conferimento dell'incarico.

Al RPCT compete:

- a) elaborare la proposta di Piano della prevenzione, che deve essere adottato dall'organo di indirizzo politico
- b) definire canali di comunicazione adeguati per la segnalazione di comportamenti sospetti e/o non in linea con quanto definito dal PTPC e dal Codice Etico

- c) definire d'intesa con i responsabili competenti procedure appropriate per selezionare e formare i dipendenti destinati a operare in settori particolarmente esposti alla corruzione
- d) verificare e monitorare, in raccordo con i Referenti, l'efficace attuazione del Piano e la sua idoneità, nonché proporre i necessari adeguamenti, in caso di violazioni delle relative prescrizioni o di mutamenti dell'organizzazione
- e) monitorare il recepimento e il rispetto da parte dei Referenti dei protocolli e delle misure previste dal PTPC nell'ambito delle aree di competenza
- f) gestire le segnalazioni pervenute mediante i canali istituzionali attivati
- g) proporre modifiche al Piano in caso di accertamento di significative violazioni o di mutamenti dell'organizzazione o dell'attività dell'amministrazione
- h) verificare, d'intesa con i responsabili competenti, l'effettiva rotazione degli incarichi negli uffici preposti allo svolgimento delle attività nel cui ambito è più elevato il rischio che siano commessi reati di corruzione
- i) individuare d'intesa con i responsabili competenti il personale da inserire nei percorsi di formazione sui temi dell'etica e della legalità
- j) vigilare sull'osservanza del Piano.

In merito all'incarico e alle attività del RPCT le novità introdotte dalla Determinazione n. 831 attengono:

- 1) alla durata dell'incarico del RPCT che deve essere correlata a quella del contratto sottostante all'incarico dirigenziale già svolto, al fine di garantire la sua autonomia e indipendenza
- 2) all'estensione generalizzata dei doveri di segnalazione all'Autorità di eventuali misure discriminatorie, quindi non più solo in caso di revoca, dirette o indirette, nei suoi confronti collegate all'esercizio delle sue funzioni.
- 3) all'esclusione dall'imputazione di responsabilità (per omesso controllo, sul piano disciplinare) nei casi di ripetute violazioni delle misure di prevenzione previste dal Piano, qualora possa provare di aver comunicato agli uffici le misure da adottare e le modalità attuative e di aver vigilato sull'osservanza del medesimo Piano (art. 41, co. 1 lett. l, d. lgs. 97/2016). I dirigenti pertanto rispondono della mancata attuazione delle misure di prevenzione della corruzione ove il RPCT dimostri di aver effettuato le dovute comunicazioni agli uffici e di aver vigilato sull'osservanza del Piano.

Il RPCT deve avere poteri di interlocuzione e controllo nei confronti della struttura organizzativa.

Il RPCT ha il potere di indicare agli uffici competenti all'esercizio dell'azione disciplinare i nominativi dei dipendenti che non hanno attuato correttamente le misure in materia di prevenzione della corruzione e di trasparenza. Dall'altro lato, il RPCT ha il dovere di segnalare all'organo di indirizzo le disfunzioni inerenti all'attuazione delle misure in materia di prevenzione della corruzione e di trasparenza.

In tema di trasparenza al Responsabile della prevenzione della corruzione e della trasparenza (RPCT) compete in particolare:

- svolgere stabilmente un'attività di controllo sull'adempimento da parte della Società degli obblighi di pubblicazione normativamente previsti, garantendo la completezza, la chiarezza e l'aggiornamento delle informazioni pubblicate, nonché segnalando agli organi di indirizzo politico, all'Organismo di vigilanza, all'Autorità nazionale anticorruzione i casi di mancato o ritardato adempimento degli obblighi di pubblicazione;
- controllare e assicurare la regolare attuazione dell'accesso civico.

Il RPCT individua in uno o più responsabili di servizi i Referenti per i controlli interni e per la trasparenza, ai quali compete:

- l'adempimento degli obblighi di pubblicazione degli atti normativamente previsti, garantendo il tempestivo e regolare flusso delle informazioni da pubblicare ai fini del rispetto dei termini stabiliti dalla legge;
- garantire l'integrità, il costante aggiornamento, la completezza, la tempestività, la semplicità di consultazione, la comprensibilità, l'omogeneità, la facile accessibilità delle informazioni pubblicate.

Il RPCT è tenuto a predisporre una Relazione recante i risultati dell'attività svolta nell'anno precedente.

Come indicato dall'ANAC la Relazione è pubblicata sul sito istituzionale nella sezione "Amministrazione Trasparente".

Nei casi in cui l'organo di indirizzo politico lo richieda, il RPCT è tenuto a riferire personalmente sull'attività svolta. Nel caso in cui, nello svolgimento della sua attività, egli riscontri dei fatti che possano rappresentare una rilevanza disciplinare deve darne tempestiva comunicazione al dirigente preposto all'ufficio a cui il dipendente è addetto, o al dirigente gerarchicamente superiore, se trattasi di dirigente, e al servizio risorse umane affinché possa essere applicata l'azione disciplinare.

Ove il RPCT ravvisi fatti suscettibili di dar luogo a danno erariale, deve presentare tempestiva denuncia alla competente Corte di Conti.

Qualora riscontri fatti che rappresentano notizie di reato, deve presentare denuncia alla Procura della Repubblica o a un ufficiale di polizia giudiziaria con le modalità previste dalla legge (art. 311 c.p.p) e deve darne tempestiva comunicazione all'ANAC.

Per l'adempimento dei compiti sopra elencati e di tutti quelli previsti dalla L. n. 190/2012 il RPCT può in ogni momento:

- a) verificare e chiedere delucidazioni per iscritto e verbalmente a tutti i dipendenti su comportamenti che possano integrare, anche solo potenzialmente, corruzione e illegalità;
- b) richiedere ai dipendenti che hanno istruito un procedimento di fornire motivazioni per iscritto circa le circostanze di fatto e di diritto che sottendono all'adozione del provvedimento finale;
- c) effettuare verifiche e ispezioni a campione, al fine di procedere al controllo del rispetto delle condizioni di correttezza e legittimità dei procedimenti in corso o già conclusi.

In caso di inadempimento da parte del RPC ai compiti attribuitigli lo stesso incorre in:

- responsabilità dirigenziale per la mancata predisposizione del Piano (art. 1 comma 8 Legge 190/12)
- responsabilità dirigenziale in caso di mancata adozione delle misure per la selezione e formazione dei dipendenti destinati a operare nei settori maggiormente esposti alla corruzione (art. 1 comma 8).

Il RPC inoltre, in caso di commissione all'interno dell'amministrazione, di un reato di corruzione accertato con sentenza passata in giudicato, risponde ai sensi dell'art. 21 del D. Lgs. 30 marzo 2001 n. 165² e successive modificazioni, nonché sul piano disciplinare, oltre che per il danno erariale e all'immagine della PA salvo che provi:

- a) di aver predisposto prima della commissione del fatto il Piano e di aver osservato le prescrizioni di cui ai commi 9 (contenuto minimo del Piano) e 10 (compiti del RPC) della Legge;
- b) di aver vigilato sul funzionamento e sull'osservanza del Piano.

La sanzione disciplinare del RPC non può essere inferiore alla sospensione dal servizio con privazione della retribuzione da un minimo di un mese a un massimo di sei mesi.

3.3 I Referenti per la prevenzione

I Referenti per la Prevenzione sono i responsabili di Area cui competono i seguenti compiti:

² Art. 21. Responsabilità dirigenziale.

1. Il mancato raggiungimento degli obiettivi accertato attraverso le risultanze del sistema di valutazione di cui al Titolo II del decreto legislativo di attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni ovvero l'inosservanza delle direttive imputabili al dirigente comportano, previa contestazione e ferma restando l'eventuale responsabilità disciplinare secondo la disciplina contenuta nel contratto collettivo, l'impossibilità di rinnovo dello stesso incarico dirigenziale. In relazione alla gravità dei casi, l'amministrazione può inoltre, previa contestazione e nel rispetto del principio del contraddittorio, revocare l'incarico collocando il dirigente a disposizione dei ruoli di cui all'articolo 23 ovvero recedere dal rapporto di lavoro secondo le disposizioni del contratto collettivo.

1-bis. Al di fuori dei casi di cui al comma 1, al dirigente nei confronti del quale sia stata accertata, previa contestazione e nel rispetto del principio del contraddittorio secondo le procedure previste dalla legge e dai contratti collettivi nazionali, la colpevole violazione del dovere di vigilanza sul rispetto, da parte del personale assegnato ai propri uffici, degli standard quantitativi e qualitativi fissati dall'amministrazione, conformemente agli indirizzi deliberati dalla Commissione di cui all'articolo 13 del decreto legislativo di attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni, la retribuzione di risultato è decurtata, sentito il Comitato dei garanti, in relazione alla gravità della violazione di una quota fino all'ottanta per cento.

- coadiuvare il RPCT nel monitoraggio del rispetto delle previsioni del PTPC da parte delle strutture facenti capo al loro processo/strutture di riferimento;
- informare tempestivamente il RPCT, mediante i canali di comunicazione definiti, di eventuali anomalie riscontrate nel corso del loro monitoraggio, proponendo anche le soluzioni da adottare ai fini del corretto presidio dei rischi, monitorandone l'effettiva attuazione;
- facilitare i flussi informativi da/verso le strutture coinvolte nei processi di propria responsabilità;
- segnalare tempestivamente il manifestarsi di nuovi rischi riscontrati nell'ambito delle attività sovrintese;
- segnalare al RPCT ogni esigenza di aggiornamento/modifica dei presidi di controllo in essere, per esempio in caso di cambiamenti organizzativi;
- operare in coordinamento con il RPCT per esigenze formative e di sensibilizzazione interna alle strutture di riferimento.

4. Trasparenza

Per trasparenza si intende "l'accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche".

In attuazione della Legge n. 190/2012 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione", il 10 marzo 2013 è entrato in vigore il D. Lgs. n. 33/2013 recante "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni", il cui art. 11 ha delineato l'ambito soggettivo di applicazione, individuando quali principali destinatarie le amministrazioni di cui all'art. 1, comma 2, del D. Lgs. n. 165/2001.

All'attuale quadro normativo in materia di trasparenza il d. lgs. 97/2016 ha apportato rilevanti innovazioni.

Con la Determinazione 831, si è avuta inoltre la soppressione del riferimento al Piano Triennale per la Trasparenza e l'integrità dei dati. Le modalità di attuazione della trasparenza costituiscono ora un'apposita sezione del PTPC.

4.1 Responsabili della trasmissione e della pubblicazione dei dati, dei documenti e delle informazioni

Al fine di supportare il RPCT nell'espletamento delle rispettive attività, le funzioni relative agli adempimenti operativi in materia di trasparenza amministrativa sono assegnate alla Direzione Amministrativa, a cui compete anche la pubblicazione sul sito web aziendale delle informazioni, dei dati e dei documenti su cui vige l'obbligo di pubblicazione.

I responsabili della trasmissione dei dati, dei documenti e delle informazioni sono i Responsabili degli uffici che detengono i dati, oggetto di pubblicazione.

4.2 Caratteristica delle informazioni

I Referenti devono curare la qualità della pubblicazione affinché si possa accedere in modo agevole alle informazioni e se ne possano comprendere i contenuti.

In particolare, i dati ed i documenti dovranno essere pubblicati:

- in forma chiara e semplice, per essere facilmente comprensibili al soggetto che ne prende visione;
- completi nel loro contenuto;
- aggiornati tempestivamente, in tempi tali da garantire l'utile fruizione per l'utente;
- in formato di tipo aperto e raggiungibili direttamente dalla pagina dove le informazioni sono riportate.

Nella pubblicazione di dati e documenti e di tutto il materiale soggetto agli obblighi di trasparenza deve essere garantito il rispetto delle normative sulla privacy.

4.3 Controllo e monitoraggio

Il RPCT svolge il controllo sull'attuazione delle misure per l'attuazione della trasparenza riferendo al Consiglio di Amministrazione eventuali inadempimenti e ritardi.

A tale fine il RPCT informa i Referenti circa le eventuali carenze o mancanze rilevate, che dovranno essere sanate a cura dei predetti entro 30 giorni dalla segnalazione. In caso di inadempimento, il RPCT ne darà comunicazione al Consiglio di Amministrazione.

Il RPCT attesta l'assolvimento degli obblighi relativi alla trasparenza ed all'integrità tramite report periodici al Consiglio di Amministrazione.

Eventuali ritardi negli aggiornamenti previsti, che possano comportare sanzioni, potranno costituire oggetto di provvedimento disciplinare.

4.4 Accesso civico

Chiunque ha il diritto di richiedere documenti, informazioni o dati su cui vige l'obbligo di pubblicazione.

La richiesta di accesso civico è gratuita, non deve essere motivata, non è sottoposta ad alcuna limitazione rispetto alla legittimazione soggettiva del richiedente e va presentata al Responsabile per l'accesso civico generalizzato tramite posta elettronica all'indirizzo pubblicato sul sito aziendale.

A seguito di richiesta di accesso civico, l'ufficio allo scopo incaricato provvede, entro 30 giorni lavorativi, a:

- pubblicare nel sito web istituzionale il documento, l'informazione o il dato richiesto;
- comunicare contemporaneamente al richiedente ed al Responsabile per la trasparenza l'avvenuta pubblicazione, indicando il relativo collegamento ipertestuale;
- indicare al richiedente il collegamento ipertestuale dove reperire il documento, l'informazione o il dato, qualora già pubblicati.

4.5 Accesso civico generalizzato

La nuova tipologia di accesso, delineata nell'art. 5 co. 2 e ss. Del d. lgs. 33/2013 come modificato dal d. lgs. 97/2016, si aggiunge all'accesso civico già disciplinato dal medesimo decreto e all'accesso agli atti ex l. 241/1990 ed è volto a favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico. Ciò in attuazione del principio di trasparenza che il novellato art. 1 co. 1 del decreto definisce anche, con una modifica assai significativa, come strumento di tutela dei diritti dei cittadini e di promozione della partecipazione degli interessati all'attività amministrativa.

Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle PA, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del decreto 33/13, nel rispetto dei limiti fissati dal Decreto.

L'esercizio del diritto non ha limitazione alcuna quanto alla legittimazione soggettiva del richiedente. L'istanza può essere trasmessa:

- a) all'Ufficio che detiene i dati, le informazioni o i documenti
- b) all'Ufficio relazioni con il pubblico
- c) a un altro ufficio indicato dall'amministrazione nella sezione Amministrazione Trasparente del sito istituzionale.

Il procedimento di accesso civico deve concludersi con provvedimento espresso e motivato nel termine di 30 gg dalla presentazione dell'istanza con la comunicazione al richiedente e agli eventuali controinteressati.

Il RPCT, oltre alla facoltà di richiedere agli uffici della relativa amministrazione informazioni sull'esito delle istanze, deve occuparsi, per espressa disposizione normativa (art. 5 co. 7, d. lgs. 33/2013 come modificato dal d. lgs. 97/2016) dei casi di riesame (sia che l'accesso riguardi dati a pubblicazione obbligatoria o meno).

Al Responsabile dell'accesso civico e generalizzato compete decidere sulle richieste di accesso con le modalità disciplinate dalla normativa ed espletare tutti gli atti inerenti.

Titolare del potere sostitutivo è il RPCT, al quale il richiedente potrà ricorrere nel caso di ritardata o mancata risposta o diniego.

6. Analisi di contesto

L'analisi del contesto riguarda gli aspetti legati all'organizzazione interna, ai ruoli e responsabilità, alla cultura organizzativa ecc. che, come indicato dall'ANAC, possono influenzare la sensibilità della struttura al rischio di corruzione.

L'assetto organizzativo costituisce l'impianto generale di deleghe, attività e controlli sul quale si innestano le regole del PTPC, del Modello di prevenzione e controllo 231/01, del Codice Etico, l'azione del RPCT e dell'Organismo di vigilanza.

In merito al sistema di deleghe e poteri della Fondazione, si rimanda a quanto illustrato nel Capitolo sulla Governance.

Ai sensi dell'art. 2381 c.c. 5° comma, compete agli organi delegati curare l'assetto organizzativo/contabile in relazione alla natura e dimensione dell'impresa.

Il Direttore generale adempie il suo dovere/potere di curare l'adeguatezza organizzativa, attraverso la definizione e il controllo della struttura operativa, delle missioni, dei ruoli e delle responsabilità attribuite mediante un sistema di sub deleghe e procure interne o esterne tali da garantire l'efficacia aziendale, nel rispetto della normativa di riferimento.

In tale contesto adotta politiche delle risorse umane centrate sulla valorizzazione, meritocrazia e responsabilizzazione di dirigenti, quadri e personale dipendente in un ambiente operativo basato sull'assunzione ponderata dei rischi d'impresa e sull'attenzione del management alla trasparenza informativa, alla conformità a norme e regolamenti, alla rendicontazione e al controllo interno.

7. Casi giudiziari, episodi di corruzione

Non si sono verificati episodi di corruzione e non sono in corso procedimenti giudiziari.

8. Formazione

La formazione è volta a diffondere la cultura della legalità e dei principi di comportamento, la conoscenza delle politiche e dei programmi mirati a prevenire la corruzione.

La programmazione degli interventi formativi sarà svolta dal RPCT secondo due livelli, uno generale rivolto a tutti i dipendenti, uno specifico rivolto a: dirigenti e funzionari operanti nelle aree di rischio, eventuali referenti individuati per la prevenzione.

Le iniziative previste nel livello generale rivolte a tutti i dipendenti avranno la finalità in particolare di diffondere le tematiche dell'etica e della legalità, quelle previste a livello specifico potranno riguardare le politiche, i programmi e i vari strumenti utilizzati per la prevenzione della corruzione in relazione al ruolo svolto da ciascun dipendente. Le attività formative saranno svolte attraverso lezioni in aula e distribuzione del materiale informativo.

8. Gestione del rischio

8.1 Mappatura dei processi e valutazione del rischio

Il processo di definizione delle aree sensibili del PTPC, è stato condotto incentrando l'analisi degli eventi a rischio sulle aree obbligatorie individuate dalla Legge n. 190/2012, nonché su ulteriori aree risultate potenzialmente esposte al rischio di corruzione ad esito dell'attività di *risk assessment* condotta nell'ambito delle attività relative anche al D. Lgs. 231/2001. Tale ricognizione è stata svolta proprio nell'ottica di rendere l'analisi delle aree sensibili del PTPC il più possibile aderente alla realtà aziendale e alle peculiarità del business della Società e di strutturare un processo di prevenzione via via più focalizzato sugli aspetti più significativi.

Sulla base di tali evidenze il PTPC potrà progressivamente, nell'ambito dell'attuazione delle misure programmatiche già previste e da prevedere, focalizzare in maniera mirata e puntuale gli interventi sulle aree via via più esposte al rischio e quindi rafforzare ulteriormente il processo di minimizzazione dei rischi di corruzione.

Sulla scorta di tali risultanze e delle esperienze operative maturate con l'esercizio del Piano, i presidi e le misure di rafforzamento della prevenzione potranno progressivamente arricchirsi di ulteriori elementi di controllo sulle aree a rischio individuate dal PTPC e di iniziative di adeguamento delle procedure esistenti, con l'obiettivo di contribuire a una gestione sempre più virtuosa delle attività.

Le aree a rischio sono state ulteriormente analizzate in base alla probabilità concreta del verificarsi dell'evento corruttivo e in considerazione dell'impatto economico, organizzativo e reputazionale dell'eventuale fatto (c.d. rischio "in concreto").

Tale valutazione e attribuzione del punteggio numerico è avvenuta mediante utilizzo della Tabella "Valutazione del rischio" di cui all'allegato 5 al PNA, come modificata dal Dipartimento della Funzione Pubblica, secondo quanto disposto dal PNA stesso. Il rischio per ciascuna area è stato valutato *basso, medio o alto* in relazione alla valutazione della probabilità che esso si realizzi e delle conseguenze che il rischio produce.

IMPATTO PROBABILITA'	BASSA	MEDIA	ALTA
ALTO	Rischio medio	Rischio alto	Rischio alto
MEDIO	Rischio basso	Rischio medio	Rischio alto
BASSO	Rischio basso	Rischio basso	Rischio medio

La mappatura dei processi è stata effettuata per le cd. aree di rischio obbligatorie individuate dalla Legge 190/12 e dall'Allegato 2 del PNA e per altre attività di rischio specifiche dell'attività svolta dalla Fondazione.

AREA DI RISCHIO	PROCESSI E ATTIVITA'	LIVELLO DI RISCHIO
Affidamento di lavori, servizi e forniture	<ul style="list-style-type: none"> - Definizione dell'oggetto dell'affidamento - Individuazione modalità di scelta del contraente - Individuazione dei requisiti di qualificazione - Valutazione delle offerte - Verifica dell'eventuale anomalia delle offerte - Individuazione dei requisiti di aggiudicazione - Predisposizione degli atti di gara (bando, disciplinare, capitolato, contratto) - Nomina del Responsabile del procedimento - Revoca del bando - Gestione ed esecuzione del contratto - Rendicontazione del contratto - Gestione varianti e riserve in corso d'opera - Collaudi - Gestione delle controversie - Comunicazioni e rapporti con l'Autorità 	Alto
Acquisizione, progressione e gestione del personale	<ul style="list-style-type: none"> - Reclutamento mediante selezioni a evidenza pubblica - Assunzioni obbligatorie per categorie protette - Progressioni di carriera 	Basso
Conferimenti di incarichi dirigenziali		Basso
Autorizzazioni, concessioni	<ul style="list-style-type: none"> - Richiesta di autorizzazioni o concessioni - Gestione di autorizzazioni o concessioni 	Medio

8.2 Trattamento del rischio

La fase di trattamento del rischio ha previsto l'individuazione e la valutazione delle misure predisposte per ridurre il rischio di corruzione e la definizione delle priorità d'intervento.

9. MISURE DI PREVENZIONE E CONTROLLO

Le misure generali di prevenzione e controllo sono quelle che attengono a:

- attribuzione degli incarichi e nomina Commissioni - verifica dei precedenti penali;
- rotazione del personale;
- tutela del segnalante (c.d. *whistleblower*).

9.1 Attribuzione degli incarichi e nomina Commissioni – verifica dei precedenti penali

La condanna, anche non definitiva, per i reati contro la Pubblica Amministrazione impedisce:

- a) la partecipazione, anche con compiti di segreteria, di commissioni per l'accesso o la selezione a pubblici impieghi;
- b) l'assegnazione, anche con funzioni direttive, agli uffici preposti alla gestione delle risorse finanziarie, all'acquisizione di beni, servizi e forniture, nonché alla concessione o all'erogazione di sovvenzioni, contributi, sussidi, ausili finanziari o attribuzioni di vantaggi economici a soggetti pubblici e privati;
- c) la partecipazione alle commissioni per la scelta del contraente per l'affidamento di lavori, forniture e servizi, per la concessione o l'erogazione di sovvenzioni, contributi, sussidi, ausili finanziari, nonché per l'attribuzione di vantaggi economici di qualunque genere.

9.2 Rotazione del personale

La rotazione del personale ha come obiettivo l'alternanza tra più professionisti nell'assunzione delle decisioni e nella gestione delle procedure, nelle aree a più elevato rischio di corruzione, al fine di ridurre il pericolo che possano crearsi relazioni particolari tra amministrazioni ed utenti, con il conseguente consolidarsi di situazioni di privilegio e l'aspettativa a risposte illegali improntate a collusione.

Tale misura deve essere valutata in considerazione dell'altrettanto importante principio di continuità dell'azione amministrativa, che implica la valorizzazione della professionalità acquisita dai dipendenti in certi ambiti e settori di attività.

Considerata la struttura organizzativa e l'organico in forza, allo stato attuale, non si ritiene percorribile l'attuazione della suddetta misura di controllo che sarà altresì oggetto di valutazione nel futuro in caso di crescita dell'organico della Società.

All'atto di adozione del presente PTPC, in alternativa alla rotazione del personale, viene attuata la c.d. segregazione delle funzioni, cioè un'articolazione di competenze che attribuisce a soggetti diversi i compiti relativi a: a) svolgimento di istruttorie e accertamenti b) adozione di decisioni c) attuazione delle decisioni prese d) effettuazione delle verifiche.

9.3 Tutela del segnalante (c.d. *whistleblower*)

L'obiettivo di tale misura di controllo consiste nella sensibilizzazione dell'attività del segnalante, il cui ruolo assume rilevanza di interesse pubblico, dando conoscenza, se possibile tempestiva, di problemi o pericoli alla Società, incentivando e proteggendo tali segnalazioni.

Nel PNA 2016 è sottolineata la necessità che la segnalazione sia "in buona fede"; essa cioè deve essere effettuata nell'interesse dell'integrità della pubblica amministrazione, l'istituto quindi non deve essere utilizzato per esigenze individuali, ma finalizzato a promuovere l'etica e l'integrità nella Pubblica Amministrazione.

A tal fine, la segnalazione deve contenere i seguenti elementi:

- a) generalità del soggetto che effettua la segnalazione, con indicazione della posizione o funzione svolta nell'ambito della Fondazione;

- b) una chiara e completa descrizione dei fatti oggetto di segnalazione;
- c) se conosciute, le circostanze di tempo e di luogo in cui sono stati commessi;
- d) se conosciute, le generalità o altri elementi che consentano di identificare il soggetto/i che ha/hanno posto/i in essere i fatti segnalati;
- e) l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;
- f) l'indicazione di eventuali documenti che possono confermare la fondatezza di tali fatti.

La segnalazione deve essere indirizzata al RPCT con le seguenti modalità:

- a) mediante invio, all'indirizzo di posta elettronica dedicato. In tal caso, l'identità del segnalante sarà conosciuta solo dal RPCT che ne garantirà la riservatezza, fatti salvi i casi in cui non è opponibile per legge;
- b) a mezzo del servizio postale o tramite posta interna; in tal caso, per poter usufruire della garanzia della riservatezza, è necessario che la segnalazione venga inserita in una busta chiusa che rechi all'esterno la dicitura "riservata/personale";
- c) verbalmente, mediante dichiarazione rilasciata e riportata a verbale da uno dei soggetti legittimati alla loro ricezione;

Inoltre vige l'obbligo di riservatezza a carico di tutti coloro che ricevono o vengono a conoscenza della segnalazione e di coloro che successivamente venissero coinvolti nel processo di gestione della segnalazione, salve le comunicazioni di legge.

AREE DI RISCHIO

1. CONTRATTI PUBBLICI

L'area di rischio dei contratti pubblici è di seguito analizzata secondo le indicazioni dell'ANAC e suddivisa nelle fasi di: programmazione, progettazione della gara, selezione del contraente, verifica dell'aggiudicazione e stipula del contratto, esecuzione e rendicontazione del contratto.

1.1 Programmazione

Il rischio intrinseco di questa fase è che venga definito un fabbisogno non correlato ai criteri di efficienza/efficacia/economicità, ma alla volontà di favorire uno specifico operatore economico.

Possibili anomalie riconducibili a questa fase possono essere il ritardo o la mancata approvazione degli strumenti di programmazione, l'eccessivo ricorso a procedure d'urgenza o proroghe contrattuali, la reiterazione di piccoli affidamenti aventi il medesimo oggetto, la presenza di gare aggiudicate con frequenza ai medesimi soggetti.

Ai fini della prevenzione il RPC verifica che sia:

- a) effettuata una stima del valore degli appalti in base all'art. 35 del Codice *Metodi di calcolo del valore stimato dei contratti pubblici*
- b) vietato il ricorso a procedure di urgenza nonché la reiterazione di piccoli affidamenti (c.d. sotto soglia) riferiti agli stessi acquisti in un determinato arco temporale.

Tra le ulteriori possibili misure di prevenzione adottate si richiamano:

- a) programmazione annuale degli investimenti
- b) previa gara, contratti di durata per forniture periodiche e ripetitive
- c) per rilevanti importi contrattuali, tempestivo obbligo di informazione nei confronti del RPC in caso di proroga o affidamenti d'urgenza

1.2 Progettazione della gara

Alcuni dei rischi di questa fase sono riconducibili a: a) nomina del Responsabile del procedimento in rapporti di contiguità con imprese concorrenti o privi di requisiti idonei ad assicurare la terzietà e l'indipendenza b) fuga di notizie che anticipino ad alcuni concorrenti i contenuti della documentazione di gara c) elusione delle regole di affidamento degli appalti mediante l'utilizzo di particolari sistemi di affidamento (ad esempio concessione in luogo di appalto) d) predisposizione di clausole contrattuali vaghe per disincentivare la partecipazione alla gara o per consentire modifiche in fase di esecuzione e) definizione di requisiti *ad hoc* per favorire una determinata impresa f) formulazione di criteri di valutazione e attribuzione di punteggi atti ad avvantaggiare il fornitore uscente.

Tra le possibili misure di prevenzione adottate si richiamano:

- a) l'obbligo di motivazione nella determina a contrarre in merito alla scelta della procedura e del sistema di affidamento adottato nei casi di affidamento diretto o nei casi di scelta di procedure non previste dal codice degli appalti.
- b) l'adozione di misure volte a garantire la nomina di RP a persone in possesso dei necessari requisiti.

In caso di procedure negoziate:

- c) la preventiva individuazione, mediante direttive e circolari, dei presupposti legali per indire le stesse o procedere ad affidamenti diretti da parte del Responsabile del procedimento
- d) l'adozione di direttive e linee guida che disciplinino la procedura da seguire con riguardo alla pubblicità delle sedute di gara e alla pubblicazione della determina a contrarre ai sensi dell'art. 37 del D. Lgs 33/13

Come in fase di programmazione, anche in quella di progettazione, il RPC verifica che sia:

- a) evitato il ricorso a concessioni o altre fattispecie contrattuali anziché agli appalti
- b) vietata la previsione di ingiustificati requisiti restrittivi alla partecipazione

c) vietato il ricorso a procedure di urgenza nonché la reiterazione di piccoli affidamenti (c.d. sotto soglia) riferiti agli stessi acquisti in un determinato arco temporale.

Rimane salva la possibilità di proporre solo il conferimento di appositi incarichi a supporto dell'intera procedura o di parte di essa, nel caso di appalti di particolare complessità in relazione all'opera da realizzare ovvero alla specificità della fornitura o del servizio, che richiedano necessariamente valutazioni e competenze altamente specialistiche, (D. Lgs. 50/16 art. 31, VII comma). Ulteriormente il nono comma del medesimo art. 31 prevede la possibilità della stazione appaltante di istituire, allo scopo di migliorare la qualità della progettazione e della programmazione complessiva, una struttura stabile a supporto dei RUP, anche alle dirette dipendenze del vertice della pubblica amministrazione di riferimento. In conclusione si rileva la necessità che il ruolo di responsabile del procedimento sia ricoperto da un unico e qualificato soggetto, salva la possibilità da parte dello stesso avvalersi di un supporto, nei termini e alle condizioni sopra riportate.

1.3 Selezione del contraente

I possibili rischi di questa fase riguardano la manipolazione dei processi di pubblicazione del bando, fissazione dei termini per la ricezione delle offerte, trattamento e custodia della documentazione di gara, nomina della commissione di gara, gestione delle sedute di gara, verifica dei requisiti di partecipazione, valutazione e verifica delle anomalie delle offerte, aggiudicazione provvisoria, annullamento della gara, gestione di elenchi o albi di operatori economici da parte degli attori coinvolti (RP, commissione di gara, soggetti coinvolti nella verifica dei requisiti ecc.), al fine di pilotare l'aggiudicazione della gara.

Le anomalie possono essere: l'assenza di pubblicità del bando o di altra documentazione rilevante, l'alto numero di concorrenti esclusi, la presenza di reclami e ricorsi da parte di concorrenti esclusi, la presenza di gare aggiudicate con frequenza agli stessi operatori, la presenza di gare con un ristretto numero di partecipanti o con una sola offerta valida.

Il RPC, con il supporto degli altri dirigenti responsabili, monitora il numero di procedure attivate in un determinato arco temporale per le quali è pervenuta una sola offerta e del numero delle offerte escluse in un determinato arco temporale rispetto alle offerte presentate.

Tra le possibili misure di prevenzione adottate si richiamano:

- a) accessibilità on line della documentazione di gara o pubblicazione delle modalità per acquisire la documentazione
- b) predisposizione di inalterabili sistemi di protocollazione delle offerte
- c) obblighi di trasparenza/pubblicità delle nomine dei componenti delle commissioni
- d) individuazione di appositi archivi per la conservazione della documentazione.

1.4 Verifica dell'aggiudicazione e stipula del contratto

I possibili rischi di questa fase riguardano sia l'alterazione o l'omissione dei controlli e delle verifiche per favorire un aggiudicatario privo di requisiti o alterare la graduatoria, sia la violazione delle norme sulla trasparenza per evitare o ritardare la proposizione di ricorsi da parte di soggetti esclusi o non aggiudicatari.

Il RPC, con il supporto degli altri dirigenti responsabili, anche sulla base di presenza di denunce/ricorsi che evidenzino violazioni di legge, mancata, inesatta o incompleta effettuazione delle comunicazioni inerenti i mancati inviti, immotivato ritardo nella formalizzazione del processo di aggiudicazione definitiva e nella stipula del contratto, vigila sulla ricorrenza delle aggiudicazioni ai medesimi operatori economici.

1.5 Esecuzione del contratto

I possibili rischi di questa fase riguardano la mancata o insufficiente verifica dell'effettivo stato di avanzamento lavori rispetto al cronoprogramma al fine di evitare penali o risoluzione del contratto, l'abusivo ricorso alle varianti, l'apposizione di riserve generiche, il ricorso a sistemi alternativi per dirimere le controversie.

Le anomalie che possono manifestarsi in questa fase riguardano la motivazione incoerente o illogica sull'adozione di varianti, la concessione di proroghe non motivate nei tempi di esecuzione, la mancata segnalazione all'ANAC delle varianti, l'assenza del PSC, l'ammissione di riserve oltre i limiti consentiti dalla legge.

Il RPC vigila, con il supporto dei dirigenti responsabili, durante le fasi di approvazione delle modifiche del contratto originario, autorizzazione al subappalto, ammissione delle varianti, verifiche in corso di esecuzione, verifica delle disposizioni in materia di sicurezza con particolare riferimento ai contenuti del Piano di Sicurezza e Coordinamento (PSC) e del DUVRI, apposizione di riserve, gestione delle controversie, effettuazione di pagamenti in corso di esecuzione.

Tra le possibili misure di prevenzione che la Fondazione adotta si richiamano:

- a) controllo sull'applicazione di penali per il ritardo nell'esecuzione
- b) previsione di una relazione con valore interno da inviarsi al RPC da parte del RP contenente l'istruttoria condotta sulla legittimità delle riserve
- c) verifica del corretto assolvimento dell'obbligo di comunicazione all'ANAC delle varianti, in caso di subappalto.

1.6 Rendicontazione del contratto

I possibili rischi di questa fase riguardano le alterazioni o le omissioni delle attività di controllo, l'effettuazione di pagamenti ingiustificati o non tracciati. I processi rilevanti di questa fase sono: nomina del collaudatore, procedimento di verifica della corretta esecuzione per il rilascio del certificato di collaudo, attività connesse alla rendicontazione dei lavori in economia da parte del RP.

Il RPC vigila, con il supporto dei dirigenti responsabili, anche sulla base dello scostamento medio dei costi e dei tempi rispetto ai contratti aggiudicati, su: incompletezza della documentazione inviata dal RP ai sensi dell'art. 10 c. 7 del DPR 207/2010 (contratto, relazione al conto finale, ordinativi di pagamento con gli allegati di spesa relativi, relazione degli organi di collaudo e certificato di collaudo, esiti stragiudiziali, arbitrali e giudiziali sulle controversie), mancato invio al RP della documentazione prevista (ad es. verbali di visita), emissione di un certificato di regolare esecuzione relativo a prestazioni non effettivamente eseguite.

2. ACQUISIZIONE E GESTIONE DEL PERSONALE

L'Area HR:

1. provvede al reclutamento dei collaboratori attraverso procedure di evidenza pubblica (call) delineando profili e posizioni
2. procede alla selezione del personale con il Direttore Generale e alle azioni di contrattualizzazione e avviamento al lavoro
3. supervisiona le procedure di amministrazione del personale, le denunce iniziali e periodiche agli enti, la gestione corrente dei collaboratori, i rapporti con il consulente del lavoro
4. gestisce il reclutamento e l'organizzazione di tirocinanti e volontari
5. provvede eventuali attività di formazione interna

Comunica periodicamente gli esiti dell'attività svolta al RPCT.

3. NOMINA DEGLI ORGANI DI INDIRIZZO POLITICO E CONFERIMENTO DI INCARICHI DIRIGENZIALI

La Fondazione è tenuta al rispetto delle seguenti disposizioni sia in sede di nomina degli organi di indirizzo politico sia in caso di conferimento di incarichi dirigenziali.

Condizione di efficacia del conferimento dell'incarico dirigenziale è la presentazione, da parte dell'interessato, della dichiarazione di insussistenza delle cause di inconfiribilità³ previste dal d.lgs. n. 39/2013; il decreto citato stabilisce inoltre,

³ **Inconfiribilità**: preclusione, permanente o temporanea, a conferire incarichi a coloro che abbiano riportato condanne penali per i reati previsti dal capo I del titolo II del libro secondo del codice penale, a coloro che abbiano svolto incarichi o ricoperto cariche in enti di diritto privato regolati o

che il Dirigente deve presentare annualmente una dichiarazione in ordine all'insussistenza delle cause di incompatibilità⁴ ivi indicate.

Il D. Lgs. 39/2013, recante disposizioni in materia di inconferibilità e incompatibilità degli incarichi ha disciplinato:

- 1) particolari ipotesi di inconferibilità di incarichi agli organi di indirizzo politico o a dirigenti in relazione all'attività svolta dall'interessato in precedenza
- 2) incompatibilità per i titolari di incarichi
- 3) inconferibilità di incarichi per i soggetti destinatari di sentenze di condanna per delitti contro la pubblica amministrazione.

In particolare il decreto regola le ipotesi di inconferibilità degli incarichi in riferimento a:

- a) incarichi a soggetti provenienti da enti di diritto privato regolati o finanziati dalle pubbliche amministrazioni;
- b) incarichi a soggetti che sono stati componenti di organi di indirizzo politico.

La Fondazione adotta a presidio le seguenti misure:

- verifica la sussistenza di eventuali condizioni ostative in capo a dipendenti o soggetti cui il Direttore intende conferire incarico all'atto del conferimento degli incarichi dirigenziali e degli altri incarichi previsti dai Capi III e IV del D. Lgs. 39/2013, mediante una dichiarazione resa dall'interessato ai sensi degli artt. 46 e 47 del DPR 445/2000 e pubblicato sul sito;
- impartisce direttive interne affinché i soggetti interessati rendano la dichiarazione di insussistenza delle cause di inconferibilità all'atto del conferimento dell'incarico.

La dichiarazione è presentata ai sensi degli artt. 46 e 47 d.P.R. n. 445/2000 dagli interessati:

- ai fini del conferimento dell'incarico, entro 15 giorni dalla richiesta del Direttore;
- per l'accertamento annuale dell'insussistenza di cause d'incompatibilità per tutta la durata dell'incarico, a prescindere da una espressa richiesta da parte della Società.

La mancata presentazione della dichiarazione, in ogni caso, sarà valutata ai fini della responsabilità disciplinare.

Le dichiarazioni presentate da ciascun incaricato sull'insussistenza di cause di inconferibilità e/o di incompatibilità sono:

- pubblicate, per la parte richiesta dal citato d.lgs. n. 39, sul sito internet della Fondazione nell'apposita sezione Amministrazione Trasparente;
- verificate dal RPCT.

La dichiarazione rivelatasi mendace comporta la nullità dell'incarico, l'inconferibilità di qualsiasi incarico all'interessato per un periodo di 5 anni, la pubblicazione del relativo provvedimento sul sito internet della Società, nonché la segnalazione del fatto all'ANAC e alla Corte dei Conti.

Nel caso in cui emergano:

- situazioni di incompatibilità, il RPCT contesterà all'incaricato la circostanza e l'interessato dovrà, entro 15 giorni, indicare a quale incarico intende rinunciare. In mancanza di comunicazione, l'interessato decade dall'incarico conferito dall'Ente e il contratto si risolve;

finanziati da pubbliche amministrazioni o svolto attività professionali a favore di questi ultimi, a coloro che siano stati componenti di organi di indirizzo politico.

⁴ **Incompatibilità:** l'obbligo per il soggetto cui viene conferito l'incarico di scegliere, a pena di decadenza, entro il termine perentorio di quindici giorni, tra la permanenza nell'incarico e l'assunzione e lo svolgimento di incarichi e cariche in enti di diritto privato regolati o finanziati dalla pubblica amministrazione che conferisce l'incarico, lo svolgimento di attività professionali ovvero l'assunzione della carica di componente di organi di indirizzo politico. In particolare, gli incarichi dirigenziali che comportano poteri di vigilanza o controllo sulle attività svolte dagli enti di diritto privato regolati o finanziati dall'amministrazione che conferisce l'incarico, sono incompatibili con l'assunzione e il mantenimento, nel corso dell'incarico, di incarichi e cariche in enti di diritto privato regolati o finanziati dall'amministrazione che conferisce l'incarico, nonché con lo svolgimento in proprio di un'attività professionale se questa è regolata, finanziata o comunque retribuita dall'amministrazione che conferisce l'incarico. Inoltre, gli incarichi dirigenziali sono incompatibili con l'assunzione e il mantenimento, nel corso dell'incarico, della carica di componente dell'organo di indirizzo nella stessa amministrazione che ha conferito l'incarico.

- cause di inconferibilità, il RPCT contesta all'incaricato la circostanza e adotta il conseguente provvedimento, sentito l'Organo Amministrativo: nei casi di condanna non definitiva, al dirigente di ruolo, salve le ipotesi di sospensione o cessazione del rapporto, per la durata del periodo di inconferibilità, possono essere conferiti incarichi diversi da quelli che comportano l'esercizio delle competenze di amministrazione e gestione, ad esclusione di incarichi relativi ad uffici preposti alla gestione delle risorse finanziarie, all'acquisizione di beni, servizi e forniture, nonché alla concessione o all'erogazione di sovvenzioni, contributi, sussidi, ausili finanziari o attribuzioni di vantaggi economici a soggetti pubblici e privati, di incarichi che comportano esercizio di vigilanza o controllo. Qualora ciò non sia possibile, il dirigente è posto a disposizione del ruolo senza incarico per il periodo di inconferibilità dell'incarico.

La situazione di inconferibilità cessa di diritto se è pronunciata sentenza, anche non definitiva, di proscioglimento per il reato che ha determinato l'inconferibilità. In caso di soggetto esterno, la condanna o la sentenza ex art. 444 c.p.p., anche non definitiva, comporta la sospensione dell'incarico e dell'efficacia del contratto di lavoro subordinato o di lavoro autonomo stipulato con l'amministrazione, della stessa durata del periodo di inconferibilità.

Per tutto il periodo della sospensione non spetta alcun trattamento economico. Fatto salvo il termine finale del contratto, all'esito della sospensione l'amministrazione valuta la persistenza dell'interesse all'esecuzione dell'incarico, anche in relazione al tempo trascorso. L'interessato è in ogni caso tenuto a comunicare qualunque variazione in ordine alle condizioni prima viste entro 15 giorni dal momento in cui lo stesso ne è venuto a conoscenza.

5. AUTORIZZAZIONI E CONCESSIONI

Allo scopo di prevenire reati di corruzione e truffa nei confronti delle controparti pubbliche (Enti locali, ASL, Vigili del fuoco, ecc.) e garantire la necessaria trasparenza nella richiesta di nuove concessioni coerentemente con quanto definito nelle relative concessioni, la Fondazione come richiamato nel par. 3.2 Sez. A del Modello adotta le seguenti misure:

1. è responsabile della gestione delle concessioni in essere il Manager Amministrativo;
2. il Manager Amministrativo è responsabile della direzione e controllo delle attività svolte dai sottoposti e dell'attività di individuazione e gestione dei rischi pertinenti lo svolgimento delle attività sotto la propria direzione;
3. è compito del Dirigente di studi e progetti monitorare l'evoluzione dell'iter amministrativo per l'ottenimento dei permessi/licenze/autorizzazioni necessari e riferire periodicamente con report scritto al RPC a titolo esemplificativo in merito a:
 - a. eventuali dinieghi delle autorizzazioni richieste e relative motivazioni;
 - b. formali contestazioni in merito alle richieste inoltrate ed alle azioni intraprese.

Di seguito una tabella di sintesi con l'indicazione delle attività a rischio, delle Direzioni/Funzioni coinvolte e delle misure adottate.

ATTIVITA'	FUNZIONI COINVOLTE	MISURE ADOTTATE
Affidamento di lavori, forniture e servizi	Organo Amministrativo, Direttore Generale, Manager Amministrativo, Responsabile dell'Area Appalti e Contratti	Modello 231/01, Codice Etico
Selezione reclutamento del personale	Organo Amministrativo, Direttore Generale, Manager Amministrativo, Responsabile HR	Modello 231/01, Codice Etico
Autorizzazioni, concessioni, gestione delle sanzioni	Organo Amministrativo, Direttore Generale, Manager Amministrativo.	Modello 231/01, Codice Etico

Conferimento incarichi di consulenza, studio, ricerca e collaborazione	Organo Amministrativo, Direttore generale, Servizio Approvvigionamento e Appalti, Responsabili di Aziende, Servizi e di Divisioni	Modello 231/01, Codice Etico
---	---	------------------------------

Sezione “B”: art. 25 ter D. Lgs. 231/01

Reati societari

La presente Sezione dedicata ai reati societari è suddivisa nelle seguenti parti:

1. **Reati e modalità di commissione;** contiene la descrizione delle fattispecie criminose rilevanti richiamate dall’art. 25 ter del Decreto
2. **Aree sensibili e processi a rischio;** in conformità a quanto prescritto dall’art. 6 co. 2 del Decreto, illustra sinteticamente le attività a rischio nell’ambito dell’organizzazione e dell’attività aziendale e il livello di rischio associato
3. **Presidi interni;** descrive le responsabilità istituzionali a norma di legge, richiama i ruoli e le responsabilità organizzative interne e individua i principi di comportamento da adottarsi.

1. Reati e modalità di commissione

Di seguito sono riportati gli articoli contenuti nell’art. 25 ter del Decreto con un commento rispetto alle condotte sanzionate e ai soggetti qualificati alla loro commissione.

False comunicazioni sociali (artt. 2621 c.c.)

Il reato previsto dall’art. 2621 c.c. è un reato proprio: conseguentemente, per la sua configurabilità, è necessario che ad agire sia un soggetto provvisto della qualifica richiesta dalla legge, ovvero Amministratori, Direttori Generali, Sindaci e Liquidatori. E’ possibile, tuttavia, che le falsità o le dolose omissioni di informazioni in bilancio e nella nota integrativa siano poste in essere dai livelli sottostanti, segnatamente dai dirigenti responsabili della redazione dei documenti contabili societari; in tal caso esse configurano reato se gli amministratori, a conoscenza delle stesse, le abbiano deliberatamente fatte proprie. Il reato è normalmente considerato ad elevato rischio intrinseco per la molteplicità delle modalità e facilità di commissione.

Fatti di lieve entità (art. 2621 bis c.c.)

Al successivo art 2621 bis, è prevista una riduzione della pena se i fatti di cui all’art. 2621 c.c. sono considerati di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità e degli effetti della condotta. La stessa riduzione della pena è prevista se i fatti di cui all’art 2621 riguardano società che non superano i limiti indicati dal secondo comma dell’art 1⁵ Regio Decreto 16 marzo 1942, n.267.

False comunicazioni sociali per le società quotate (Art. 2622 c.c.)

Il reato, applicabile alle sole società quotate, punisce i medesimi soggetti di cui sopra e il Dirigente preposto, nel caso di comunicazioni sociali dirette ai soci ed espongono consapevolmente fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti in modo concretamente idoneo ad indurre altri in errore.

Impedito controllo (art. 2625 c.c.)

5 Sostituito dall’art 1 del d.lgs. n. 5/2006 con il seguente: “Non sono piccoli imprenditori gli esercenti attività commerciale in forma individuale o collettiva, che anche alternativamente:

- a. Hanno effettuato investimenti nell’azienda per un capitale di valore superiore a euro trecentomila;
- b. Hanno realizzato, in qualunque modo risulti, ricavi lordi calcolati sulla base della media degli ultimi tre anni, o dall’inizio dell’attività se di durata inferiore, per un ammontare complessivo annuo superiore a euro duecentomila”.

Tale ipotesi di reato consiste nell'impedire od ostacolare, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali qualora tale condotta abbia cagionato un danno ai soci. L'illecito può essere commesso esclusivamente dagli amministratori.

Indebita restituzione dei conferimenti (art. 2626 c.c.)

Tale ipotesi di reato consiste nel procedere, fuori dei casi di legittima riduzione del capitale sociale, alla restituzione, anche simulata, dei conferimenti ai soci o alla liberazione degli stessi dall'obbligo di eseguirli. Soggetti attivi del reato possono essere solo gli amministratori.

Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)

Tale ipotesi di reato consiste nella ripartizione di utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, ovvero nella ripartizione di riserve (anche non costituite con utili) che non possono per legge essere distribuite. Si fa presente che la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato. Soggetti attivi del reato sono gli amministratori.

Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)

Tale ipotesi di reato consiste nel procedere – fuori dai casi consentiti dalla legge – all'acquisto od alla sottoscrizione di azioni o quote emesse dalla società (o dalla società controllante) che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge. Si fa presente che se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto. Soggetti attivi del reato sono gli amministratori. Inoltre, è configurabile una responsabilità a titolo di concorso degli amministratori della controllante con quelli della controllata, nell'ipotesi in cui le operazioni illecite sulle azioni della controllante medesima siano effettuate da questi ultimi su istigazione dei primi.

Operazioni in pregiudizio dei creditori (art. 2629 c.c.)

Tale ipotesi di reato consiste nell'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o di fusioni con altra società o di scissioni, tali da cagionare danno ai creditori. Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.)

Tale ipotesi di reato consiste nella violazione degli obblighi previsti dall'art. 2391, comma primo, c. c. da parte dell'amministratore di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione Europea o diffusi fra il pubblico in maniera rilevante ai sensi dell'art. 116 TUF (ovvero di altri soggetti sottoposti a vigilanza), se dalla predetta violazione siano derivati danni alla società o a terzi. L'art. 2391, comma primo, c. c. impone agli amministratori delle società per azioni di dare notizia agli altri amministratori di ogni interesse che, per conto proprio o di terzi, abbiano in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata. Gli amministratori delegati devono altresì astenersi dal compiere l'operazione, investendo della stessa l'organo collegiale. L'amministratore unico deve darne notizia anche alla prima assemblea utile.

Formazione fittizia del capitale (art. 2632 c.c.)

Tale ipotesi di reato è integrata dalle seguenti condotte: a) formazione o aumento in modo fittizio del capitale sociale mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale; b) sottoscrizione reciproca di azioni o quote; c) sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono gli amministratori e i soci conferenti. Si precisa che non è, invece, incriminato l'omesso controllo ed eventuale revisione da parte di amministratori e sindaci, ai sensi dell'art. 2343, 3° comma, c.c. della valutazione dei conferimenti in natura contenuta nella relazione di stima redatta dall'esperto nominato dal Tribunale.

Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)

Tale ipotesi di reato consiste nella ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori. Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato. Soggetti attivi del reato sono esclusivamente i liquidatori.

Corruzione tra privati (2635 c.c.)

Tale ipotesi di reato rileva ai fini della responsabilità amministrativa dell'ente qualora i soggetti apicali o i soggetti subordinati diano o promettano denaro o altra utilità a:

- amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori di altre società;
- coloro che siano sottoposti alla direzione o alla vigilanza di uno dei soggetti di cui al punto che precede.

Si fa presente che l'ente risponderà del reato quando i predetti soggetti agiscano come corruttori, non anche quando siano stati corrotti.

Illecita influenza sull'assemblea (art. 2636 c.c.)

Tale ipotesi di reato consiste nel determinare la maggioranza in assemblea con atti simulati o fraudolenti, allo scopo di conseguire, per sé o per altri, un ingiusto profitto. Il reato è comune, può essere pertanto commesso da "chiunque" ponga in essere la condotta criminosa.

Aggiotaggio (art. 2637 c.c.)

Tale ipotesi di reato consiste nella diffusione notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di Vigilanza (art. 2638 c.c.)

Si tratta di due ipotesi di reato distinte per modalità di condotta e momento offensivo:

- la prima si realizza (i) attraverso l'esposizione nelle comunicazioni previste dalla legge alle Autorità pubbliche di Vigilanza (al fine di ostacolare l'esercizio delle funzioni di queste ultime) di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero (ii) mediante l'occultamento, con altri mezzi fraudolenti, di fatti che avrebbero dovuto essere comunicati e concernenti la medesima situazione economica, patrimoniale o finanziaria. La responsabilità sussiste anche nell'ipotesi in cui le informazioni riguardino beni posseduti od amministrati dalla società per conto di terzi;
- la seconda si realizza con il semplice ostacolo all'esercizio delle funzioni di vigilanza svolte da parte di pubbliche Autorità, attuato consapevolmente e in qualsiasi forma, anche omettendo le comunicazioni dovute alle Autorità medesime.

Soggetti attivi dell'ipotesi di reato descritta sono gli amministratori, i direttori generali, i sindaci e i liquidatori.

Estensione delle qualifiche soggettive (art. 2639 c.c.)

Per tutti i reati previsti nella presente sezione, al soggetto formalmente investito della qualifica o titolare della funzione prevista dalla legge civile è equiparato sia chi è tenuto a svolgere la stessa funzione, diversamente qualificata, sia chi esercita in modo continuativo e significativo i poteri tipici inerenti alla qualifica o alla funzione. Fuori dei casi di applicazione delle

norme riguardanti i delitti dei pubblici ufficiali contro la pubblica amministrazione, le disposizioni sanzionatorie relative agli amministratori si applicano anche a coloro che sono legalmente incaricati dall'autorità giudiziaria o dall'autorità pubblica di vigilanza di amministrare la società o i beni dalla stessa posseduti o gestiti per conto di terzi.

2. Aree sensibili e processi a rischio

Le aree sensibili sono stabilite specificamente dal Decreto che identifica processi e attività considerate astrattamente a rischio (bilancio, operazioni sul capitale ecc.). Tra questi:

a) coordinamento e gestione della contabilità generale, con particolare riferimento alle attività di:

- rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi, finanziari ed economici;
- corretta tenuta dei rapporti amministrativi con i terzi (es. clienti, fornitori);
- gestione amministrativa e contabile dei cespiti;
- accertamenti di tutti gli altri fatti amministrativi in corso d'anno (es. costi del personale, penalità contrattuali, finanziamenti passivi e relativi interessi, ecc.);
- verifica dei dati provenienti dai sistemi alimentanti.

b) raccolta e aggregazione dei dati contabili necessari per la predisposizione delle bozze di Bilancio

c) tenuta delle scritture contabili e dei Libri Sociali.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'OdV in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati) o di fattori interni (ad esempio, modifiche organizzative o di business).

3. Presidi interni

3.1 Presidio degli amministratori

Per quanto riguarda individualmente gli amministratori, ad essi compete l'obbligo di adempiere i doveri a essi imposti dalla legge e dallo statuto con la dovuta diligenza (art. 2392 c.c.) nonché l'obbligo di agire informati (art. 2381 ultimo comma); a tale dovere si associa l'assenso alla delibera consiliare relativa ad operazioni sul capitale ovvero la manifestazione del proprio dissenso ex art. 2392. Per tutte le operazioni che comportano valutazioni soggettive inerenti a operazioni di conferimento di beni in titoli o in natura con il conseguente rischio di sopravvalutazione rilevante, il CdA nel suo plenum adotta i seguenti presidi:

- in caso di crediti, conferisce a professionista indipendente, ovvero a primaria Società di revisione iscritta all'albo Consob, l'incarico di revisione degli eventuali crediti e di valutazione del loro valore di realizzo, tenendo conto anche dei tempi necessari
- in caso di beni immobili conferisce a professionista indipendente ovvero a società di appraisal, l'incarico di valutazione dei beni conferiti, l'accertamento dell'esistenza di eventuali gravami ipotecari e diritti reali di terzi, nonché della conformità alle norme locali in materia di edilizia
- qualora il conferimento riguardi impianti e beni strumentali all'attività, incarica professionisti esperti del settore in merito alla valutazione tecnico economica che tenga anche conto dello stato di funzionalità e manutenzione, nonché dello stato di obsolescenza tecnica
- qualora il conferimento riguardi un complesso aziendale di beni organizzati, osserva le medesime prescrizioni sopra riportate.

3.2 Presidio del collegio dei revisori

Compete al Collegio l'obbligo di monitorare periodicamente lo stato dei conferimenti in essere segnalando al Consiglio eventuali more dei soci sottoscrittori e sollecitando lo stesso a intervenire qualora siano decorsi i termini entro i quali sia

legittimamente esperibile l'esclusione del socio. In occasione delle delibere assembleari che prevedono operazioni di distribuzione di utili o riserve (nei confronti dei soli soci finanziatori), compete al Collegio verificare preliminarmente che le stesse vengano effettuate in conformità alla normativa vigente ed al disposto dello statuto, rendendone edotti gli Amministratori, benché agli stessi compete l'obbligo di agire informati, prima della data fissata per la delibera.

3.3 Doveri e responsabilità delle direzioni e funzioni interne

In relazione all'ambito di manifestazione degli illeciti trattati nella presente sezione, rilevano le funzioni interne riconducibili all'area amministrativa per quanto attiene la veridicità e completezza delle informazioni fornite nel contesto delle operazioni sopra descritte. Le funzioni richiamate collaborano attivamente con il Collegio fornendo senza indugio le informazioni richieste da quest'ultimo e segnalando tempestivamente il verificarsi di anomalie o disfunzioni nel normale svolgimento delle proprie mansioni qualora lo ritengano necessario.

a) Per la prevenzione dei reati di false comunicazioni sociali (ex art. 2621 c.c.) e false comunicazioni sociali in danno dei soci e dei creditori (ex art. 2622 c.c.), la redazione del bilancio annuale, della relazione sulla gestione e della relazione semestrale si richiede:

- la sottoscrizione da parte dei responsabili che hanno concorso alla formazione della bozza di bilancio e delle altre comunicazioni sociali di una dichiarazione attestante la veridicità, la completezza e la coerenza dei dati e delle informazioni ivi contenute;
- l'esame del progetto di bilancio, antecedentemente all'approvazione assembleare, da parte dell'Organismo di Vigilanza;
- la verifica, con cadenza periodica, dei saldi dei conti di contabilità generale al fine di garantire la quadratura della contabilità generale con i rispettivi partitari e con i conti sezionali;
- l'identificazione delle risorse interessate, dei dati e delle informazioni che le stesse devono fornire, nonché delle tempistiche, per la predisposizione del bilancio o di altra comunicazione sociale;
- la verifica della completezza e correttezza dei dati e delle informazioni comunicate dalle suddette risorse e sigla sulla documentazione analizzata;

b) Per la prevenzione dei reati di indebita restituzione di conferimenti (ex art. 2626 c.c.), illegale ripartizione degli utili e delle riserve (ex art. 2627 c.c.), illecite operazioni sulle azioni sociali (ex art. 2628), operazioni in pregiudizio dei creditori (ex art. 2629 c.c.), formazione fittizia del capitale (ex art. 2632 c.c.), considerato che l'obiettivo è evitare tutte le condotte idonee, anche solo potenzialmente, a ledere l'integrità del capitale sociale, è necessario:

- assegnare specificatamente le responsabilità decisionali ed operative per l'effettuazione di attività che vengono ad incidere sul capitale sociale e stabilire meccanismi di coordinamento tra le varie funzioni coinvolte;
- informare delle attività di cui al punto precedente l'Organismo di Vigilanza.

c) Per la prevenzione dei reati di omessa convocazione dell'assemblea (ex art. 2631 c.c.) e illecita influenza sull'assemblea (ex art. 2636 c.c.), considerato che si tratta di condotte illecite dirette ad influenzare la libera e corretta formazione della volontà assembleare e del mercato è necessario disciplinare le procedure attraverso le quali l'organo amministrativo rilascia informazioni ai soci in ordine alle materie all'ordine del giorno, anche attraverso l'adozione di uno specifico regolamento assembleare;

d) Per la prevenzione dei reati inerenti i rapporti con il Collegio, i soggetti che, in ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione di tali rapporti sono tenuti ad eseguire le seguenti attività e controlli:

- espletare le attività conseguenti alle richieste del Collegio, fornendo le informazioni e l'eventuale documentazione tempestivamente, verificandone previamente l'integrità e la completezza;
- assicurare la tracciabilità della consegna della documentazione richiesta, archiviando documenti di presa in consegna della documentazione sottoscritti dai componenti del Collegio.

3.4 Ulteriori presidi

I destinatari del Modello hanno l'obbligo di:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure della Fondazione, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire al socio ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;
2. osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
3. assicurare il regolare funzionamento della società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
4. 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 vigilanza.

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

con riferimento al precedente punto 1:

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società;

con riferimento al precedente punto 2:

- restituire conferimenti ai soci o liberarli dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- procedere a formazione o aumento fittizio del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale;

con riferimento al precedente punto 3:

- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo da parte del socio, del Collegio dei revisori;
- porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- omettere di mantenere traccia di tutta la documentazione richiesta e consegnata agli organi di controllo, nonché di quella utilizzata nell'ambito delle attività assembleari;

con riferimento al precedente punto 4:

- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti dell'Autorità di Vigilanza, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalla predetta autorità;
- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della società;

- 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 di vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

Al fine di prevenire la commissione del reato di corruzione tra privati, è fatto inoltre divieto di:

- effettuare ricevere o sollecitare elargizioni in denaro, regali o vantaggi di altra natura, ove eccedano le normali pratiche commerciali e di cortesia, a soggetti appartenenti ad enti privati;
- distribuire omaggi al di fuori di quanto previsto dalla prassi aziendale (vale a dire, secondo quanto previsto dal Codice etico, 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 soggetti appartenenti ad enti privati, o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico (ad esempio, la distribuzione di libri d'arte), o la brand image della Società. I regali offerti – salvo quelli di modico valore – devono essere documentati in modo adeguato per consentire le prescritte verifiche;
- accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.), in favore di soggetti appartenenti ad enti privati, che possano determinare le stesse conseguenze previste al precedente punto;
- effettuare prestazioni in favore dei consulenti, dei partner e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere.

Sezione “C”: art. 25 septies D. Lgs. 231/01

Reati in violazione delle norme sulla tutela della salute e della sicurezza sul lavoro

La presente Sezione dedicata ai reati di omicidio colposo (art. 589 c.p.) e di lesioni personali colpose gravi o gravissime (art. 590 c.p.) commessi in violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro ex D. Lgs. 9 aprile 2008, n. 81 e s.m.i. (d’ora in poi T.U.)⁶, è articolata nei seguenti paragrafi:

1. **Reati**; descrive i reati richiamati dall’art. 25 septies del Decreto con un breve commento sulla loro natura colposa
2. **Ruoli e responsabilità in materia di sicurezza**; richiama i soggetti rilevanti per la prevenzione e le responsabilità a questi attribuiti dal TU
3. **Misure di prevenzione adottate**
4. **Archivio della documentazione rilevante**; descrive le responsabilità connesse all’archiviazione della documentazione rilevante
5. **Modalità di collegamento tra OdV e SPP**; richiama i doveri dell’OdV ed i sistemi di comunicazione con i soggetti coinvolti in materia di sicurezza sul lavoro.

1. Reati

Omicidio colposo (art. 589 c.p.)

Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni.

Lesioni personali colpose (art. 590 c.p.)

Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a euro 309.

Si tratta di reati di natura *colposa* e non solo *dolosa*. Si ricorda che il *dolo* sussiste quando l’autore del reato agisce con volontà ed è cosciente delle conseguenze della sua azione od omissione; la *colpa* sussiste quando l’autore del reato, pur agendo con volontà, non ha in alcun modo preso coscienza delle conseguenze della sua azione a causa della sua negligenza, imprudenza, imperizia o inosservanza di leggi, regolamenti, ordini e discipline.

In merito *all’interesse o a vantaggio dell’ente* quale condizione per la responsabilità dell’ente ai sensi del Decreto 231/01, e la natura *colposa* di questi reati, la dottrina sostiene che il vantaggio dell’ente vada ricercato nel risparmio dei costi sostenuti per la prevenzione.

2. Ruoli e responsabilità in materia di sicurezza

2.1 Datore di lavoro

Il Presidente del CdA in qualità di *datore di lavoro*, ha adempiuto ai doveri dettati dall’art. 17 T.U. e in particolare:

1. ha effettuato la valutazione dei rischi ed elaborato il Documento di valutazione dei rischi che contiene:
 - una relazione sulla valutazione dei rischi per la salute e la sicurezza durante l’attività lavorativa nella quale sono specificati i criteri adottati per la valutazione stessa
 - l’individuazione delle misure di prevenzione e protezione attuate e dei dispositivi di protezione individuali adottati a seguito della valutazione
 - il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza

⁶ Per “norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro” si intendono non solo quelle inserite nelle leggi specificatamente antinfortunistiche, ma anche tutte quelle che, direttamente o indirettamente perseguono il fine di evitare incidenti sul lavoro o malattie professionali e che in genere tendono a garantire la sicurezza del lavoro in relazione all’ambiente in cui esso deve svolgersi.

- l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere
 - l'indicazione del nominativo del RSPP, del RLS e del medico competente
 - l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici
2. ha designato il RSPP.

2.2 Datore di lavoro e dirigenti

Il datore di lavoro e i dirigenti ai sensi dell'art. 18 del T.U. hanno il compito di:

- a) designare preventivamente i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e di gestione dell'emergenza
- b) affidare i compiti ai lavoratori, tenere conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute e alla sicurezza
- c) fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale, sentito il responsabile del servizio di prevenzione e protezione e il medico competente, ove presente
- d) prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico
- e) richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni interne in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione
- f) richiedere al medico competente l'osservanza degli obblighi previsti dal T.U.
- g) adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa
- h) informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione
- i) adempiere agli obblighi di informazione, formazione e addestramento di cui agli articoli 36 e 37
- j) astenersi, salvo eccezione debitamente motivata da esigenze di tutela della salute e sicurezza, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave e immediato
- k) consentire ai lavoratori di verificare, mediante il rappresentante dei lavoratori per la sicurezza, l'applicazione delle misure di sicurezza e di protezione della salute
- l) elaborare il documento di cui all'articolo 26, comma 3, anche su supporto informatico come previsto dall'articolo 53, comma 5, e, su richiesta di questi e per l'espletamento della sua funzione, consegnarne tempestivamente copia ai rappresentanti dei lavoratori per la sicurezza
- m) prendere appropriati provvedimenti per evitare che le misure tecniche adottate possano causare rischi per la salute della popolazione o deteriorare l'ambiente esterno verificando periodicamente la perdurante assenza di rischio
- n) consultare il rappresentante dei lavoratori per la sicurezza nelle ipotesi di cui all'articolo 50
- o) adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro, nonché per il caso di pericolo grave e immediato, secondo le disposizioni di cui all'articolo 43. Tali misure devono essere adeguate alla natura dell'attività, alle dimensioni dell'azienda o dell'unità produttiva, e al numero delle persone presenti
- p) nell'ambito dello svolgimento di attività in regime di appalto e di subappalto, munire i lavoratori di apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro
- q) aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione

- r) vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità
- s) fornire al SPP e al medico competente informazioni in merito alla natura dei rischi, all'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive, la descrizione degli impianti e dei processi produttivi, i provvedimenti adottati dagli organi di vigilanza
- t) nominare il medico competente per l'effettuazione della sorveglianza sanitaria
- u) consegnare tempestivamente ai rappresentanti dei lavoratori per la sicurezza, su richiesta di questi e per l'espletamento della sua funzione, copia del documento di cui all'art. 17 comma 1 lettera a nonché consentire al medesimo di accedere ai dati di cui alla lettera s)
- v) convocare la riunione periodica di cui all'art. 35.

2.3 Preposto

A norma di legge è considerato *preposto* chiunque assume una posizione di preminenza tale, rispetto agli altri lavoratori, da poter impartire istruzioni e direttive sulle modalità di svolgimento del lavoro e chi conseguentemente è tenuto all'osservanza dell'attuazione delle prescritte misure di sicurezza ed al controllo del rispetto di queste da parte dei lavoratori.

Il preposto, la cui qualifica è attribuita di fatto, in relazione alle mansioni effettivamente svolte, più che in base a formali definizioni giuridiche, in ragione delle competenze professionali e nei limiti di poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli:

- sovrintende e vigila sulla osservanza da parte dei singoli lavoratori dei loro obblighi di legge, delle disposizioni in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messi a loro disposizione e, in caso di inosservanza, informa i superiori diretti;
- verifica affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;
- richiede l'osservanza delle misure per il controllo delle situazioni di rischio;
- segnala tempestivamente al datore di lavoro o al dirigente sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro, delle quali venga a conoscenza sulla base della formazione ricevuta;
- in caso di pericolo grave e immediato da istruzioni affinché i lavoratori abbandonino il posto di lavoro o la zona pericolosa; informa tempestivamente i lavoratori sul rischio stesso e sulle le disposizioni prese o da prendere in materia di protezione; si astiene, salvo eccezioni debitamente motivate, dal richiedere ai lavoratori di riprendere la loro attività.

Il preposto è soggetto alle sanzioni di cui all'art. 56 del T.U.

2.4 RSPP e addetti al Servizio di Prevenzione e Protezione

Il RSPP e gli addetti al Servizio di Prevenzione e Protezione svolgono i compiti attribuiti dal Testo Unico e in particolare provvedono:

- all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
- a elaborare, per quanto di competenza, le misure preventive e protettive e i sistemi di controllo di tali misure;
- a proporre i programmi di informazione e formazione dei lavoratori;
- a elaborare le procedure di sicurezza per le varie attività;
- a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonché alla riunione periodica ex art. 35.

2.5 Lavoratori incaricati della gestione delle emergenze

I lavoratori incaricati di primo soccorso, salvataggio, lotta antincendio e gestione dell'emergenza, designati dal datore di lavoro ex art. 18 lett. b), sono destinatari di specifici corsi di formazione e dispongono di attrezzature adeguate tenuto conto delle dimensioni e dei rischi specifici.

2.6 RLS

In conformità alle disposizioni del T.U., il Rappresentante dei lavoratori per la Sicurezza è consultato preventivamente e tempestivamente:

- in ordine alla valutazione dei rischi, ricevendo le informazioni e la documentazione aziendale relativa;
- sulla designazione del Responsabile e degli addetti al servizio di prevenzione e sulla nomina del medico competente;
- sull'attività di prevenzione incendi, di primo soccorso, di evacuazione dei luoghi di lavoro;
- in merito all'organizzazione dell'attività di formazione;
- in occasione di visite e verifiche effettuate dalle autorità competenti, esprimendo in tali circostanza osservazioni e pareri.

Il RLS è informato sull'attività svolta dai servizi di vigilanza e sulle misure di prevenzione adottate dal datore di lavoro e dai dirigenti in relazione alla gestione delle sostanze e dei preparati pericolosi, all'organizzazione e agli ambienti di lavoro, agli infortuni e alle malattie professionali. Qualora il Responsabile ritenga che tali misure e i mezzi impiegati per attuarle non siano idonei a garantire la sicurezza e la salute durante il lavoro può fare ricorso alle autorità competenti.

2.7 Medico competente

Il medico competente attua un programma di sorveglianza sanitaria e in particolare effettua visite mediche e altri esami necessari per verificare l'idoneità dei lavoratori a svolgere una mansione specifica. Le visite e gli esami sono mirati al tipo di rischio a cui i soggetti sono sottoposti in relazione all'attività da questi svolta e sono prescritti prima della immissione al lavoro (visita pre assuntiva) e poi con periodicità variabile (visita periodica).

Il medico competente è soggetto alle sanzioni di cui all'art. 58 del T.U.

2.8 Lavoratori

Nell'ambito dell'attività formativa ai dipendenti è data altresì comunicazione dei doveri che a questi spettano per legge in materia di sicurezza (art. 20 T.U.)

In particolare i lavoratori hanno il dovere di:

- osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti ai fini della protezione collettiva ed individuale;
- utilizzare correttamente i macchinari, le apparecchiature, gli utensili, le sostanze e i preparati pericolosi, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;
- segnalare immediatamente al responsabile della sicurezza, al dirigente o al preposto le deficienze dei mezzi e dispositivi di cui alle lettere b) e c), nonché le altre eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli, dandone notizia al rappresentante dei lavoratori per la sicurezza;
- non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;
- sottoporsi ai controlli sanitari previsti nei loro confronti;
- contribuire, insieme al responsabile della sicurezza, ai dirigenti e ai preposti, all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro;

- partecipare ai programmi di formazione e addestramento organizzati dalla società.

I lavoratori sono soggetti alle sanzioni di cui all'art. 59 del T.U.

3. Misure adottate nei luoghi di lavoro

Il Presidente del CdA, in qualità di datore di lavoro (DL), ha adempiuto ai doveri del TU:

- 1) ha elaborato, con il supporto del RSPP e del medico competente all'uopo designati, il Documento di Valutazione dei Rischi (DVR) dopo aver considerato i luoghi di lavoro aziendale, le attività svolte, le responsabilità e le pratiche inerenti, attenendosi ai precetti di cui all'art. 15 tra cui: la valutazione dei rischi, la programmazione della prevenzione, l'eliminazione dei rischi e, ove ciò non sia possibile, la loro riduzione al minimo, il rispetto dei principi ergonomici, la riduzione dei rischi alla fonte, la sostituzione di ciò che è pericoloso con ciò che non lo è, o lo è di meno, la limitazione al minimo dei lavoratori esposti al rischio, l'utilizzo limitato degli agenti nocivi, la priorità delle misure di protezione collettiva rispetto alle misure di protezione individuale, il controllo sanitario dei lavoratori, l'allontanamento del lavoratore dall'esposizione al rischio per motivi sanitari inerenti la sua persona e l'adibizione, ove possibile, ad altra mansione, l'informazione, la formazione e l'addestramento, la partecipazione e la consultazione dei lavoratori, le misure di emergenza, l'uso di segnaletica, la regolare manutenzione di ambienti, attrezzature e impianti.
- 2) ha nominato il RSPP.

Conformemente alla disciplina di riferimento, oltre al datore di lavoro, soggetti rilevanti ai fini delle misure di prevenzione e protezione per i luoghi di lavoro riconducibili alla sede aziendale sono il Dirigente, il Responsabile del Servizio di Prevenzione e Protezione (RSPP) e gli altri addetti (ASPP), i preposti, i lavoratori incaricati della gestione delle emergenze, il Rappresentante dei Lavoratori per la Sicurezza (RLS), il Lavoratore e il Medico Competente, le cui responsabilità sono descritte al paragrafo precedente.

Il DVR, in conformità all'art. 28 del T.U.:

- a) individua e descrive i luoghi di lavoro aziendale
- b) descrive le attività svolte all'interno dei luoghi di lavoro individuati, con particolare attenzione a quelle che espongono i lavoratori a particolari rischi
- c) identifica i rischi per la salute e sicurezza dei lavoratori
- d) valuta la conformità delle misure di prevenzione adottate e propone pertanto azioni correttive che permettano di eliminare/ridurre/controllare il pericolo in conformità alle disposizioni legislative vigenti o tenendo conto delle norme di buona tecnica,
- e) contiene il Piano di Emergenza, il protocollo sanitario e la valutazione del rischio per mansioni specifiche

In caso di affidamento di lavori, servizi e forniture, contratti d'opera o di somministrazione nell'ambito dei luoghi di lavoro aziendale compete al RSPP:

1. verificare l'idoneità tecnica professionale delle imprese in relazione ai lavori, servizi e forniture da affidare, attraverso l'acquisizione del *certificato d'iscrizione alla Camera di commercio, industria ed artigianato* o *l'autocertificazione rilasciata dalla stessa impresa appaltatrice* (o lavoratori autonomi)
2. fornire alle imprese e/o ai lavoratori autonomi affidatarie ed esecutrici dei lavori, dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui sono destinati a operare e sulle misure di prevenzione e di emergenza adottate
3. valutare che il valore economico dell'offerta delle imprese sia adeguato e sufficiente rispetto al costo del lavoro e al costo relativo alla sicurezza, il quale, se del caso, deve essere specificamente indicato e risultare congruo rispetto all'entità e alle caratteristiche dei lavori, dei servizi o delle forniture;
4. promuovere la cooperazione e il coordinamento nei luoghi di lavoro elaborando un *unico documento di valutazione dei rischi* (DUVRI) portato a conoscenza dei dipendenti che indichi le misure adottate per eliminare

o ridurre al minimo i rischi derivanti dalle possibili interferenze tra l'attività dei propri lavoratori e quella dei soggetti affidatario

Se del caso, il RSPP monitora l'esecuzione dei lavori, ovvero affida la supervisione a un preposto dell'area di riferimento.

4. Archivio della documentazione rilevante

La responsabilità della conservazione della documentazione inerente quanto sopra descritto compete:

- a. al RSPP per quanto attiene
 - i. il DVR, gli aggiornamenti relativi e le procedure di sicurezza
 - ii. l'attività di formazione e informazione
 - iii. le statistiche relative agli infortuni
 - iv. le comunicazioni agli uffici pubblici di competenza
 - v. i verbali delle riunioni periodiche
 - vi. i verbali redatti dalle autorità del Servizio di Vigilanza nonché la raccolta delle disposizioni rilevanti;
- b. al medico competente per quanto attiene la sorveglianza sanitaria e le visite mediche.

5. Flussi informativi tra OdV e soggetti del SPP

Ai sensi dell'art. 30 del T.U., ad integrazione di quanto previsto dal d. lgs. 231/01 compete all'OdV monitorare l'adempimento degli obblighi previsti e mantenere adeguato supporto documentale delle attività di monitoraggio svolte. Atteso che il complesso degli adempimenti descritti nei paragrafi precedenti è conforme alle disposizioni del Testo Unico sulla sicurezza sul lavoro e al SPP adottato, l'OdV monitora l'adempimento degli obblighi riportati nei paragrafi precedenti.

Al fine di realizzare gli obiettivi sopra richiamati, occorre che i vari soggetti coinvolti nel sistema di prevenzione RSPP, RLS e tutti gli altri soggetti individuati per la compliance al Testo Unico si raccordino con l'Organismo di Vigilanza.

In particolare, con periodicità almeno semestrale, ciascuno dei soggetti e per le proprie competenze, trasmette all'OdV un report contenente:

- ♦ informazioni su infortuni verificatisi, distinti per gravità, con l'indicazione delle relative cause, dell'area aziendale di appartenenza del lavoratore e delle principali azioni correttive attuate;
- ♦ indici di frequenza e di gravità degli infortuni suddivisi per Funzioni;
- ♦ ispezioni effettuate dagli Enti preposti alla vigilanza (ASL, Guardia di Finanza, Vigili del fuoco, ecc.) sull'applicazione della legislazione in materia di salute e sicurezza sui luoghi di lavoro e dei provvedimenti adottati dagli stessi enti, nonché delle conseguenti azioni correttive attuate;
- ♦ esiti delle attività di monitoraggio in materia di sicurezza sul lavoro o che possono avere un impatto sulle principali attività a rischio

Il RSPP trasmette annualmente all'OdV un report avente ad oggetto:

- ♦ variazioni organizzative ritenute di rilievo ai fini dell'efficacia del Modello
- ♦ variazioni nella gestione di fatto delle attività, ritenute tali da incidere sull'efficacia del Modello
- ♦ le date delle riunioni tenute con il RLS, gli addetti del SPP e il medico competente
- ♦ le date degli aggiornamenti del DVR
- ♦ gli esiti delle ispezioni interne per la verifica del rispetto della normativa
- ♦ la situazione riepilogativa degli infortuni sul lavoro e delle eventuali iniziative intraprese per la loro prevenzione

Devono essere fornite con immediatezza all'Organismo di Vigilanza le informazioni su situazioni di riscontrata inadeguatezza e/o non effettività e/o non conformità al Modello e alle relative procedure, nonché di quelle relative alle norme generali e specifiche del T.U. affinché l'OdV possa trasmetterle all'organo dirigente che avrà il compito di convocare il SPP.

Il mancato rispetto delle misure indicate nel Modello a tutela della salute e sicurezza dei luoghi di lavoro potrà essere sanzionato in via disciplinare, previa segnalazione da parte dell'OdV, all'organo dirigente.

Sezione “D”: art. 24 bis D. Lgs. 231/01

Delitti di criminalità informatica e trattamento illecito dei dati

La presente Sezione della Parte Speciale dedicata ai reati societari, è suddivisa nelle seguenti parti:

1. **Reati e modalità di commissione;** contiene la descrizione delle fattispecie criminose rilevanti richiamate dall’art. 24 bis del Decreto
2. **Aree sensibili e processi a rischio;** in conformità a quanto prescritto dall’art. 6 co. 2 del Decreto, illustra sinteticamente le attività a rischio nell’ambito dell’organizzazione
3. **Protocolli di prevenzione;** sono richiamate le linee guida del garante della privacy sull’utilizzo delle risorse informatiche
4. **Flussi informativi verso l’OdV**

1. Reati e modalità di commissione

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

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

I reati la cui commissione è stata ritenuta remota, sono i seguenti:

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

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1. se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2. se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3. se dal fatto deriva la distruzione o il danneggiamento del sistema o l’interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all’ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d’ufficio.

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

Se il fatto di cui all’art. 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da 1 a 4 anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da 3 a 8 anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell’art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

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

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a 3 anni e con la multa da 51 a 1.032 euro.

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

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a 5.164 euro.

La pena è della reclusione da uno a due anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

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

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora cancella, altera o sopprime informazioni, dati o programmi informatici altrui, è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al n. 1) del secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

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

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione sino a due anni e con la multa sino a 10.329 euro.

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

Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

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

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

Chiunque, fuori dei casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

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.)

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da 3 a 8 anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

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

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da 1 a 5 anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Trattamento illecito di dati (art. 167 D.Lgs. 196/2003)

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per se' o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per se' o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

Falsità nelle dichiarazioni e notificazioni al Garante (art. 168 D.Lgs. 196/2003)

Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

Inosservanza di provvedimenti del Garante (art. 170 D.Lgs. 196/2003)

Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni.

Indebito utilizzo, falsificazione, alterazione e ricettazione di carte di credito o di pagamento (articolo 55 comma 9 D.Lgs. 231/2007)

Chiunque, al fine di trarne profitto per se' o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla

prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da 310 a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per se' o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonchè ordini di pagamento prodotti con essi.

Frode informatica commessa con sostituzione d'identità digitale (art. 640-ter c.p. come modificato dallo stesso D.L. 93/2013);

1. All'articolo 640-ter del codice penale, sono apportate le seguenti modificazioni:

- a) dopo il secondo comma, è inserito il seguente: "La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con sostituzione dell'identità digitale in danno di uno o più soggetti.";
- b) all'ultimo comma, dopo le parole "di cui al secondo" sono inserite le seguenti: "e terzo".

2. Aree sensibili

La società risulta essere esposta al rischio di commissione dei reati descritti nello svolgimento delle seguenti attività:

- creazione, gestione e diffusione di documenti informatici;
- accesso e gestione di sistemi informatici o telematici protetti da misure di sicurezza;
- installazione e diffusione di apparecchiature, dispositivi o programmi informatici.

3. Protocolli di prevenzione

La società ispirandosi ai principi di necessità, correttezza e segretezza enunciati nel Codice della Privacy, adotta un adeguato sistema di sicurezza basato su:

- regolamentazione dei comportamenti
- formazione obbligatoria
- controllo del personale interno ed esterno

che rappresenta un valido strumento per contrastare i rischi di:

- distruzione o perdita, anche accidentale, dei dati personali oggetto del trattamento;
- accesso non autorizzato;
- trattamento non consentito o non conforme alle finalità della raccolta.

Il Responsabile designato al fine di assicurare la funzionalità e il corretto impiego da parte degli utenti delle risorse informatiche:

- individua tutte le funzioni potenzialmente collegabili al rischio di reati informatici
- valuta il grado di rischio di commissione dei reati da parte del personale o di soggetti esterni (consulenti, agenti ecc.)
- ne definisce le modalità d'uso nell'organizzazione dell'attività lavorativa;
- adotta idonee misure di sicurezza, di tipo organizzativo e tecnologico per garantire la disponibilità e l'integrità di sistemi informativi e di dati e per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
- monitora il corretto impiego degli strumenti informatici, rispettando ad ogni modo, il divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese strumentazioni *hardware* e *software* mirate al controllo dell'utente attraverso ad esempio:
 - la lettura e la registrazione sistematica dei messaggi di posta elettronica;
 - la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
 - la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
 - l'analisi occulta di computer portatili affidati in uso
- elabora un Regolamento Interno relativo a:

- utilizzo del personal computer,
 - utilizzo della rete interna aziendale,
 - assegnazione e gestione delle password,
 - accesso a particolari informazioni,
 - prescrizioni sulla sicurezza dei dati e dei sistemi,
 - utilizzo e conservazione dei supporti rimovibili,
 - uso della posta elettronica,
 - uso della rete internet e dei relativi servizi,
 - policy in materia di privacy;
- osserva e garantisce il rispetto delle disposizioni contenute nel Regolamento;
 - aggiorna il Regolamento aziendale al verificarsi di eventi tali da pregiudicarne l'efficacia (modifiche legislative e regolamentari, mutamenti della struttura aziendale e delle funzioni coinvolte nello svolgimento dell'attività ecc.);
 - rende consapevoli i lavoratori delle potenzialità degli strumenti e dei programmi elettronici implementati dall'azienda, attraverso un'attività di formazione obbligatoria che illustra:
 - i rischi che incombono sui dati,
 - le misure disponibili per prevenire eventi dannosi
 - i profili della disciplina sulla privacy più rilevanti in rapporto alle relative attività
 - le responsabilità che ne derivano
- e che viene implementata al momento dell'assunzione, in occasione di cambiamenti di mansioni e in relazione all'introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati personali.

Internet e relativi servizi

L'utilizzo di internet deve avvenire nel rispetto della legge, dei principi di etica professionale e unicamente a fini interni, al solo scopo di coadiuvare l'utilizzatore nell'esercizio delle proprie mansioni e non per questioni personali.

L'uso imprudente di alcuni servizi della rete internet, ancorché nell'ambito della normale attività aziendale, può essere fonte di particolari minacce alla sicurezza dei dati e dell'immagine aziendale.

Conformemente alle Linee Guida sulla privacy FONDAZIONE adotta le seguenti misure:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevenivano determinate operazioni, reputate estranee all'attività lavorativa, quali l'*upload* o l'accesso a determinati siti (inseriti in una sorta di *black list*) e/o il *download* di *file* o *software* aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza

In relazione all'impiego di internet, ogni utente:

- deve evitare lo scaricamento (*upload* e/o *download*) di file e/o programmi software, anche gratuiti, se non per esigenze strettamente organizzative e fatti salvi i casi di esplicita autorizzazione della Direzione;
- non può effettuare transazioni finanziarie di ogni genere, ivi comprese le operazioni di *remote banking*, acquisti online e simili, salvo i casi direttamente autorizzati dalla Direzione competente e con il rispetto delle normali procedure degli acquisti;
- non può partecipare a forum non della Fondazione, né utilizzare chat-line, bacheche elettroniche anche utilizzando pseudonimi e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non strettamente inerenti all'attività aziendale;
- non può accedere a servizi con finalità ludiche o estranei all'attività per tempi eccessivamente prolungati e comunque durante l'orario di servizio;
- non può manomettere o creare nuovi collegamenti (internet);

- deve evitare di condividere file su internet, in quanto tale operazione significa lasciare una “porta aperta” a virus e a particolari software (spyware, key logger) che inviano, a chi li realizza, informazioni personali a insaputa dell’utente;
- non deve fornire informazioni personali a siti sospetti, verificando sempre la sicurezza del sito, mediante la presenza del prefisso “” nell’indirizzo web e dell’icona “lucchetto chiuso” nella barra degli strumenti;
- non può visualizzare, archiviare, trasmettere o scaricare materiale fraudolento, pornografico, osceno, diffamatorio, intimidatorio e/o illegale. La società e le sue rappresentanze locali non si assumono alcuna responsabilità a riguardo.

Uso del Personal Computer

L’utente è responsabile delle macchine ad esso affidate per quanto riguarda la conservazione, l’efficienza, la regolarità di funzionamento e la pulizia.

Ogni Personal Computer, in qualunque configurazione, viene consegnato all’utente dotato di tutto ciò che necessita per il corretto funzionamento sia per quanto riguarda hardware che software:

Infatti, tutti i computer sono protetti mediante:

- un *software antivirus* che:
 - protegge in tempo reale e quotidianamente il computer e i dati letti/scritti;
 - verifica che tutte le informazioni presenti nei dischi siano libere da virus;
 - aggiorna automaticamente il dizionario dei virus ad ogni collegamento alla Intranet aziendale;
 - gestisce e rende visibile centralmente lo stato dei computer;
 - distribuisce gli aggiornamenti mediante i server di sede;
 - è attivo per qualsiasi file che entra sul computer;
- una o più *password* di accesso, così come previsto dalle misure minime di sicurezza regolate dal Codice. Le password assegnate:
 - devono essere composte da almeno otto caratteri alfanumerici, oppure, nel caso in cui lo strumento elettronico non lo consenta, da un numero di caratteri pari al massimo consentito;
 - non devono contenere riferimenti agevolmente riconducibili all’incaricato e devono essere periodicamente modificate.
 - sono personali e non devono essere divulgate a terzi ed all’esterno dell’azienda;
 - devono essere custodite dall’assegnatario con la massima diligenza;
- dispositivi di filtraggio (firewall): si tratta di dispositivi hardware o software, che filtrano tutti i pacchetti entranti ed uscenti, da e verso una rete o un computer, applicando regole che innalzano il livello di sicurezza della rete e permettendo sia agli utenti interni che a quelli esterni di operare nel massimo della sicurezza.

Con riferimento all’uso di personal computer, al lavoratore è vietato:

- modificare la struttura del disco fisso predisposta dal Servizio I.T.;
- manomettere la struttura logica (driver, schede di memoria ecc.) della macchina;
- far utilizzare i PC o darli in uso a terzi (o familiari) che non siano dipendenti della società o da questa specificatamente autorizzati;
- utilizzare software provenienti da fonti irregolari o non regolarmente acquistati;
- divulgare dati, schede o software della Società senza l’autorizzazione del proprio superiore gerarchico;
- collegarsi al sistema informatico celando la propria identità e utilizzando il nome e/o la password di un altro utente;
- installare nella rete aziendale un proprio software che non rientri nello scopo per cui il sistema informatico è stato assegnato all’utente, al fine di evitare il rallentamento o il blocco della rete informatica aziendale.

Fermo restando quanto sopra a carico di tutti i Destinatari è fatto divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;

- porre in essere condotte, anche con l'ausilio di terzi, miranti ad accedere in maniera non autorizzata ai sistemi informativi utilizzati dalla Pubblica Amministrazione o a sistemi informativi altrui con l'obiettivo di:
 - acquisire abusivamente informazioni contenute nei suddetti Sistemi Informativi;
 - danneggiare, distruggere o alterare dati o programmi contenuti nei suddetti Sistemi Informativi;
 - alterare, in qualsiasi modo, il funzionamento del sistema informativo;
 - utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi.
- formare falsamente documenti societari aventi rilevanza esterna, mediante accesso ai sistemi e alterazione dei dati;
- distruggere, alterare, danneggiare informazioni, dati, programmi informatici della Società o della Pubblica Amministrazione, per ottenere vantaggi o condizioni favorevoli per l'azienda.
- porre in essere condotte miranti alla distruzione o all'alterazione dei documenti informatici aventi finalità probatoria in assenza di una specifica autorizzazione;
- utilizzare o installare programmi diversi da quelli autorizzati;
- aggirare o tentare di aggirare i meccanismi di sicurezza
- lasciare il proprio Personal Computer incustodito;
- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
- detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato.

Sono infine previste le seguenti regole nell'utilizzo e nella gestione dei sistemi informativi:

- deve essere assicurata una corretta gestione degli utenti di amministrazione, con la finalità di impedire l'utilizzo di tali credenziali a personale non autorizzato;
- devono essere assicurati il corretto mantenimento e l'integrità dei file di log generati dai sistemi;
- deve essere assicurata un'adeguata manutenzione/aggiornamento periodico delle credenziali utente al fine di prevenire eventuali erronee abilitazioni ai sistemi applicativi. A tal fine devono essere osservate, con riferimento ai diversi applicativi della Fondazione, le regole atte ad assicurare l'aggiornamento delle password dei singoli utenti;
- la navigazione in Internet e l'utilizzo della posta elettronica attraverso i Sistemi Informatici deve avvenire esclusivamente per lo svolgimento della propria attività lavorativa;
- non è consentito l'accesso alle aree riservate (quali server rooms, locali tecnici, ecc.) alle persone che non dispongono di idonea autorizzazione, temporanea o permanente;
- deve essere garantita la sicurezza fisica dell'infrastruttura tecnologica della Società, anche mediante monitoraggio delle attività di gestione e manutenzione sulla stessa.
- Nell'ambito delle attività svolte, i fornitori terzi devono rispettare i principi di comportamento e le regole indicate nella presente Parte Speciale al fine di tutelare la sicurezza dei dati ed il corretto utilizzo dei sistemi informativi.

Il Responsabile Interno:

- diviene il soggetto referente e responsabile delle attività a rischio;
- garantisce, nell'ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- collabora con l'OdV nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- comunica tempestivamente all'OdV eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello;

4. Flussi informativi verso l'OdV

Ciascun utente è tenuto a segnalare al Responsabile interno designato ogni violazione, tentativo o sospetto di violazione, nonché qualsiasi malfunzionamento del sistema informatico.

Il Responsabile Interno effettua i controlli nelle aree a rischio individuate e segnala tempestivamente all'OdV qualsiasi anomalia dovesse riscontrare e ogni modifica apportata al regolamento aziendale sull'utilizzo dei sistemi informativi.

La rete informatica aziendale è periodicamente sottoposta ad attività di controllo, amministrazione e back – up finalizzate alla rimozione di ogni file o applicazione ritenuti pericolosi per la sicurezza o non inerenti all'attività lavorativa sia sui PC dei lavoratori, sia sulla rete aziendale.

Il Responsabile segnala altresì periodicamente la necessità di sottoporre l'intero sistema informatico aziendale a check-up da parte di società specializzate.

Sezione “E”: art. 25 undecies D. Lgs. 231/01

Reati ambientali

Tra i reati ambientali previsti dal Decreto⁷ all’art. 25 undecies quelli che possono astrattamente configurarsi nella realtà della Fondazione sono solo quelli legati ai rifiuti prodotti negli uffici (toner per stampanti e fotocopiatrici esausti e RAEE – rifiuti da apparecchiature elettriche ed elettroniche), pertanto la Sezione è incentrata sulla descrizione dei soli reati inerenti alla gestione e smaltimento dei rifiuti e non contempla i reati inerenti a scarichi industriali, discariche, autorizzazioni ambientali, emissioni in atmosfera.

1. Reati inerenti alla gestione dei rifiuti

Attività di gestione dei rifiuti non autorizzata (art. 256 TUA)

La fattispecie punisce chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti (pericolosi e non) in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212, 214, 215 e 216. Le stesse pene si applicano ai «titolari di imprese e i responsabili di enti che abbandonano o depositano in modo incontrollato i rifiuti ovvero li immettono nelle acque superficiali o sotterranee in violazione del divieto di cui all’articolo 192, commi 1 e 2.» ; Chiunque realizza

7 Violazione articoli Testo Unico Ambientale:

- Scarico di acque reflue industriali contenenti sostanze pericolose in violazione alle prescrizioni contenute nell’autorizzazione allo scarico (art. 137 co. 3°)
- Scarico nelle acque del mare da parte di navi o aeromobili di sostanze o materiali vietati da Convenzioni internazionali ratificate e vigenti in Italia (art. 137 co. 13°)
- Attività di gestione di rifiuti non autorizzata e in particolare (art. 256)
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 co. 4°)
- Traffico illecito di rifiuti (Art. 259 co. 1°)
- Gestione degli impianti che generano emissioni in atmosfera in violazione ai valori limite e alle prescrizioni (art. 279)
- Bonifica dei siti (art. 257)
- Sistema informatico di controllo della tracciabilità dei rifiuti (art. 260 – bis)
- Apertura o effettuazione di nuovi scarichi di acque reflue industriali contenenti sostanze pericolose senza autorizzazione o in seguito a sospensione o revoca dell’autorizzazione (art. 137 co. 2°)
- Scarico di acque reflue industriali in violazione dei valori limite fissati per le sostanze contenute nella tabella 3/A dell’Allegato 5 (art. 137 co. 5°)
- Scarichi sul suolo, nel sottosuolo e nelle acque sotterranee in violazione agli art. 103 e 104 (art. 137 co. 11°)
- Attività di gestione di rifiuti non autorizzata e in particolare: in caso di condanna per realizzazione discarica abusiva (Art. 256, co 3°, secondo periodo)
- Attività organizzate per il traffico illecito di rifiuti (Art. 260)
- Attività organizzate per il traffico illecito di rifiuti (Art. 260)

Violazione articoli Codice Penale:

- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727 – bis)
 - Distruzione o deterioramento di habitat all’interno di un sito protetto (art. 733 – bis)
 - Inquinamento ambientale (art. 452 bis)
 - Disastro ambientale (art. 452 quater)
 - Delitti colposi contro l’ambiente (art. 452 quinquies)
 - Traffico e abbandono di materiale ad alta radioattività (art. 452 sexies)
 - Circostanze aggravanti (art. 452 octies)
- Reati previsti dalla l. 150/1992 sul commercio internazionale delle specie animali e vegetali in via di estinzione

Reati previsti dall’art. 3 della legge 549/1993 sulle misure a tutela dell’ozono stratosferico e dell’ambiente.

D. Lgs. 202/07 art. 8 - Inquinamento doloso art. 9 - Inquinamento colposo

o gestisce una discarica non autorizzata di rifiuti pericolosi e non; Chiunque non osservi le prescrizioni contenute o richiamate nelle autorizzazioni o non abbia i requisiti o le condizioni richiesti per le iscrizioni o comunicazioni; Chiunque, in violazione del divieto di cui all'articolo 187, effettua attività non consentite di miscelazione di rifiuti; Chiunque viola gli obblighi di cui agli articoli 231 (Veicoli fuori uso non disciplinati dal decreto legislativo 24 giugno 2003, n. 209), co. 7, 8 e 9, 233 (Consorzio nazionale di raccolta e trattamento degli oli e dei grassi vegetali ed animali esausti), co. 12 e 13, e 234 (Consorzio nazionali per il riciclaggio di rifiuti di beni in polietilene), co. 14.

Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 co.4 TUA) ovvero del Sistema Informatico di Controllo della tracciabilità dei rifiuti (art. 260 bis co. 6 TUA)

La prima fattispecie punisce: “le imprese che raccolgono e trasportano i propri rifiuti non pericolosi di cui all’articolo 212, comma 8, che non aderiscono, su base volontaria, al sistema di controllo della tracciabilità dei rifiuti (SISTRI) di cui all’articolo 188-bis, comma 2, lettera a), ed effettuano il trasporto di rifiuti senza il formulario di cui all’articolo 193 ovvero indicano nel formulario stesso dati incompleti o inesatti sono puniti con la sanzione amministrativa pecuniaria da milleseicento euro a novemila trecento euro. Si applica la pena di cui all’articolo 483 del codice penale a chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi fa uso di un certificato falso durante il trasporto. La seconda punisce: “ Colui che nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell’ambito del sistema di controllo della tracciabilità dei rifiuti fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico fisiche dei rifiuti e a chi inserisce un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti. Il trasportatore che omette di accompagnare il trasporto dei rifiuti (pericolosi e non) con la copia cartacea della scheda SISTRI- Area movimentazione e, ove necessario sulla base della normativa vigente, con la copia del certificato analitico che identifica le caratteristiche dei rifiuti; o che fa uso, durante il trasporto, di un certificato di analisi dei rifiuti contenente false indicazioni sulla natura, composizione e sulle caratteristiche chimico fisiche dei rifiuti trasportati. Il trasportatore che accompagna il trasporto dei rifiuti con una copia cartacea della scheda SISTRI- area movimentazione fraudolentemente alterata”.

Traffico illecito di rifiuti (art. 259 co. 1 TUA) e Attività organizzate per il traffico illecito di rifiuti (art. 260 TUA)

La prima fattispecie punisce: *Chiunque effettua una spedizione di rifiuti costituente traffico illecito ai sensi dell’art. 26 Reg. CEE 1 febbraio 1993, n. 259.* La seconda punisce: *Chiunque, al fine di perseguire un ingiusto profitto, con più operazioni e attraverso l’allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantità di rifiuti.*

2. Ruoli e responsabilità a presidio

In considerazione della irrilevanza dell’attività svolta dal punto di vista dell’impatto ambientale non è stato designato alcun responsabile diretto salvo il responsabile per gli adempimenti sulla tracciabilità dei rifiuti. Tutti i dipendenti sono comunque individualmente responsabili dello svolgimento delle attività in conformità ed esercitano un’attività di reciproca vigilanza che li impegna a riferire all’OdV su ogni comportamento tale da esporre la società ai reati ex D. Lgs. 231/01.

3. Aree sensibili e protocolli di prevenzione

Come premesso, l’area sensibile che potrebbe teoricamente esporre la società ai rischi reati è la sola gestione dei rifiuti costituiti da toner per stampanti, fax e fotocopie e dai RAEE. In conformità a quanto prescritto dal TUA in materia di responsabilità del produttore di rifiuti, per lo smaltimento dei propri rifiuti la Fondazione dovrà rivolgersi a soggetti autorizzati al ritiro e al trasporto presso smaltitore autorizzato.

Il responsabile operativo dovrà verificare il possesso delle autorizzazioni dei soggetti coinvolti nel trasporto e nello smaltimento e garantire la tracciabilità dei rifiuti consegnati mediante l’archiviazione della documentazione di legge (Formulario di identificazione dei rifiuti rilasciato dal trasportatore).

In merito alla gestione dei RAEE (i rifiuti rappresentati da apparecchiature elettriche ed elettroniche fuori uso), in conformità a quanto prescritto dal d. lgs. 151/2005 la Fondazione dispone il loro ritiro tramite consegna ai produttori o a terzi autorizzati, che provvedono all’invio ai centri di trattamento.

Sezione “F”: art. 25 decies

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria

1. Reati

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria (art. 377-bis c. p.)

L’art. 377-bis c.p. punisce il fatto di chi induce (mediante violenza o minaccia o con l’offerta o la promessa di danaro o altra utilità) a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere dichiarazioni utilizzabili in un procedimento penale, quando tale soggetto ha la facoltà di non rispondere. La condotta di induzione a non rendere dichiarazioni (cioè di avvalersi della facoltà di non rispondere ovvero di rendere dichiarazioni false) deve essere realizzata in modo tipico (o mediante violenza o minaccia, ovvero con l’offerta di danaro o di qualunque altra utilità).

Il soggetto passivo è necessariamente un soggetto al quale la legge attribuisca la facoltà di non rispondere: l’indagato (o l’imputato) di reato connesso o collegato (sempre che gli stessi non abbiano già assunto l’ufficio di testimone), nonché a quella ristretta categoria di testimoni (i prossimi congiunti), cui l’art. 199 c.p.p. conferisce la facoltà di astenersi dal testimoniare. E’ ipotizzabile il caso di un dipendente imputato o indagato che venga indotto a rendere false dichiarazioni (o ad astenersi dal renderle) per evitare un maggior coinvolgimento della responsabilità risarcitoria dell’ente stesso collegata al procedimento penale nel quale il dipendente è coinvolto.

2. Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate l’attività ritenuta più specificamente a rischio è la gestione dei contenziosi giudiziali e in particolare la gestione dei rapporti con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale.

3. Principi di comportamento

E’ fatto divieto a carico di tutti i Destinatari di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- prendere contatti con dipendenti o terzi coinvolti in procedimenti penali, allo scopo di indurli a rendere dichiarazioni atte ad evitare l’eventuale rischio di un coinvolgimento della società;
- porre in essere atti di minaccia o altre forme analoghe di coartazione ovvero di dare o promettere elargizioni in danaro o altre forme di utilità affinché il soggetto (dipendente o terzo) coinvolto in un procedimento penale non presti una fattiva collaborazione al fine di rendere dichiarazioni veritiere, trasparenti e correttamente rappresentative dei fatti o non esprima liberamente le proprie rappresentazioni dei fatti, esercitando la propria facoltà di non rispondere attribuita dalla legge, in virtù delle suddette forme di condizionamento.

In particolare, nel corso di procedimenti giudiziari, è fatto divieto di:

- elargire somme di denaro ai soggetti coinvolti quali testimoni nel procedimento penale;
- offrire omaggi e regali alle figure coinvolte come testimoni in un procedimento penale o a loro familiari, o a conferire loro qualsiasi forma di utilità che possa influenzare la testimonianza o impedirla, ostacolarla o indurre a false dichiarazioni in fase di dibattimento per assicurare un qualsivoglia vantaggio per l’azienda;
- accordare altri vantaggi di qualsiasi natura (promesse di assunzione, promozione, ecc.) alle persone coinvolte quali testimoni in un procedimento penale, o loro familiari;
- effettuare alle persone coinvolte quali testimoni in un procedimento penale qualsiasi tipo di pagamento in contanti o in natura.

Sezione "G": art. 25 nonies D. Lgs. 231/01

Delitti in materia di violazioni del diritto di autore

1. Le tipologie dei Delitti in materia di violazioni del diritto di autore (art. 25-novies del decreto)

Per quanto concerne la presente Sezione, si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 25-novies del Decreto, e suddivisi tra: reati potenzialmente realizzabili e reati che, per quanto non si possano escludere *tout court*, sono stati ritenuti remoti in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente coperti dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico adottato dalla Società.

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

Immissione su sistemi di reti telematiche a disposizione del pubblico, mediante connessioni di qualsiasi genere, di opere dell'ingegno protette o parte di esse (art. 171, primo comma, lett. a-bis) Legge 633/41); Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, terzo comma Legge 633/41)

Punisce la condotta di messa a disposizione del pubblico, tramite l'immissione di un sistema di reti telematiche e mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o parte di essa. Altresì, la pena è aggravata se i reati di cui sopra sono commessi su di un'opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Tale norma tutela l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere frustrate le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete.

Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di un programma per elaboratori (art. 171-bis, Legge 633/41)

Punisce chi abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE); ovvero chi, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati.

Tale norma è posta a tutela penale del software e delle banche dati. Con il termine "software", si intendono i programmi per elaboratore, in qualsiasi forma espressi, purché originali, quale risultato della creazione intellettuale dell'autore; mentre con "banche dati", si intendono le raccolte di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo.

I reati la cui commissione è stata ritenuta remota, sono i seguenti:

Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o

drammatico – musicali, multimediali, anche se inserite in opere collettive o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita, cessione o importazione abusiva di oltre 50 copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di opere dell'ingegno protette (art. 171-ter, Legge 633/41)

Punisce chi a fini di lucro:

a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;

b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;

c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);

d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro

supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;

f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;

f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con

la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

g) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102 quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse;

h) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;

h-bis) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;

i) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;

l) promuove o organizza le attività illecite di cui sopra.

Tale norma è volta alla tutela di una numerosa serie di opere dell'ingegno, sia quelle destinate al circuito radiotelevisivo e cinematografico, ma anche opere musicali, letterarie, scientifiche o didattiche. Le condizioni di punibilità riguardano l'utilizzo non personale dell'opera dell'ingegno e il dolo specifico di lucro.

Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies, Legge 633/41)

Punisce i produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla

univoca identificazione dei supporti medesimi; ovvero chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.

La disposizione in esame è posta a tutela delle funzioni di controllo della SIAE, in un'ottica di tutela anticipata del diritto d'autore. Si tratta pertanto di un reato di ostacolo che si consuma con la mera violazione dell'obbligo di comunicazione.

Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzazione per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies, Legge 633/41)

Punisce chi, a fini fraudolenti, produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

2. Aree a rischio

In relazione ai reati e alle condotte criminose sopra esplicitate l'area di attività ritenuta più specificamente a rischio è la gestione del sistema informativo aziendale che comprende l'utilizzo, la gestione di software nell'ambito dei sistemi informativi e la gestione delle attività connesse all'implementazione, manutenzione e aggiornamento del sito internet e della rete telematica aziendale. Eventuali integrazioni delle suddette aree di attività a rischio potranno essere proposte dall'OdV in considerazione del verificarsi di fattori esterni (ad esempio legislativi: introduzione di nuove categorie di reati) o di fattori interni (ad esempio, modifiche organizzative o di business).

3. Destinatari della Parte Speciale e principi di comportamento

La presente Sezione ha la funzione di:

- fornire un elenco dei principi di comportamento cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

La Sezione prevede l'espresso divieto a carico di tutti i Destinatari di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-novies del d.lgs. 231/2001);

- connettere ai sistemi informatici della Società personal computer, periferiche o altre apparecchiature e/o installare software senza preventiva autorizzazione del soggetto aziendale responsabile;
- procedere ad installazioni di prodotti software e/o hardware in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi ed i regolamenti che disciplinano e tutelano il diritto d'autore;
- modificare la configurazione software o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale ovvero, in diversa ipotesi, se non previa espressa e debita autorizzazione;
- acquisire e/o utilizzare prodotti tutelati da diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;
- accedere abusivamente al sito internet della Società al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto ovvero allo scopo di immettere dati o contenuti multimediali (immagini, video, ecc.) in violazione della normativa sul diritto d'autore e dei principi di comportamento previsti nella presente Parte Speciale.

Inoltre la Società, al fine di evitare il verificarsi dei reati oggetto della presente Sezione, considerati in via potenziale applicabili alla Società, ha previsto le seguenti regole di comportamento che i Destinatari sono tenuti a rispettare e che potranno, ove opportuno, essere implementate in specifiche procedure:

- i dipendenti, gli stagisti e gli altri soggetti (es. collaboratori e consulenti) devono essere adeguatamente informati dell'importanza di utilizzare correttamente i software e banche dati in dotazione e di non inserire dati, immagini o altro materiale coperto dal diritto d'autore senza avere ottenuto le necessarie autorizzazioni dai propri superiori gerarchici;
- deve essere prevista un'attività di comunicazione e sensibilizzazione in favore dei dipendenti e collaboratori esterni al fine di diffondere una chiara consapevolezza sui rischi derivanti dall'utilizzo improprio delle risorse informatiche;
- gli utilizzatori dei sistemi informatici devono essere informati che i software per l'esercizio dell'attività di competenza sono protetti da leggi sul diritto d'autore ed in quanto tali ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;
- deve essere prevista, nei rapporti contrattuali con fornitori di servizi software e banche dati sviluppati in relazione alle specifiche esigenze della Fondazione, clausole di manleva volte a tenere indenne la Società da eventuali responsabilità in caso di condotte, poste in essere dagli stessi fornitori, che possano determinare violazione di qualsiasi diritto di proprietà intellettuale di terzi;
- devono essere vietati l'installazione e l'utilizzo non autorizzato di sistemi di file sharing;
- deve essere vietata l'installazione di qualsiasi tipologia di software applicativo non autorizzato ed in assenza di licenza d'uso;
- devono essere predisposti meccanismi di controllo, anche automatici, per il rispetto dei divieti di cui sopra.

4. Responsabile interno

Il Responsabile Interno:

- diviene il soggetto referente e responsabile delle attività a rischio;
- garantisce, nell'ambito delle aree a rischio di sua competenza, il rispetto dei principi di riferimento del Modello e la corretta attuazione del sistema dei controlli individuati;
- collabora con l'OdV nello svolgimento di ogni attività necessaria ai fini dell'espletamento delle funzioni di vigilanza e controllo;
- comunica tempestivamente all'OdV eventuali comportamenti rilevati non in linea con le regole di condotta adottate in aderenza ai principi del Modello;

Sezione “H”: art. 25 octies D. Lgs. 231/01

Reati di ricettazione, riciclaggio e impiego di denaro, beni e utilità di provenienza illecita

Di seguito in relazione al basso livello di rischio connesso all’attività aziendale e per sole finalità cognitive ed esplicative si riportano le fattispecie di reato richiamate dall’art. 25 octies del D. Lgs. 231/01 (riciclaggio, ricettazione e impiego di denaro, beni o utilità di provenienza illecita di cui agli artt. 648 bis e 648 ter del codice penale).

Non si analizza tra i reati previsti all’articolo quello di ricettazione (art. 648 c.p.) in quanto l’attività svolta dalla Società è avulsa dalla possibilità di una sua commissione.

Riciclaggio (art. 648 bis c.p.)

La fattispecie di reato punisce *chi, fuori dei casi di concorso nel reato, sostituisce denaro, beni o altre utilità provenienti dai delitti di rapina aggravata, di estorsione aggravata, di sequestro di persona a scopo di estorsione o dai delitti concernenti la produzione o il traffico di sostanze stupefacenti o psicotrope, con altro denaro, altri beni o altre utilità, ovvero ostacola l’identificazione della loro provenienza dai delitti suddetti.*

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

La fattispecie di reato punisce *chi, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648 bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti dai delitti di rapina aggravata, di estorsione aggravata, di sequestro di persona a scopo di estorsione o dai delitti concernenti la produzione o il traffico di sostanze stupefacenti o psicotrope;*

Il Decreto Antiriciclaggio (d. lgs. 231/07) ha individuato specifici soggetti (tra i quali banche, intermediari finanziari, professionisti ecc.) per il monitoraggio e gli adempimenti informativi connessi all’esercizio delle loro attività/ professioni, estendendo ai sensi del D. Lgs. 231/01 la responsabilità in capo alle società.

1. Aree sensibili e presidi

La Fondazione non rientra tra i soggetti destinatari del decreto e pertanto non è tenuta ad osservare gli obblighi di:

1. adeguata verifica della clientela (Titolo II Capo I del decreto antiriciclaggio)
2. conservazione e registrazione delle informazioni (Titolo II Capo II)
3. tenuta di un archivio unico informatico (Titolo II Capo II)
4. segnalazione di operazioni sospette (Titolo II Capo III)
5. formazione del personale (Titolo III).

Poiché i revisori sono soggetti destinatari degli obblighi sopra riportati, si ritiene adeguato anche il presidio relativo al rischio residuale di attività di riciclaggio con le altri controparti negoziali.

2. Segnalazioni del Collegio all’Organismo di Vigilanza

Qualsiasi notizia relativa a operazioni finanziarie sospette di riciclaggio (art. 648 bis c.p.) ovvero di impiego di danaro o beni di provenienza illecita (art. 648 ter c.p.) deve essere tempestivamente comunicata dal Collegio all’Organismo di Vigilanza.

SISTEMA DISCIPLINARE

Premessa

Il presente sistema disciplinare, adottato ai sensi art. 6, comma secondo, lett. e) D. Lgs. 231/01 deve ritenersi complementare e non alternativo al sistema disciplinare stabilito dallo stesso C.C.N.L. vigente ed applicabile alle diverse categorie di dipendenti in forza alla Società.

L'irrogazione di sanzioni disciplinari a fronte di violazioni del Modello 231 e del Codice Etico prescinde dall'eventuale instaurazione di un procedimento penale per la commissione di uno dei reati previsti dal Decreto.

Nessun procedimento disciplinare potrà essere archiviato, né alcuna sanzione disciplinare potrà essere irrogata, per violazione del Modello, senza preventiva informazione e parere dell'Organismo di Vigilanza.

1. Destinatari

Lavoratori subordinati

Il sistema disciplinare ha quali soggetti destinatari i soggetti legati alla società da un rapporto di subordinazione, tra i quali dirigenti, quadri, impiegati e operai.

In altri termini, il presente sistema sanzionatorio è inquadrato nel più ampio contesto del potere disciplinare del quale è titolare il datore di lavoro, ai sensi degli artt. 2106 c.c. e 7 della L. 300/70, sebbene il decreto stesso non contenga prescrizioni specifiche in merito alle sanzioni da adottare, limitandosi a prescrizioni di carattere generale.

Lavoratori parasubordinati

Il sistema disciplinare è destinato anche ai soggetti legati alla Società da contratti di lavoro "parasubordinato".

Dopo la soppressione del D. Lgs. 10.09.2003 n° 276, recante "Attuazione delle deleghe in materia di occupazione e mercato del lavoro" in via residuale il sistema disciplinare risulta applicabile alle collaborazioni coordinate e continuative e alla collaborazione permanente, per un solo committente, di un lavoratore autonomo.

Tali lavoratori non possono essere sottoposti al potere disciplinare della Società e alla conseguente irrogazione di sanzioni propriamente disciplinari.

Sarà opportuno, quindi, adottare con tali soggetti specifiche clausole contrattuali che impegnino gli stessi a non adottare atti e/o procedure che comportino violazioni del Codice Etico, nel rispetto della correttezza e buona fede nell'esecuzione del contratto di cui il Codice è parte integrante.

In tal modo, la Società potrà sanzionare il mancato rispetto dei principi contenuti nel Codice Etico, nonché delle norme e degli standard generali di comportamento indicati nel Modello, ai sensi degli artt. 2222 ss. c.c.

Lavoratori autonomi - collaboratori e consulenti

Il sistema disciplinare deve altresì avere, quali soggetti destinatari, i collaboratori esterni a vario titolo, nonché i soggetti esterni che operano nell'interesse della Società.

Anche in tal caso, al fine di evitare comportamenti non conformi, è opportuno che si concordino con i propri consulenti, collaboratori, specifiche clausole contrattuali che vincolino i soggetti terzi all'osservanza del Codice Etico e del Modello Organizzativo, come meglio specificato più avanti.

Altri destinatari

Sono soggetti a sanzioni anche gli amministratori, i sindaci e tutti i partners che a vario titolo intrattengono rapporti con la Società.

2. Criteri di applicazione delle sanzioni

Il tipo e l'entità delle sanzioni specifiche saranno applicate nei singoli casi in base ai criteri generali di seguito indicati ed in proporzione alla gravità delle mancanze, fermo restando, in ogni caso, che il comportamento sarà considerato illecito disciplinare qualora sia effettivamente idoneo a produrre danni alla Società.

I fattori rilevanti ai fini della irrogazione della sanzione sono:

- elemento soggettivo della condotta, a seconda del dolo o della colpa (negligenza, imprudenza, imperizia),

- rilevanza degli obblighi violati,
- entità del danno derivante alla Società o dall'eventuale applicazione delle sanzioni previste dal Decreto,
- livello di responsabilità gerarchica e/o tecnica,
- presenza di circostanze aggravanti o attenuanti con particolare riguardo alle precedenti prestazioni lavorative,
- eventuale condivisione di responsabilità con altri dipendenti che abbiano concorso nel determinare la mancanza,
- recidiva.

Nel caso in cui con un solo atto siano state commesse più infrazioni si applica la sanzione più grave.

3. Misure per i dipendenti

Per ogni rapporto di lavoro subordinato, oltre allo Statuto dei lavoratori (legge 300/1970) si fa riferimento alla normativa dei contratti collettivi di lavoro e alle norme del codice civile, tra cui gli artt. 2104, 2105 e 2106 che qui si riportano.

- Art. 2104 *Diligenza del prestatore di lavoro*. Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende.
- Art. 2105 *Obbligo di fedeltà*. Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad esso pregiudizio.
- Art. 2106 *Sanzioni disciplinari*. L'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo all'applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione (e in conformità delle norme corporative).

3.1 Tipologie di comportamenti sanzionabili dei dipendenti

Le sanzioni previste di seguito si applicano nei confronti di quadri, impiegati ed operai, alle dipendenze della Fondazione che pongano in essere illeciti disciplinari derivanti da:

- a) mancato rispetto delle misure dirette a garantire lo svolgimento dell'attività e/o a scoprire ed eliminare tempestivamente situazioni di rischio, ex D. Lgs. 231/01;
- b) inosservanza delle modalità e delle procedure formulate per l'acquisizione e gestione delle risorse finanziarie predisposte per la prevenzione di fattispecie di reati presupposto;
- c) mancata, incompleta o non veritiera rappresentazione dell'attività svolta relativamente alle modalità di documentazione, di conservazione e di controllo degli atti relativi alle procedure in modo da impedire la trasparenza e verificabilità delle stesse;
- d) violazione e/o elusione del sistema di controllo, poste in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione della procedura ovvero impedendo il controllo o l'accesso alle informazioni ed alla documentazione ai soggetti preposti, incluso l'Organismo di Vigilanza;
- e) inosservanza delle prescrizioni contenute nel Codice Etico;
- f) inosservanza delle disposizioni relative ai poteri di firma e del sistema delle deleghe, in relazione ai rischi connessi, con riguardo ad atti e documenti verso la Pubblica Amministrazione;
- g) inosservanza dell'obbligo di dichiarazioni periodiche (o falsità in dichiarazione) relative a: rispetto del Codice Etico e del Modello; assenza di conflitti di interessi, con riguardo a rapporti con la Pubblica Amministrazione;
- h) comportamenti di ostacolo o elusione ai controlli dell'Organismo di Vigilanza, impedimento ingiustificato dell'accesso ad informazioni ed alla documentazione nei confronti dei soggetti incaricati dei controlli;
- i) omissioni nell'osservanza, nell'attuazione e nel controllo o violazione delle norme di tutela della salute e sicurezza sul lavoro (D. Lgs. 81/08 e s.m.i.) che possono costituire fonte di reati presupposto;
- l) violazioni plurime ingiustificate e reiterate dei protocolli del Modello e della sua implementazione per il continuo aggiornamento;

- m) omessa segnalazione dell'inosservanza ed irregolarità commesse anche da soggetti apicali
- n) omessa informativa all'Organismo di Vigilanza e alle funzioni nonché all'organo dirigente di ogni situazione a rischio reato presupposto avvertita nello svolgimento delle attività.
- o) omessa vigilanza sul comportamento del personale operante all'interno della propria sfera di responsabilità al fine di verificarne le azioni nell'ambito delle aree a rischio reato e, comunque, nello svolgimento di attività strumentali a processi operativi a rischio reato.

3.2 Possibili sanzioni

Il mancato rispetto delle misure e delle procedure indicate nel Modello, a seconda della gravità dell'infrazione, è sanzionato con i seguenti provvedimenti disciplinari:

- a) richiamo verbale: verrà applicata la sanzione del richiamo verbale nei casi di violazione colposa dei principi del Codice Etico e/o di norme procedurali previste dal Modello o di errori procedurali, non aventi rilevanza esterna, dovuti a negligenza del lavoratore.
- b) ammonizione scritta: verrà applicata nei casi di:
 - violazione colposa di norme procedurali previste dal Modello o di errori procedurali, aventi rilevanza esterna, dovuti a negligenza del lavoratore;
 - recidiva nelle violazioni di cui al punto a), per cui è prevista la sanzione del richiamo verbale.
- c) multa per un importo fino a tre ore di retribuzione: oltre che nei casi di recidiva nella commissione di infrazioni da cui possa derivare l'applicazione del rimprovero scritto, la multa potrà essere applicata nei casi in cui, per il livello di responsabilità gerarchico o tecnico, o in presenza di circostanze aggravanti, il comportamento colposo e/o negligente possa minare, sia pure a livello potenziale, l'efficacia del Modello; quali a titolo esemplificativo ma non esaustivo:
 - l'inosservanza delle procedure previste dal Modello riguardanti un procedimento in cui una delle parti necessarie è la Pubblica Amministrazione;
 - reiterate violazioni di cui al precedente punto b), per cui è prevista la sanzione dell'ammonizione scritta;
- d) sospensione dal lavoro e dalla retribuzione fino a 3 giorni: verrà applicata, oltre che nei casi di recidiva nella commissione di infrazioni da cui possa derivare l'applicazione della multa, nei casi di gravi violazioni procedurali tali da esporre la Società a responsabilità nei confronti dei terzi.

A titolo esemplificativo ma non esaustivo si applica in caso di:

- inosservanza dell'obbligo delle dichiarazioni periodiche (o falsità in dichiarazione) relative al rispetto del Codice Etico e del Modello; delle dichiarazioni relative all'assenza di conflitti di interessi, con riguardo a rapporti con la Pubblica Amministrazione e delle attestazioni scritte richieste dalla procedura relativa al processo di bilancio;
- inosservanza delle disposizioni relative ai poteri di firma e del sistema delle deleghe, in relazione ai rischi connessi, con riguardo ad atti e documenti verso la P.A.;
- omessa vigilanza sul comportamento del personale operante all'interno della propria sfera di responsabilità al fine di verificare le loro azioni nell'ambito delle aree a rischio reato e, comunque, nello svolgimento di attività strumentali a processi operativi a rischio reato;
- reiterate violazioni di cui al precedente punto c).

Ove i dipendenti sopra indicati siano muniti di procura con potere di rappresentare all'esterno la Società, l'applicazione della sanzione descritta comporterà anche la revoca automatica della procura stessa.

e) licenziamento con preavviso: verrà applicata nei casi di reiterata grave violazione delle procedure aventi rilevanza esterna nello svolgimento di attività che implicano rapporti giudiziali, negoziali ed amministrativi con la P.A., nonché di reiterata inosservanza delle prescrizioni contenute nel Codice Etico e del Modello 231, di cui al precedente punto d).

f) licenziamento senza preavviso: verrà applicata per mancanze commesse dolosamente e così gravi da non consentire la prosecuzione anche provvisoria del rapporto di lavoro, quali a titolo esemplificativo, ma non esaustivo:

- violazione dolosa di procedure aventi rilevanza esterna e/o elusione fraudolenta realizzata attraverso un comportamento inequivocabilmente diretto alla commissione di un reato ricompreso fra quelli previsti dal Decreto tale da far venir meno il rapporto fiduciario con il datore di lavoro;

- violazione e/o elusione del sistema di controllo, poste in essere con dolo mediante la sottrazione, la distruzione o l'alterazione della documentazione della procedura ovvero impedendo il controllo o l'accesso alle informazioni ed alla documentazione ai soggetti preposti, incluso l'Organismo di Vigilanza;
- mancata, incompleta o non veritiera documentazione dell'attività svolta relativamente alle modalità di documentazione e di conservazione degli atti delle procedure, dolosamente diretta ad impedire la trasparenza e verificabilità delle stesse
- gravi inadempimenti degli obblighi di legge sulla sicurezza sul lavoro che potrebbero causare direttamente o indirettamente lesioni personali colpose gravi o gravissime o omicidio colposo, di cui all'art. 25 septies del Decreto.

In ogni caso, qualora il lavoratore sia incorso in una delle mancanze di cui al presente punto f) la Società potrà disporre, in attesa del completo accertamento delle violazioni, la sospensione cautelare non disciplinare del medesimo con effetto immediato per un periodo non superiore a 10 giorni.

Nel caso in cui la Società decida di procedere al licenziamento, lo stesso avrà effetto dal giorno in cui ha avuto inizio la sospensione cautelare.

* * * * *

Il datore di lavoro non potrà comminare alcuna sanzione al lavoratore senza avergli preventivamente contestato l'addebito e senza aver sentito la sua difesa.

La contestazione del datore di lavoro, salvo che per il richiamo verbale, dovrà essere effettuata per iscritto ed i provvedimenti disciplinari non potranno essere comminati prima che siano trascorsi 5 giorni, nel corso dei quali il lavoratore potrà presentare la sua difesa. Se entro ulteriori 5 giorni non viene adottato alcun provvedimento, si riterranno accolte le giustificazioni del lavoratore.

La difesa del lavoratore può essere effettuata anche verbalmente, anche con l'assistenza di un rappresentante dell'associazione sindacale cui aderisce. La comminazione del provvedimento dovrà essere motivata e comunicata per iscritto. I provvedimenti, fatta eccezione del richiamo verbale, possono essere impugnati dal lavoratore, in sede sindacale, secondo le norme contrattuali relative alle vertenze.

4. Misure per gli apicali

Dirigenti

Anche nei confronti dei dirigenti che attuino comportamenti in violazione delle prescrizioni del presente Modello, verranno adottate le misure più idonee in conformità a quanto previsto dal regolamento di disciplina dello Statuto dei Lavoratori. Tenuto conto della natura fiduciaria del rapporto di lavoro, il mancato rispetto delle disposizioni previste dal Modello e dal Codice Etico, è sanzionato considerando in sede applicativa del principio di proporzionalità previsto dall'art. 2106 del c.c. e valutando, per ciascuna fattispecie, la gravità oggettiva del fatto costituente infrazione disciplinare, il grado di colpa, l'eventuale reiterazione di un medesimo comportamento, nonché l'intenzionalità del comportamento stesso.

I provvedimenti disciplinari applicabili ai dirigenti sono quelli previsti dalle norme contrattuali collettive e dalle norme legislative in vigore per gli impiegati di massima categoria dipendenti dell'azienda cui il dirigente appartiene.

Il datore di lavoro non potrà comminare alcuna sanzione al lavoratore senza avergli preventivamente contestato l'addebito e senza aver sentito la sua difesa.

La contestazione del datore di lavoro, salvo che per il richiamo verbale, dovrà essere effettuata per iscritto ed i provvedimenti disciplinari non potranno essere comminati prima che siano trascorsi 5 giorni, nel corso dei quali il lavoratore potrà presentare la sua difesa. Se entro ulteriori 5 giorni non viene adottato alcun provvedimento, si riterranno accolte le giustificazioni del lavoratore.

La difesa del lavoratore può essere effettuata anche verbalmente, anche con l'assistenza di un rappresentante dell'associazione sindacale cui aderisce.

La comminazione del provvedimento dovrà essere motivata e comunicata per iscritto.

I provvedimenti, fatta eccezione del richiamo verbale, possono essere impugnati dal lavoratore, in sede sindacale, secondo le norme contrattuali relative alle vertenze.

Amministratori

In caso di violazione del modello da parte degli amministratori, l'Organismo di Vigilanza informerà tempestivamente l'intero Consiglio di Amministrazione, affinché ciascun consigliere, singolarmente, ovvero ciascun organo, nel suo complesso, a seconda delle rispettive competenze, provveda ad assumere le iniziative più opportune ed adeguate coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo statuto (dichiarazioni nei verbali delle adunanze, richiesta di convocazione/convocazione riunione di consiglio di amministrazione, richiesta convocazione/convocazione assemblee con all'ordine del giorno adeguati provvedimenti nei confronti dei soggetti responsabili della violazione, ecc.).

Si ricorda che a norma dell'art. 2392 c.c. gli amministratori sono responsabili verso la società per non aver adempiuto ai doveri imposti dalla legge con la dovuta diligenza. Pertanto in relazione al danno cagionato da specifici eventi pregiudizievoli strettamente riconducibili al mancato esercizio della dovuta diligenza, potrà correlarsi l'esercizio di un'azione di responsabilità sociale ex art. 2393 c.c. e seguenti a giudizio dell'Assemblea.

4.1 Tipologia di comportamenti sanzionabili degli apicali

Qui di seguito sono elencate alcune tipologie di comportamenti sanzionabili degli apicali:

1. inosservanza dei protocolli e dei procedimenti di programmazione della formazione delle decisioni dell'organo dirigente (consiglieri di amministrazione, amministratore unico, amministratore delegato, consiglieri di gestione) nello svolgimento delle proprie funzioni;
2. inosservanza delle procedure e dei processi di attuazione delle decisioni dell'organo dirigente nelle attività organizzative;
3. Inosservanza delle modalità e delle procedure formulate per l'acquisizione e gestione delle risorse finanziarie predisposte per la prevenzione dei reati
4. Inosservanza dell'obbligo di documentazione delle fasi decisionali previsto nei processi a rischio di reato individuati nel Modello
5. Omissione di comportamenti e di procedure prescritti e formulati nel Modello che espongono la società a rischi reato
6. Omissioni di osservanza di norme e di condotte cogenti previste da leggi nazionali ed europee, che dispongono regole di organizzazione e prevenzione, dirette in modo univoco al compimento dei reati presupposto previsti dal Decreto
7. Comportamenti di ostacolo o elusione dei controlli dell'OdV, impedimento ingiustificato dell'accesso ad informazioni e alla documentazione nei confronti dei soggetti incaricati dei controlli
8. Omissione nell'osservanza, nell'attuazione e nel controllo o violazione delle norme di tutela della salute e sicurezza sul lavoro (D. Lgs. 81/08 e s.m.i.) che possono costituire fonte dei reati presupposto
9. Violazioni plurime ingiustificate e reiterate dei protocolli del Modello e della sua implementazione per il continuo adeguamento;
10. Omessa segnalazione di inosservanze ed irregolarità commesse anche da soggetti apicali;
11. Omessa valutazione e tempestiva presa di provvedimenti in merito alle segnalazioni e richiami per interventi evidenziati dall'Organismo di Vigilanza nelle attività di competenza dei soggetti apicali.

4.2 Possibili sanzioni

I provvedimenti disciplinari che possono essere intrapresi nei confronti degli apicali in caso di adozione di comportamenti della fattispecie di cui al paragrafo precedente sono:

- richiamo e intimazione a conformarsi
- sospensione se le infrazioni sono gravi e reiterate
- revoca se si verifica una reiterazione dopo la sospensione
- revoca se si realizza il reato presupposto

La valutazione e la scelta sul tipo di sanzione da irrogare tra quelle possibili previste dovrà tenere conto della gravità e

reiterazione delle condotte.

La reiterazione nel tempo di azioni, omissioni e condotte del par. 4.1 costituisce sintomo di maggiore gravità delle violazioni.

5. Misure nei confronti dei lavoratori autonomi

L'inosservanza delle prescrizioni contenute nel Modello e nel Codice Etico da parte di ciascun lavoratore autonomo può determinare, in conformità a quanto disciplinato nello specifico rapporto contrattuale, la risoluzione del relativo contratto, fermo restando la facoltà di richiedere il risarcimento dei danni verificatisi in conseguenza di detti comportamenti, inclusi i danni causati dall'applicazione da parte del giudice delle misure previste dal Decreto.

In particolare, si renderà necessaria l'utilizzazione di un'apposita clausola contrattuale, del tipo che segue, e che formerà oggetto di espressa accettazione da parte del terzo contraente e, quindi, parte integrante degli accordi contrattuali.

Con questa clausola, tali collaboratori dichiareranno di essere a conoscenza, di accettare e di impegnarsi a rispettare il Codice Etico ed il Modello Organizzativo adottati dalla Società, di aver eventualmente adottato anch'essi un analogo codice etico e Modello Organizzativo e Gestionale e di non essere mai stati implicati in procedimenti giudiziari relativi ai reati contemplati nel Modello Organizzativo e di cui al D. Lgs. 231/2001.

Nel caso in cui tali soggetti siano stati implicati nei procedimenti di cui sopra, dovranno dichiararlo ai fini di una maggiore attenzione da parte della società, qualora si addivenga all'instaurazione del rapporto.

La clausola anzidetta, potrà avere il seguente tenore letterale:

"Le parti contraenti dichiarano di non essere a conoscenza di fatti e/o atti rilevanti ai sensi degli artt. 24, 25 e ss. e 26 del D. Lgs. 231/2001, nella fase delle trattative, nonché nella stipulazione del presente contratto.

Il Collaboratore/Consulente si impegna, oltre a ciò, a rispettare il Codice etico allegato al presente contratto di cui costituisce parte integrante ed essenziale, a vigilare sull'esecuzione del contratto, nonché ad attivare idonee procedure interne al fine di ridurre e, ove occorrer possa, eliminare il rischio di commissione dei reati di cui al D. Lgs. 231/2001".

Nel rispetto della correttezza e buona fede nell'esecuzione del contratto, fatta salva la disciplina di legge, la Società, in caso di violazione di una raccomandazione da parte di un collaboratore o consulente, potrà:

- a) contestare l'inadempimento al destinatario con la contestuale richiesta di adempimento degli obblighi contrattualmente assunti e previsti dal presente Codice di Comportamento, se del caso, concedendo un termine ovvero immediatamente, nonché
- b) richiedere un risarcimento del danno pari al corrispettivo percepito per l'attività svolta nel periodo decorrente dalla data dell'accertamento della violazione della raccomandazione all'effettivo adempimento.

Fatta salva la disciplina di legge, in caso di violazione di n° 3 (tre) divieti contenuti nel Codice Etico o nel Modello, la Società potrà:

- c) risolvere automaticamente il contratto in essere per grave inadempimento, ex art. 1453 c.c. nonché
- d) richiedere un risarcimento del danno pari al corrispettivo percepito per l'attività svolta nel periodo decorrente dalla data dell'accertamento della terza violazione di raccomandazione o della violazione del divieto alla data di comunicazione della risoluzione.

5.1 Tipologia di comportamenti sanzionabili dei lavoratori autonomi

Possibili comportamenti sanzionabili dei lavoratori autonomi sono:

1. inosservanza delle procedure e dei processi di attuazione delle decisioni dell'organo dirigente nelle attività organizzative;
2. Inosservanza delle modalità e delle procedure formulate per l'acquisizione e gestione delle risorse finanziarie predisposte per la prevenzione dei reati
3. Inosservanza dell'obbligo di documentazione delle fasi decisionali previsto nei processi a rischio di reato individuati nel Modello
4. Omissione di comportamenti e di procedure prescritti e formulati nel Modello che espongono la società a rischi reato Omissione nell'osservanza, nell'attuazione e nel controllo o violazione delle norme di tutela della salute e sicurezza sul lavoro (D. Lgs. 81/08 e s.m.i.) che possono costituire fonte dei reati presupposto

5. Violazioni plurime ingiustificate e reiterate dei protocolli del Modello e della sua implementazione per il continuo adeguamento;
6. Omessa segnalazione di inosservanze ed irregolarità commesse anche da soggetti apicali;
7. Omessa valutazione e tempestiva presa di provvedimenti in merito alle segnalazioni e richiami per interventi evidenziati dall'Organismo di Vigilanza nelle attività di competenza dei soggetti apicali.

5.2 Possibili sanzioni

Le possibili sanzioni che possono essere previste nei confronti dei lavoratori autonomi in caso di adozione di comportamenti della fattispecie di cui al paragrafo precedente, da prevedere anche in seno ai singoli contratti sono:

1. Richiamo e intimazione a conformarsi
2. Comminazione di una penale ex. art. 1382 c.c.
3. Risoluzione ex. art. 1456 c.c. nei casi più gravi in ipotesi di realizzazione del reato presupposto
4. Revoca se si verifica una reiterazione dopo la sospensione
5. Revoca se si realizza il reato presupposto

La valutazione e la scelta sul tipo di sanzione da irrogare tra quelle possibili previste dovrà tenere conto della gravità e reiterazione delle condotte.

La reiterazione nel tempo di azioni, omissioni e condotte del par. 5.1 costituisce sintomo di maggiore gravità delle violazioni.