Modello di Organizzazione, Controllo e Gestione ai sensi del D.Lgs. n. 231 del 8 giugno 2001

Approvato con delibera del CdA
In data 12 dicembre 2013

INDICE

"L'Azienda"

"L'Azienda" – Breve sintesi dell'attività di ENERCOM

ENERCOM S.r.l. (nel seguito ENERCOM) si occupa di vendita di gas ed energia elettrica. Insieme alla capogruppo G.E.I. Gestione Energetica Impianti S.p.A. e a Omnia Servizi S.r.l. fa parte del Gruppo ENERGEI, la cui storia aziendale ha inizio nel 1921 con la cessione dei diritti di distribuzione, illuminazione e produzione di gas da parte della Anonima Gasometri Riuniti di Roma. La sede è a Crema, in via S. Chiara n. 9.

ENERCOM, nata nel 2002 dalla scissione del ramo d'azienda imposta dal D.Lgs. n. 164/2000 di liberalizzazione del settore gas, svolge essenzialmente attività di commercializzazione di gas naturale ed energia elettrica in regime di mercato, libero e tutelato, per gli utenti finali in un'ampia area di Piemonte, Lombardia e Veneto. In quest'ottica ha continui rapporti con i clienti (civili e industriali) e con i fornitori della materia prima (soprattutto traders). Nell'espletamento delle proprie attività ENERCOM è soggetta ad attività di controllo da parte di Enti Fiscali ed di Enti preposti al controllo sulla regolarità di trattamento delle risorse umane e da parte di altri Enti Pubblici tra cui in particolare, per suo stesso scopo istitutivo, l'Autorità per l'Energia Elettrica ed il Gas (AEEG).

L'attività di vendita nel suo complesso è costituita da numerosi processi produttivi, che si sviluppano in particolare nelle aree commerciale, gestionale ed amministrativa.

Tutti i processi, eccetto quelli amministrativi/contabili in quanto regolati dalle norme in materia, sono stati individuati e procedurizzati nel Sistema di Qualità Aziendale di cui si è dotata la società, conseguendo altresì la Certificazione UNI EN ISO 9001:2008. Alla base del suddetto Sistema è l'Organigramma Aziendale (Organigramma Funzionale negli Allegati), che è tenuto aggiornato e individua le dipendenze funzionali, coerentemente con quelle gerarchiche, di tutta la struttura aziendale esplicitata nelle proprie funzioni e servizi, alcuni dei quali affidati in outsourcing a società del medesimo gruppo.

La documentazione, che regolamenta la vita dell'Azienda, è alla base del presente Modello Organizzativo, più specificatamente finalizzato a prevenire i reati di cui al D.Lgs. 231/2001 e che ha lo scopo di individuare le *"aree a rischio reato"*, per integrare il sistema gestionale con procedure mirate alla loro prevenzione.

Parte generale 1

PRINCIPI GENERALI

LA RESPONSABILITÀ AMMINISTRATIVA DELLE PERSONE GIURIDICHE

Il Decreto Legislativo n. 231 dell'8 giugno 2001, che introduce la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*" (di seguito il "Decreto"), ha adeguato la normativa italiana in materia di responsabilità delle persone giuridiche, di cui – sino all'adozione del Decreto – nel nostro ordinamento si era sempre negata qualsiasi responsabilità in relazione ai reati commessi dai dirigenti e dipendenti delle medesime.

A tal proposito si precisa che i reati sono condotte che per il loro particolare disvalore sociale sono ritenute dal legislatore punibili penalmente, ovvero soggette a sanzione penale. La responsabilità penale si caratterizza per il fatto di essere punita, oltre che con sanzioni pecuniarie quali l'ammenda e la multa, anche con sanzioni quali l'arresto e la reclusione, ovvero la detenzione o privazione della libertà personale del reo. È tuttavia ovvio che quest'ultima tipologia di sanzioni non possa essere applicata alle persone giuridiche, ragion per cui nell'ordinamento italiano, prima del Decreto, non era prevista alcuna forma di responsabilità penale delle medesime, a differenza di molti paesi esteri.
Per adeguare il nostro ordinamento al panorama giuridico internazionale, il Decreto ha introdotto nell'ordinamento italiano un regime di responsabilità amministrativa (equiparabile sostanzialmente alla responsabilità penale), a carico delle persone giuridiche (di seguito denominate Enti), che va ad aggiungersi alla responsabilità della persona fisica che ha realizzato materialmente i reati e che mira a coinvolgere, nella punizione degli stessi, gli Enti nel cui interesse o vantaggio tali reati siano stati compiuti. Lo scopo della normativa è quello di ampliare la responsabilità per la commissione di taluni illeciti penali coinvolgendo nella punizione degli stessi il patrimonio degli enti e, in definitiva, gli interessi economici dei soci, i quali, fino all'entrata in vigore del decreto in esame, non pativano conseguenze dalla realizzazione di reati commessi, con vantaggio della società, da amministratori e/o dipendenti, se non l'eventuale risarcimento del danno, se ed in quanto esistente.
La società e i suoi soci vengono dunque coinvolti nel procedimento penale per reati commessi a vantaggio o nell'interesse dell'ente. Il che, ovviamente, determina un interesse dei soci, che partecipano alle vicende patrimoniali dell'ente, al controllo della regolarità e della legalità dell'operato sociale.
Questa responsabilità della società sorge peraltro con riferimento non a tutti i reati previsti dalla legge, ma soltanto in occasione della realizzazione di determinati tipi di reati – indicati dal decreto stesso – da parte di soggetti legati a vario titolo all'ente e solo allorquando la condotta illecita sia stata realizzata nell'*interesse* o *a vantaggio* di esso. È bene precisare che la responsabilità della società sorge non soltanto allorché il comportamento illecito abbia determinato un vantaggio, patrimoniale o meno, per la società, ma anche nell'ipotesi in cui, pur in assenza di tale concreto risultato, il fatto-reato trovi ragione nell'*interesse* della stessa.

I soggetti che, commettendo un reato nell'interesse o a vantaggio della società, ne possono determinare la responsabilità, possono in particolare essere:

1. persone poste all'interno della società in posizioni apicali, ovvero che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;
2. persone sottoposte alla direzione o vigilanza da parte di uno dei soggetti sopraindicati.

SANZIONI PREVISTE DAL DECRETO

Le tipologie di sanzioni previste a carico della società per gli illeciti amministrativi dipendenti da reato previsti dal Decreto sono:

- Sanzioni amministrative
- Sanzioni amministrative pecuniarie
- Sanzioni interdittive
- Confisca
- Pubblicazione della sentenza

In particolare le principali sanzioni interdittive consistono in:

- interdizione dall'esercizio dell'attività
- divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito
- esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o la revoca di quelli eventualmente già concessi
- divieto di pubblicizzare beni o servizi

AZIONI DI ESONERO DALLA RESPONSABILITÀ AMMINISTRATIVA

Gli artt. 6 e 7 del Decreto prevedono tuttavia che la società non risponde per i reati commessi nell'interesse o a vantaggio della società sia da soggetti apicali sia da dipendenti se è in grado di dimostrare al giudice, in sede di procedimento penale per uno dei reati considerati a carico dell'autore materiale del fatto illecito, di aver **adottato ed efficacemente attuato modelli di organizzazione, gestione e controllo idonei a prevenire la realizzazione degli illeciti penali** considerati.

Nel caso di reati commessi da soggetti in posizione apicale l'art. 6 prevede l'esonero qualora la società stessa dimostri che:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli d'organizzazione, controllo e gestione idonei a prevenire reati della specie di quello verificatosi (di seguito anche "**Modello 231**");

b) il compito di vigilare sul funzionamento e l'osservanza dei modelli, di curare il loro aggiornamento è stato affidato a un organo dell'ente appositamente costituito, **l'Organismo di Vigilanza** (di seguito anche "OdV"), dotato di autonomi poteri di iniziativa e di controllo;

c) le persone hanno commesso il reato eludendo fraudolentemente i modelli d'organizzazione e di gestione;

d) non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Per quanto concerne i dipendenti, l'art. 7 prevede l'esonero nel caso in cui l'ente ha adottato ed efficacemente attuato prima della commissione del reato un modello d'organizzazione gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

Più precisamente, l'art. 6, co. 1, lett. c) del Decreto richiede, **ai fini dell'esclusione della responsabilità** amministrativa della società, che **le persone abbiano "*commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione*"**, ovvero che lo stesso reato sia realmente voluto dall'agente sia come condotta che come evento.

Un'eccezione a tale requisito della fraudolenza è peraltro costituita dai casi di reati di omicidio colposo e lesioni personali colpose commessi con violazione delle norme in materia di salute e sicurezza sul lavoro (per i quali si rimanda all'apposito capitolo della parte speciale).

Il sistema prevede quale presupposto indispensabile al fine dell'esonero da responsabilità anche l'istituzione di un apposito organo di controllo interno all'ente dotato di autonomi poteri di iniziativa e controllo, il cosiddetto Organismo di Vigilanza, con il compito di vigilare sull'efficacia reale ovvero sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento.

A tal proposito è però opportuno precisare che il massimo vertice societario, vale a dire il Consiglio di Amministrazione, pur con l'istituzione dell'OdV, mantiene invariate tutte le sue attribuzioni e responsabilità previste dal Codice Civile, alle quali si aggiunge oggi quella relativa all'adozione ed all'efficacia del Modello, nonché all'istituzione dell'Organismo (art. 6, co. 1, lett. a) e b)).

Il Decreto prevede, inoltre, che il Modello 231, debba rispondere alle seguenti esigenze:

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

Il modello di organizzazione, gestione e controllo consiste dunque in un tipico sistema di gestione dei rischi (*risk management*), il quale, da un lato, identifica i rischi (si rimanda all'apposito allegato sull'analisi del rischio), ovvero analizza il contesto aziendale per evidenziare dove (in quale area/settore di attività) e secondo quali modalità si possono verificare eventi pregiudizievoli per gli obiettivi indicati dal D.Lgs. n. 231/01, e, dall'altro, disegna il sistema di controllo, ovvero prevede un insieme di protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente per prevenire quegli stessi reati.
Ciò richiede che il sistema operante all'interno della società sia valutato ed eventualmente adeguato con riguardo alla sua capacità di contrastare efficacemente, cioè ridurre ad un livello accettabile, i rischi ritenuti rilevanti.
L'eliminazione o riduzione del rischio può essere effettuata intervenendo (congiuntamente o disgiuntamente) sulla probabilità di accadimento dell'evento e/o sull'impatto dell'evento stesso.

Il detto sistema, per risultare efficacie, deve peraltro operare con costanza e continuità o quantomeno con una periodicità adeguata e in particolare allorché si verificano cambiamenti della struttura e dell'organizzazione aziendale (apertura di nuove sedi, ampliamento di attività, acquisizioni, riorganizzazioni, ecc.).

Fondamentale affinché il modello organizzativo possa essere idoneo a prevenire i reati di origine sia dolosa che colposa previsti dal D.Lgs. n. 231/01 è che le attività che comportano un rischio di reato siano procedimentalizzate al fine di evitare la commissione di reati.

Una volta attuato il modello, gli stessi reati potranno comunque essere commessi ma, laddove si tratti di reati dolosi, soltanto se dall'agente siano realmente voluti, sia come condotta che come evento. In tal caso, infatti, l'agente, per poter commettere il reato, non solo dovrà "volere" l'evento reato (ad esempio corrompere un pubblico funzionario) ma potrà attuare il suo proposito criminoso soltanto aggirando e forzando

fraudolentemente (ad esempio attraverso artifizi e/o raggiri) le indicazioni e le procedure della società contenute nel modello e nei relativi protocolli.
Per quanto riguarda, invece, i reati colposi (omicidio colposo e lesioni personali colpose gravi o gravissime commessi con violazione delle norme in materia di salute e sicurezza sul lavoro), gli stessi devono essere voluti dall'agente solo come condotta e non anche come evento.
A tal riguardo, con riguardo alla intervenuta estensione della responsabilità amministrativa degli enti ex D.Lgs. n. 231/01 per i reati di omicidio colposo e lesioni personali colpose gravi o gravissime commessi con violazione delle norme in materia di salute e sicurezza sul lavoro, é bene tener presente che la vigente disciplina legislativa della prevenzione dei rischi lavorativi detta i principi e criteri essenziali per la gestione della salute e sicurezza sul lavoro in azienda e pertanto, in questo ambito, il modello organizzativo non potrà prescindere da tale precondizione.

Avendo ENERCOM già in precedenza attivato processi di autovalutazione dell'organizzazione interna, anche mediante i percorsi di certificazione, il presente Modello 231 prende dunque da essi le mosse per focalizzarne l'applicazione anche per tutte le tipologie di rischio e con tutte le modalità contemplate dal Decreto.

LINEE GUIDA DI CONFINDUSTRIA E DOCUMENTI DI SISTEMA

La predisposizione del presente Modello 231 è ispirata alle *Linee Guida* emanate da Confindustria il 31 marzo 2008 (di seguito le "Linee Guida").

Il percorso da queste indicato per l'elaborazione del Modello 231 può essere schematizzato secondo i seguenti punti fondamentali:

- individuazione delle aree a rischio, volta a verificare in quali aree/settori aziendali sia possibile la realizzazione dei reati;
- analisi degli scostamenti tra il modello di prevenzione e l'attuale sistema di controllo e procedure esistenti nell'azienda (gap analysis);
- predisposizione di un sistema di controllo in grado di ridurre i rischi attraverso l'adozione di apposite procedure e/o disposizioni organizzative. A supporto di ciò vi è l'insieme coordinato di strutture organizzative, attività e regole operative applicate – su indicazione del vertice apicale – dal management e dal personale aziendale, volto a fornire una ragionevole sicurezza in merito al raggiungimento delle finalità rientranti in un buon sistema di controllo interno.

Le componenti più rilevanti del sistema di controllo preventivo sono:

- Codice Etico;
- sistema organizzativo;
- procedure manuali ed informatiche;
- poteri autorizzativi e di firma;
- sistemi di controllo e gestione;
- comunicazioni al personale e sua formazione;
- sistema di verifiche

Il sistema di controllo inoltre deve essere informato ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- separazione delle funzioni (nessuno può gestire in autonomia tutte le fasi di un processo);
- documentazione dei controlli;
- introduzione di un adeguato sistema sanzionatorio e disciplinare per le violazioni delle norme e delle procedure previste dal modello;
- individuazione di un OdV i cui principali requisiti siano:
    - autonomia ed indipendenza,

  - professionalità,
  - continuità di azione.
- obbligo da parte delle funzioni aziendali, e segnatamente di quelle individuate come maggiormente "a rischio", di fornire informazioni all'OdV, sia su base strutturata (informativa periodica in attuazione del Modello 231 stesso), sia per segnalare anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (in quest'ultimo caso l'obbligo è esteso a tutti i dipendenti senza seguire linee gerarchiche).

Resta inteso che la scelta di non seguire in alcuni punti specifici le Linee Guida non inficia la validità di un Modello 231. Questo infatti essendo redatto con riferimento alla peculiarità di una società particolare, può discostarsi dalle Linee Guida che per loro natura hanno carattere generale.

MODELLO DI ORGANIZZAZIONE E DI GESTIONE DI ENERCOM

MOTIVAZIONI DI ENERCOM NELL'ADOZIONE DEL MODELLO 231

Sebbene l'adozione del Modello sia prevista dalla legge come facoltativa e non obbligatoria, ENERCOM, al fine di assicurare sempre più condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, ha ritenuto conforme alle proprie politiche aziendali procedere all'adozione di un modello di organizzazione, controllo e di gestione in linea con le prescrizioni del Decreto e sulla base delle Linee Guida emanate da Confindustria. Tale iniziativa, unitamente all'adozione del Codice Etico approvato da ENERCOM e richiamato nella Parte 2 del presente documento, è stata assunta nella convinzione che l'adozione di tale Modello 231 - al di là delle prescrizioni del Decreto, che indicano il Modello stesso come elemento facoltativo e non obbligatorio - possa costituire un valido strumento di sensibilizzazione nei confronti di tutti i dipendenti dell'Azienda e di tutti gli altri soggetti alla stessa cointeressati (Clienti, Fornitori, Partners, Collaboratori a diverso titolo), affinché seguano, nell'espletamento delle proprie attività, comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto.

Una forte spinta in tal senso è giunta anche dal Gruppo ENERGEI ("Gruppo" ai sensi dell'art. 2359, primo e secondo comma del Codice Civile), che ha ritenuto conforme alle proprie politiche aziendali procedere all'estensione del Modello 231 alle società controllate, tenendo conto della loro specifica struttura organizzativa e della peculiarità del loro business per definire un adeguato Modello 231.

FINALITÀ DEL MODELLO

Il Modello 231 predisposto da ENERCOM si fonda su un sistema strutturato ed organico di procedure nonché di attività di controllo che nella sostanza:

1. individuano le aree/i processi di possibile rischio nell'attività aziendale, vale a dire quelle attività nel cui ambito si ritiene più alta la possibilità che siano commessi i reati;
2. definiscono un sistema normativo interno diretto a programmare la formazione e l'attuazione delle decisioni dell'Azienda in relazione ai rischi/reati da prevenire tramite:
   - un Codice Etico, che fissa i principi ed orientamento generali,
   - procedure formalizzate e finalizzate a disciplinare in dettaglio le modalità operative nei settori "sensibili" (Elenco delle Procedure del Sistema Qualità di ENERCOM negli Allegati);
   - un sistema di deleghe di funzioni e di procure per la firma di atti aziendali che assicuri una chiara e trasparente rappresentazione dei processi e di attuazione delle decisioni;
3. determinano una struttura organizzativa coerente volta ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara ed organica attribuzione dei compiti, applicando una giusta segregazione delle funzioni, assicurando che gli assetti voluti della struttura organizzativa siano realmente attuati;
4. individuano i processi di gestione e controllo delle risorse finanziarie nelle attività a rischio;
5. attribuiscono all'OdV il compito di vigilare sul funzionamento e sull'osservanza del Modello 231 e di proporne l'aggiornamento.

Pertanto il Modello 231 si propone come finalità quelle di:

1. Migliorare il sistema di Governance Aziendale;
2. Predisporre un sistema strutturato ed organico di prevenzione e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi all'attività aziendale con particolare riguardo alla riduzione di eventuali comportamenti illegali;

3. Determinare, in tutti coloro che operano in nome e per conto di ENERCOM nelle "aree di attività a rischio di reato", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale ed amministrativo, non solo nei propri confronti ma anche nei confronti dell'azienda;
4. Informare tutti coloro che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse di ENERCOM che la violazione delle prescrizioni contenute nel Modello 231 comporterà l'applicazione di apposite sanzioni ovvero la risoluzione del rapporto contrattuale.
5. Ribadire che ENERCOM non tollera comportamenti illeciti, di qualsiasi tipo ed indipendentemente da qualsiasi finalità, in quanto tali comportamenti (anche nel caso in cui l'Azienda fosse apparentemente in condizione di trarne vantaggio) sono comunque contrari ai principi etici cui ENERCOM intende attenersi.

STRUTTURA DEL DOCUMENTO

Il presente documento (Modello 231) è costituito dalle seguenti parti:

a. "**Parte 1: Principi Generali**": dopo un richiamo ai principi del Decreto, sono illustrate le componenti essenziali del Modello con particolare riferimento all'OdV, alla formazione del personale ed alla diffusione del Modello 231 nel contesto aziendale, al sistema disciplinare ed alle misure da adottare in caso di mancata osservanza delle prescrizioni del Modello.

b. "**Parte 2: "Codice Etico**": sono illustrati i principi che hanno portato ENERCOM a redigere e diffondere il "Codice" in Azienda e tra tutti i dipendenti ed i partners.

c. "**Parti Speciali**" (con numerazione progressiva): predisposte per le differenti tipologie di reato contemplate nel Decreto 231/01 e successive integrazioni considerate di possibile "rischio-reato" da parte di ENERCOM. Le "Parti Speciali" sono riferite ai risultati della matrice ***Analisi Rischio-Modello 231***, documento di correlazione fra reati individuati, aree aziendali, attività a rischio-reato, probabilità di accadimento, controlli, regole, procedure ed istruzioni operative predisposte per mitigare il rischio.

MODIFICHE ED INTEGRAZIONI DEL MODELLO

Il presente Modello 231 è un "atto d'emanazione dell'organo dirigente" - in conformità alle prescrizioni dell'art. 6, comma 1, lettera a) del Decreto – pertanto la sua adozione, così come le successive modifiche ed integrazioni sono rimesse alla competenza del CdA di ENERCOM.

In particolare è demandato al CdA di ENERCOM la decisione d'integrare il presente Modello 231 con ulteriori Parti Speciali relative a nuove tipologie di reato a seguito di nuovi aggiornamenti al Decreto stesso.

DESTINATARI DEL MODELLO 231

I destinatari del Modello sono coloro che operano per il conseguimento degli obiettivi della società e tra questi sono compresi i membri degli organi sociali, i dipendenti, partner, i consulenti, i fornitori.

L'ORGANISMO DI VIGILANZA (ODV)

Si è già detto che il sistema organizzativo deve prevedere quale presupposto indispensabile al fine dell'esonero da responsabilità anche l'istituzione di un apposito organo di controllo interno all'ente dotato di autonomi poteri di iniziativa e controllo, il cosiddetto Organismo di Vigilanza (nel seguito OdV), che ha il compito di vigilare sull'efficacia reale ovvero sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento.

L'affidamento di detti compiti all'Organismo e, ovviamente, il corretto ed efficace svolgimento degli stessi costituiscono, infatti, presupposti indispensabili per l'esonero della società dalla responsabilità, in quanto l'efficace attuazione del Modello richiede, oltre all'istituzione di un sistema disciplinare, una sua verifica periodica, evidentemente da parte dell'organismo a ciò deputato.

Funzioni e poteri dell'OdV

La *mission* dell'OdV di ENERCOM consiste nel:

1. vigilare sull'applicazione del Modello 231 in relazione alle diverse tipologie di reati contemplate dal Decreto e risultate "sensibili" dalle analisi di ENERCOM;
2. verificare l'efficacia del Modello 231 e la sua capacità di prevenire la commissione dei reati di cui al Decreto;
3. individuare e proporre al CdA aggiornamenti e modifiche del Modello 231 in relazione alla mutata normativa o alle mutate condizioni aziendali.

Su di un piano più operativo sono affidati all'OdV di ENERCOM i seguenti compiti:

- Verificare periodicamente la matrice delle aree a rischio reato al fine di adeguarla ai mutamenti dell'attività e/o della struttura aziendale. A tal fine la Direzione e gli addetti alle attività di controllo nell'ambito delle singole funzioni devono segnalare all'OdV le eventuali situazioni in grado di esporre l'azienda al rischio di reato. Tutte le comunicazioni devono essere scritte (messaggi di posta elettronica) e non anonime.
- Effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici, posti in essere nell'ambito delle aree di attività a rischio come definite nelle singole Parti Speciali del Modello 231.
- Raccogliere, elaborare e conservare le informazioni (comprese le segnalazioni indicate al paragrafo *Flussi informativi verso* ***l'OdV)*** rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere obbligatoriamente trasmesse allo stesso OdV.
- Condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello 231 portate all'attenzione dell'OdV da segnalazioni o emerse nel corso dell'attività di vigilanza dello stesso.
- Verificare che gli elementi previsti dalle singole Parti Speciali del Modello 231 per le diverse tipologie di reati (adozione di regole interne, procedure, istruzioni operative ecc.) siano comunque adeguati e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto, provvedendo, in caso contrario, a proporre aggiornamenti degli elementi stessi.

Per lo svolgimento dei compiti suddetti l'OdV è dotato di tutti i poteri necessari, anche ispettivi e di accesso ai documenti aziendali, per assicurare una puntuale ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello organizzativo adottato dalla società, secondo quanto stabilito dall'art. 6 del D.Lgs. n. 231/2001, e segnatamente per l'espletamento dei seguenti compiti:
a) verifica dell'efficienza ed efficacia del Modello organizzativo adottato rispetto alla prevenzione ed all'impedimento della commissione dei reati previsti dal D.Lgs. n. 231/2001;

b) verifica del rispetto delle modalità e delle procedure previste dal Modello organizzativo e rilevazione degli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie funzioni;
c) formulazione delle proposte all'organo dirigente per gli eventuali aggiornamenti ed adeguamenti del Modello organizzativo adottato, da realizzarsi mediante le modifiche e/o le integrazioni che si dovessero rendere necessarie in conseguenza di:
- significative violazioni delle prescrizioni del Modello organizzativo;
- significative modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività d'impresa;
- modifiche normative.
Gli incontri con il CdA, cui l'OdV riferisce, vengono verbalizzati e copia della documentazione viene custodita dall'OdV;
d) segnalazione al CdA, affinché assuma gli opportuni provvedimenti, dell'accertamento di violazioni del Modello organizzativo che possono determinare una responsabilità in capo alla società. Gli incontri con il CdA, cui l'OdV riferisce, vengono verbalizzati e copia della documentazione viene custodita dall'OdV;
e) predisposizione di una relazione informativa, su base almeno annuale, per l'organo dirigente e, in particolare, in ordine alle attività di verifica e controllo compiute ed all'esito delle stesse;
f) trasmissione della relazione di cui al punto precedente al Collegio sindacale.

L'attività posta in essere dall'Organismo non può essere sindacata da alcun altro organismo o struttura aziendale, fermo restando in ogni caso l'obbligo di vigilanza sull'adeguatezza dell'operato dell'OdV in capo al CdA, in quanto organo dirigente cui spetta la responsabilità ultima del funzionamento e dell'efficacia del modello organizzativo.
L'OdV ha libero accesso presso tutte le funzioni della Società - senza necessità di alcun consenso preventivo - onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal D.Lgs. n. 231/01 e si avvale - sotto la sua diretta sorveglianza e responsabilità - del supporto e della cooperazione delle strutture aziendali che possano essere interessate o comunque coinvolte nelle attività di controllo ovvero di consulenti esterni. In merito deve peraltro precisarsi che, con riferimento all'estensione dell'applicazione del Decreto ai delitti colposi, il piano della sicurezza e quello del modello organizzativo, nonché le attività dei soggetti responsabili dei controlli in materia di salute e sicurezza sul lavoro e l'organismo di vigilanza presentano ciascuno una autonomia di funzioni che non consente una sovrapposizione dei rispettivi compiti di controllo, in quanto i diversi soggetti deputati al controllo svolgono i propri compiti su piani differenti.

L'OdV dispone di risorse finanziarie e professionali adeguate ed idonee a supportare le decisioni di spesa necessarie ad assolvere le proprie funzioni (consulenze specialistiche, missioni e trasferte, aggiornamento, etc.). L'assegnazione di un budget, su proposta dall'Organismo stesso, consente all'OdV di operare in autonomia e con gli strumenti opportuni per un efficace espletamento delle attività che gli sono assegnate nel presente Modello e da quanto previsto dal D.Lgs. 231/01.

Caratteristiche dell'OdV

Secondo le disposizioni del Decreto (artt. 6 e 7) e le indicazioni contenute nella Relazione di accompagnamento al Decreto, le caratteristiche dell'OdV debbono essere:

- Autonomia ed indipendenza,
- professionalità,
- continuità d'azione.

a) Autonomia ed indipendenza

I requisiti di autonomia e indipendenza dell'OdV sono fondamentali ai fini della funzionalità dello stesso e dell'assolvimento dei compiti che la legge assegna allo stesso e sono stati assicurati collocando l'OdV in una posizione gerarchica la più elevata possibile onde garantirne l'autonomia dell'iniziativa di controllo da ogni forma d'interferenza e/o di condizionamento da parte di qualunque componente dell'ente e in particolare del Consiglio di Amministrazione, nei cui confronti è tenuto alla sola attività di reporting.

La necessaria autonomia di iniziativa e l'indipendenza è stata inoltre assicurata escludendo che l'OdV possa essere direttamente coinvolto nelle attività operative e gestionali che costituiscono l'oggetto della sua attività di controllo e che, rendendolo partecipe di decisioni ed attività operative, ne minerebbero l'obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello.
Con riferimento ai componenti dell'Organismo reclutati all'esterno i requisiti di autonomia ed indipendenza debbono essere riferiti ai singoli componenti. Non essendo invece esigibile dai componenti di provenienza interna una totale indipendenza dalla società, questi ultimi non possono svolgere, nell'ambito della società o di soggetti da questa controllati o che la controllano, funzioni operative e il grado di indipendenza dell'Organismo deve essere valutato nella sua globalità.

b) Professionalità

L'OdV deve possedere al suo interno le competenze tecnico professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche unite all'indipendenza garantiscono l'obbiettività di giudizio.

In particolare, l'OdV, per poter svolgere efficacemente l'attività affidatagli, deve possedere un bagaglio di strumenti e tecniche specialistici propri di chi svolge attività "ispettiva", ma anche consulenziale di analisi dei sistemi di controllo e di tipo giuridico e, più in particolare, penalistico.

È essenziale la conoscenza della struttura e delle modalità realizzative dei reati, che è stata e viene assicurata mediante l'utilizzo delle risorse aziendali ovvero della consulenza esterna.
A questo riguardo, per quanto concerne le tematiche di tutela della salute e sicurezza sul lavoro, l'Odv si avvale di tutte le risorse attivate per la gestione dei relativi aspetti (RSPP - Responsabile del Servizio di Prevenzione e Protezione, ASPP – Addetti al Servizio di Prevenzione e Protezione, RLS – Rappresentante dei Lavoratori per la Sicurezza, MC - Medico Competente, addetti primo soccorso, addetto emergenze in caso d'incendio), comprese quelle previste dalle normative di settore quali, ad esempio, il già citato D.Lgs. n. 81/08.

c) Continuità d'azione

L'OdV deve:

- lavorare costantemente sulla vigilanza del Modello con i necessari poteri d'indagine,
- essere pertanto strutturato in modo tale da garantire la continuità dell'attività di vigilanza,
- curare l'attuazione del Modello e assicurarne il costante aggiornamento,
- non svolgere mansioni operative che possano condizionare la visione d'insieme delle attività aziendali che ad esso si richiede.

Per garantire l'efficace e costante attuazione di un modello organizzativo così articolato e complesso, è necessaria una struttura, quale è l'OdV, dedicata esclusivamente all'attività di vigilanza sul Modello e priva di mansioni operative che possano portarla ad assumere decisioni con effetti economico-finanziari.
Peraltro, l'OdV può fornire anche pareri consultivi sulla costruzione e aggiornamento del Modello, i quali non intaccano l'indipendenza e l'obiettività di giudizio su specifici eventi.

La definizione degli aspetti attinenti alla continuità dell'azione dell'Organismo, quali la calendarizzazione dell'attività, la verbalizzazione delle riunioni e la disciplina dei flussi informativi dalle strutture aziendali all'Organismo, viene rimessa allo stesso Organismo, che per tali attività provvede a disciplinare autonomamente

il proprio funzionamento, se del caso anche mediante apposito regolamento interno (ad es. determinazione delle cadenze temporali dei controlli, individuazione dei criteri e delle procedure di analisi, ecc.).

Nomina e composizione dell'OdV

Al fine di garantire una maggiore effettività dei controlli demandati dalla legge e tenuto conto della dimensione e complessità organizzativa di ENERCOM, si è ritenuto opportuno optare per una composizione plurisoggettiva dell'OdV, con componenti muniti dei requisiti di cui sopra.

L'OdV di ENERCOM (la composizione dell'OdV è disponibile negli Allegati), è un organo collegiale, composto da 3 (tre) membri che presentano i requisiti di autonomia, onorabilità e professionalità necessari per lo svolgimento dei compiti richiesti, attestati anche dall'iscrizione nei relativi albi professionali.

I componenti hanno una significativa conoscenza dell'Azienda che permette all'OdV, nella sua attività collegiale, di comprenderne pienamente le dinamiche ed assicurare l'indispensabile continuità d'azione.

L'OdV di ENERCOM è nominato dal Consiglio di Amministrazione (CdA). Sono di competenza dell'OdV, le attività di vigilanza e controllo previste dal Modello 231.

In considerazione della peculiarità delle proprie attribuzioni e dei contenuti professionali specifici da esse richiesti, l'OdV nello svolgimento dei propri compiti si avvale delle Funzioni aziendali di ENERCOM che, di volta in volta, si possono rendere utili allo svolgimento delle attività stesse.

Durata dell'incarico e causa di cessazione dell'OdV

L'incarico ai componenti dell'OdV è conferito per la durata stabilita dal CdA all'atto della nomina che, comunque, non può essere inferiore ad un anno e superiore a tre anni e può essere rinnovato.

La cessazione dall'incarico dell'OdV può avvenire per una delle seguenti cause:

- scadenza dell'incarico;
- revoca dell'OdV da parte del CdA di ENERCOM;
- rinuncia dei componenti dell'OdV, formalizzata con apposita comunicazione scritta inviata al CdA di ENERCOM.

La revoca dell'OdV può avvenire solo per giusta causa al fine di garantirne l'assoluta indipendenza.

Per giusta causa di revoca possono intendersi, in via non esaustiva:

- una grave negligenza nell'espletamento dei compiti riferiti all'incarico;
- il possibile coinvolgimento della Società in un procedimento, penale o civile, che sia riferito ad una omessa o insufficiente vigilanza, anche colposa.

La revoca per giusta causa è disposta dal CdA di ENERCOM.

In caso di scadenza, revoca o rinuncia, il CdA di ENERCOM provvede alla nomina di un nuovo OdV.

Reporting dell'OdV verso il vertice Societario.

Sono assegnate all'OdV di ENERCOM due linee di reporting:

- la prima, su *base continuativa*, direttamente con Direttore Generale, il Collegio Sindacale;
- la seconda, su *base periodica*, nei confronti del CdA.

La presenza dei suddetti rapporti di carattere funzionale, anche con organismi privi di compiti operativi e quindi svincolati da attività gestionali, costituisce un fattore in grado di assicurare che l'incarico venga espletato dall'OdV con le maggiori garanzie di indipendenza. L'OdV di ENERCOM potrà essere convocato in qualsiasi

momento dai suddetti organi o potrà a sua volta presentare richiesta in tal senso, per riferire in merito al funzionamento del Modello 231 od a situazioni specifiche.

Ogni anno, inoltre, l'OdV di ENERCOM trasmette al CdA, un rapporto scritto sull'attuazione del Modello 231.

Flussi informativi verso l'OdV

Il Decreto, alla lettera d) del secondo comma dell'art. 6, richiede la previsione di obblighi di informazione nei confronti dell'Organismo, quale ulteriore strumento per agevolare l'attività di vigilanza sull'efficacia del Modello e di accertamento a posteriori delle cause che hanno reso possibile il verificarsi del reato.
In particolare, l'obbligo di dare informazione all'Organismo riguarda le funzioni aziendali a rischio reato con riferimento a: *a)* le risultanze periodiche dell'attività di controllo dalle stesse posta in essere per dare attuazione ai modelli (*report* riepilogativi dell'attività svolta, attività di monitoraggio, indici consuntivi, ecc.); *b)* le anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (un fatto non rilevante se singolarmente considerato, potrebbe assumere diversa valutazione in presenza di ripetitività o estensione dell'area di accadimento).
Si precisa che i detti flussi informativi hanno lo scopo di migliorare l'attività di pianificazione dei controlli da parte dell'OdV, che non è peraltro tenuto per ogni singola segnalazione ad attivarsi, essendo rimesso alla sua discrezionalità e responsabilità stabilire in quali casi agire.
L'obbligo di informazione incombe anche ai dipendenti che vengono a conoscenza di notizie relative alla commissione dei reati in specie all'interno della società o a "pratiche" non in linea con le norme di comportamento che la società ha emanato nell'ambito del Modello disegnato dal D.Lgs. n. 231/01 (il c.d. Codice Etico).
È bene ricordare in merito che l'obbligo di informare il datore di lavoro di eventuali comportamenti contrari al Modello organizzativo rientra nel più ampio dovere di diligenza ed obbligo di fedeltà del prestatore di lavoro di cui agli artt. 2104 e 2105 del codice civile, i quali prevedono, rispettivamente:
"1. 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. 2. 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. 2104) e *"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 essa pregiudizio."* (art. 2105).
Pertanto, costituendo oggetto di espressi doveri, il corretto adempimento all'obbligo di informazione da parte del prestatore di lavoro non potrà dar luogo all'applicazione di sanzioni disciplinari nei confronti del medesimo.

0.1.1. Segnalazioni verso l'OdV

In ambito aziendale dovrà essere portata a conoscenza dell'OdV, oltre alla documentazione indicata nelle singole Parti del Modello secondo le procedure ivi contemplate, ogni altra informazione, di qualsiasi tipo, proveniente anche da terzi ed attinente all'attuazione del Modello nelle aree di attività a rischio.

Valgono al riguardo le seguenti prescrizioni:

- Devono essere raccolte eventuali segnalazioni relative alla violazione del Modello o comunque conseguenti a comportamenti non in linea con le regole di condotta adottate dalla Società stessa;
- L'OdV valuta le segnalazioni ricevute e le eventuali conseguenti iniziative a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere ad una indagine interna;

- Le segnalazioni, in linea con quanto previsto dal Codice Etico, dovranno essere in forma scritta e non anonima ed avere ad oggetto ogni violazione o sospetto di violazione del Modello. L'OdV agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti dell'Azienda o delle persone accusate erroneamente e/o in mala fede;
- Le segnalazioni che pervengono all'OdV devono essere raccolte e conservate in un apposito archivio (anche in formato digitale) al quale sia consentito l'accesso solo da parte dei membri dell'OdV.

A tal fine viene istituita l'apposita casella di posta elettronica odv@ENERCOMsrl.it , cui vanno inoltrate le suddette segnalazioni, con modalità di funzionamento tali da garantire la riservatezza a chi segnala le violazioni.

Nel contempo, vengono previste misure deterrenti contro ogni segnalazione effettuata impropriamente, sia in termini di contenuti che di forma.

0.1.2. Obblighi di informativa relativi ad atti societari

Oltre alle segnalazioni anche ufficiose di cui al capitolo precedente, devono essere obbligatoriamente trasmesse all'OdV di ENERCOM le informative concernenti:

- I provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai quadri in caso di avvio di un procedimento giudiziario per i reati previsti dal Decreto;
- I rapporti preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto;
- Le notizie riguardanti l'effettiva attuazione, a tutti i livelli aziendali, del Modello organizzativo con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i Dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- Le decisioni concernenti la richiesta, erogazione ed utilizzo di finanziamenti pubblici;
- Le commissioni d'inchiesta o relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al Decreto;
- Le notizie riguardanti commesse attribuite da enti pubblici o soggetti che svolgano funzioni di pubblica utilità;
- Informazioni riferibili alle fattispecie di reati societari;
- L'organismo di vigilanza deve altresì ricevere copia della reportistica periodica in materia di salute e sicurezza sul lavoro.

0.1.3. Sistema delle deleghe: comunicazione e modifica.

All'OdV, infine, deve essere comunicato il sistema delle deleghe adottato da ENERCOM ed ogni modifica che intervenga sullo stesso.

Profili penali della responsabilità dell'OdV.

Fermo restando il generale dovere di vigilanza dell'Organismo e l'impossibilità per la società di beneficiare dell'esonero dalla responsabilità nel caso in cui vi sia stata omessa vigilanza, va precisato che in caso di commissione d'illeciti da parte dell'Azienda a seguito del mancato esercizio del potere di vigilanza

sull'attuazione e sul funzionamento del Modello 231, non si configura in capo all'OdV una responsabilità penale per concorso omissivo nei reati commessi dalla società secondo il principio di cui all'art. 40, comma 2, cod. pen. (*"non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo"*).

All'OdV sono devoluti, infatti, compiti di controllo non a proposito della realizzazione dei reati ma al funzionamento ed osservanza del Modello.
Attribuire all'OdV il compito d'impedire i reati non avrebbe infatti senso, stante la sostanziale assenza in capo allo stesso di poteri impeditivi, in quanto assolve compiti consultivi a favore del CdA, cui compete il potere effettivo di modificare i modelli.

Osservazioni analoghe valgono anche per i delitti colposi realizzati con violazione delle norme in materia di salute e sicurezza sul lavoro. Anche in questo caso l'Organismo di vigilanza non ha obblighi di controllo dell'attività, ma doveri di verifica della idoneità e sufficienza dei modelli organizzativi a prevenire i reati.

FORMAZIONE ED INFORMAZIONE SUL MODELLO 231

Formazione del personale

ENERCOM promuove la conoscenza del Modello 231, delle Procedure richiamate e degli aggiornamenti, tra tutti i dipendenti che sono pertanto tenuti a conoscerne il contenuto, ad osservarle e contribuire alla loro attuazione. Ai fini dell'attuazione del Modello, la Responsabile Gestione Personale predispone con la Direzione ed in cooperazione con l'OdV, la formazione del personale che sarà continuativa ed articolata sui livelli qui di seguito indicati:

- **Personale direttivo e con funzioni di rappresentanza dell'Azienda (corso evoluto):**

  Il corso si rivolge ai dipendenti e collaboratori che operano nelle aree indicate come "a rischio-reato", all'OdV ed ai collaboratori preposti al controllo interno.

- **Altro personale (corso base):**

  Corso di formazione iniziale; nota informativa interna; informativa in sede di assunzione per i neo assunti; e-mail di aggiornamento. Il corso si rivolge ai dipendenti e collaboratori in generale.

Il materiale utilizzato nelle sessioni di formazione è reso disponibile, per la consultazione, nell'intranet Aziendale di ENERCOM.

Informativa a collaboratori interni, esterni e partners

ENERCOM da ampia divulgazione dei principi ispiratori del Modello 231, s'impegna a facilitare e promuoverne la conoscenza da parte di tutti i dipendenti, con grado di approfondimento diversificato secondo la posizione ed il ruolo.

Il Modello 231 è comunicato formalmente ad ogni componente degli organi sociali dall'OdV. Alla consegna della comunicazione viene richiesta la sottoscrizione di una dichiarazione di conoscenza ed adesione al Modello 231. Tale dichiarazione è archiviata e conservata dall'OdV.

Il Modello è comunicato formalmente a tutti i Dirigenti ed agli Uffici locali con la consegna del documento.

Il Modello è affisso nelle bacheche aziendali e l'Azienda provvede a darne ampia diffusione con iniziative mirate nei confronti dei Quadri, impiegati ed operai.

Il Modello è reso disponibile sul sito intranet aziendale. L'Azienda prevede iniziative di formazione ed informazione mirata con l'utilizzo di risorse informatiche.

ENERCOM promuove la conoscenza e l'osservanza del Modello 231 anche tra i partner commerciali e finanziari, i consulenti, i collaboratori a vario titolo, i clienti ed i fornitori.

Coerentemente con quanto previsto dal Codice Etico, informazioni sul Modello sono rese disponibili a tutti coloro che intrattengono relazioni con l'Azienda.

L'impegno al rispetto dei principi del Modello 231, da parte di terzi che hanno rapporti d'affari o contrattuali con l'Azienda, sono oggetto di apposita clausola contrattuale da sottoscrivere, in segno di accettazione, da parte delle terze parti stesse.

SISTEMA DISCIPLINARE

Principi generali

La predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni contenute nelle norme del Codice Etico, nonché nelle procedure previste dal modello è condizione essenziale per assicurare l'effettività del Modello stesso.

Al riguardo, infatti, l'articolo 6 comma 2, lettera e) del Decreto prevede che i modelli di organizzazione e gestione devono *"introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello".*

Simili violazioni ledono infatti il rapporto di fiducia instaurato con l'ente (si vedano anche gli artt. 2104 e 2105 c.c., che stabiliscono obblighi di diligenza e fedeltà del prestatore di lavoro nei confronti del proprio datore) e devono di conseguenza comportare azioni disciplinari, a prescindere dall'eventuale instaurazione di un giudizio penale nei casi in cui il comportamento costituisca reato.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello 231 sono assunte da ENERCOM in piena autonomia ed indipendentemente dalla tipologia di illecito che le violazioni del modello stesso possano determinare.
La valutazione disciplinare dei comportamenti effettuata dal datore di lavoro, salvo, naturalmente, il successivo eventuale controllo del giudice del lavoro, non deve, infatti, necessariamente coincidere con la valutazione del giudice in sede penale, data l'autonomia della violazione del codice etico e delle procedure interne rispetto alla violazione di legge che comporta la commissione di un reato. Il datore di lavoro non è tenuto ad attendere il risultato del procedimento penale eventualmente in corso. I principi di tempestività ed immediatezza della sanzione rendono infatti sconsigliabile ritardare l'irrogazione della sanzione disciplinare in attesa dell'esito del giudizio eventualmente instaurato davanti al giudice penale.
Quanto alla tipologia di sanzioni irrogabili, va ricordato che, nel caso di rapporto di lavoro subordinato, qualsiasi provvedimento sanzionatorio deve essere adottato nel rispetto delle procedure previste dall'art. 7 dello Statuto dei Lavoratori e/o da normative speciali, dove applicabili, caratterizzato dai principi di tipicità delle violazioni e delle sanzioni.
In ragione della loro valenza disciplinare, il Codice Etico e le procedure del Modello 231 il cui mancato rispetto si intende sanzionare sono formalmente dichiarati vincolanti per tutti i destinatari del Modello mediante un comunicato formale, nonché esposti, così come previsto dall'art. 7, co. 1, l. n. 300/1970, *"mediante affissione in luogo accessibile a tutti"*, evidenziando esplicitamente le sanzioni collegate alle diverse violazioni.
Agli effetti della salute e sicurezza sul lavoro, vengono indicati in modo formale come vincolanti per tutti i dipendenti i principali doveri dei lavoratori, mutuandoli dalle previsioni dell'art. 5 del D.Lgs. n. 626/1994:
1. Ciascun lavoratore deve prendersi cura della propria sicurezza e della propria salute e di quella delle altre persone presenti sul luogo di lavoro, su cui possono ricadere gli effetti delle sue azioni o omissioni, conformemente alla sua formazione ed alle istruzioni e ai mezzi forniti dal datore di lavoro.
2. In particolare i lavoratori:
a) osservano le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;
b) utilizzano 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;
c) utilizzano in modo appropriato i dispositivi di protezione messi a loro disposizione;
d) segnalano immediatamente al datore di lavoro, 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;

e) non rimuovono o modificano senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
f) non compiono di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;
g) si sottopongono ai controlli sanitari previsti nei loro confronti;
h) contribuiscono, insieme al datore di lavoro, 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.

Qualora la violazione delle norme del Modello 231 fosse invece posta in essere da un lavoratore autonomo, fornitore o altro soggetto avente rapporti contrattuali con la società è prevista, quale sanzione, la risoluzione del contratto, mediante l'inserimento di clausole risolutive espresse nei contratti di fornitura o collaborazione (agenzia, *partnership*, appalto, ecc.) che fanno esplicito riferimento al rispetto delle disposizioni del Modello 231.

Violazioni del Modello 231

A titolo esemplificativo, costituisce violazione dei principi e delle norme dettate dal Modello:

- La realizzazione di azioni e comportamenti non conformi alle regole dettate dal Modello, come l'omissione di azioni o comportamenti prescritti nelle attività considerate "sensibili",
- La realizzazione di azioni e comportamenti non conformi alle regole dettate dal Modello, ovvero l'omissione di azioni e comportamenti prescritti dal Modello, nell'espletamento delle attività nell'ambito delle aree "sensibili" che:
    - a) espongono l'azienda a situazioni di rischio di commissione di uno dei reati previsti dal D.Lgs. 231/01;
    - b) siano diretti alla realizzazione di reati previsti dal citato Decreto e/o tali da determinare, in capo all'Azienda, un rischio di sanzioni previste dal D.Lgs. 231/01;
    - c) determinano attività nel cui ambito può ricorrere il rischio di commissione di reati previsti dal D.Lgs. 231/01.
- La realizzazione di azioni e comportamenti non conformi ai principi e alle regole indicate nel Codice Etico aziendale.

Sanzioni per i lavoratori dipendenti

Il sistema disciplinare in essere in ENERCOM è costantemente monitorato dall'OdV e dalla Direzione del Personale.

Misure nei confronti di Quadri, Impiegati, Operai

I comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali dedotte nel presente Modello sono definiti come *illeciti disciplinari*.

Le sanzioni adottate nei confronti dei lavoratori dipendenti rientrano tra quelle previste dal ***Codice disciplinare aziendale*** e dal ***CCNL vigente*** tali categorie descrivono comportamenti sanzionati, in base al rilievo che assumono le singole fattispecie considerate e le sanzioni in concreto previste per gli illeciti disciplinari secondo la loro gravità.

In applicazione dei "**Provvedimenti disciplinari**" previsti dal ***CCNL* del settore Gas-Acqua,** si prevede che:

1) Incorre nei provvedimenti di ***rimprovero scritto, multa o sospensione***, a secondo della gravità dell'infrazione ed alla reiterazione della stessa, il dipendente che:

- Violi le procedure interne previste dal Modello (ad es. non osservi le procedure prescritte, ometta di dare comunicazioni all' Organismo di Vigilanza delle informazioni prescritte, ometta di svolgere controlli, ecc), o adotti, nell'espletare attività nelle aree sensibili, un comportamento non conforme alle prescrizioni del Modello;

2) Incorre nel provvedimento del ***licenziamento con preavviso***, il dipendente che:

- Adotti nell'espletamento delle Attività sensibili un comportamento non conforme alle prescrizioni del Modello e diretto in modo univoco al compimento di un reato sanzionato ai sensi del D.Lgs. 231/01;

3) Incorre nel provvedimento del ***licenziamento senza preavviso***, il dipendente che:

- Adotti, nell'espletamento delle Attività sensibili, un comportamento palesemente in violazione delle prescrizioni del Modello, tale da determinare a carico della Società misure previste dal D.Lgs. 231/01.

Misure nei confronti di Dirigenti, Amministratori, Sindaci, Consulenti e Partners

In caso di violazione, da parte dei dirigenti, delle regole previste dal Modello 231 o di adozione, nell'espletamento di attività sensibili, di un comportamento non conforme alle prescrizioni del Modello stesso, si applicheranno, nei confronti del responsabile, le misure più idonee in conformità a quanto stabilito dal CCNL. Se la violazione del Modello fa venir meno il rapporto di fiducia, la sanzione è individuata nel licenziamento per giusta causa.

In caso di violazione del Modello da parte dei Consiglieri di Amministrazione, l'OdV informa il Collegio Sindacale ed il CdA i quali prenderanno gli opportuni provvedimenti.

In caso di violazione del Modello da parte di uno o più membri del Collegio Sindacale, l'OdV informa della notizia di violazione il CdA ed il Collegio Sindacale che procederanno agli accertamenti ed assumeranno, sentito il CdA, i provvedimenti opportuni.

Le violazioni del Modello da parte dei Consulenti o dei Partners o la commissione di reati di cui al D.Lgs. 231/01, sarà sanzionata secondo le previsioni delle clausole inserite nei relativi contratti.

E' fatta salva l'eventuale richiesta di risarcimento ove dal comportamento sanzionato derivassero all'Azienda danni concreti quali l'applicazione delle misure previste dal D.Lgs. 231/01.

In caso di violazione, da parte di dirigenti, delle procedure interne previste dal presente Modello o d'adozione, nell'espletamento d'attività nelle aree a rischio di un comportamento non conforme alle prescrizioni del Modello stesso, si applicherà nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti.

Sanzioni previste dalle norme di riferimento

Nel seguito del Modello, in ogni parte sviluppata (successive alla Parte 2) per le tipologie di reato considerate di possibile rischio da parte di ENERCOM, sono riportate le "Sanzioni" così come previste dalle norme emanate per quella tipologia di reato.

VERIFICA APPLICAZIONE E ADEGUATEZZA DEL MODELLO 231

Il Modello 231 è soggetto a verifiche periodiche con cadenza minima semestrale definite nel Piano di Audit predisposto dall'OdV ed approvato dalla Presidenza.

Il piano di Audit deve prevedere la possibilità di effettuare verifiche "a sorpresa" per le aree identificate come "a rischio-reato".

Le verifiche avranno un duplice scopo:

- attività di monitoraggio sull'effettività del Modello (verifica della coerenza tra i comportamenti dei destinatari ed il Modello stesso) tramite verifiche documentate che devono evidenziare, in particolare:
  a) che siano state rispettate le indicazioni ed i contenuti del presente Modello,
  b) che siano stati rispettati i poteri di delega ed i limiti di firma;
  c) che non siano state attuate azioni non in linea con il Modello 231.

I verbali emessi a documentazione delle verifiche saranno condivisi con i responsabili delle aree verificate e saranno trasmessi all'OdV che ne valuterà i risultati e, ove necessario, attiverà con il Management interessato interventi correttivi o migliorativi e ne curerà l'archiviazione.

- verifiche delle procedure: annualmente l'effettivo funzionamento del presente Modello sarà verificato e documentato all'OdV.

Sarà inoltre intrapresa un'analisi di tutte le segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dall'OdV e dagli altri soggetti interessati, degli eventi considerati rischiosi, della consapevolezza del personale rispetto alle ipotesi di reato previste dal Decreto, con verifiche a campione.

L'esito di tale verifica, con l'evidenziazione delle possibili manchevolezze ed i suggerimenti delle azioni da intraprendere, sarà incluso nel rapporto annuale che l'OdV predispone per il CdA di ENERCOM.

Parte generale 2

CODICE ETICO

CODICE ETICO DI ENERCOM

Il Codice Etico di ENERCOM è allegato al presente Modello (Allegati).

Politica Aziendale

La Presidenza di ENERCOM ha adottato il Codice Etico e l'Azienda si aspetta che tutti i suoi dipendenti, i partner commerciali e finanziari, i consulenti, i collaboratori a vario titolo, i clienti ed i fornitori si attengano ai

- "principi etici" del Codice Etico
- "regole comportamentali e regole di espresso divieto" indicate nello stesso codice etico.

Procedura

Tutti i dipendenti, ed i neo-assunti devono leggere e firmare una Dichiarazione di Accettazione/Presa visione del Codice Etico, prima di iniziare l'operatività aziendale.

ENERCOM promuove la conoscenza e l'osservanza dei due documenti anche tra i partner commerciali e finanziari, i consulenti, i collaboratori a vario titolo, i clienti ed i fornitori.

Su base annuale ed in occasione di aggiornamenti significativi, L'OdV deve coinvolgere le posizioni chiave dell'Azienda per garantire la conformità delle stesse, con il Codice Etico. Ai livelli interessati (Presidenza, le posizioni direttive delle funzioni coinvolte e altri dipendenti che possono potenzialmente operare con i Partners di ENERCOM) è richiesta la certificazione di conformità con la politica Aziendale con sottoscrizione di una Dichiarazione predisposta a tale scopo.

Responsabilità di applicazione

L'OdV è responsabile dell'attuazione della Politica, ivi compreso l'ottenimento delle certificazioni indicate sopra e della loro archiviazione.

I dirigenti tutti sono responsabili dell'applicazione della conformità alla Politica.

Applicazione

La Politica Aziendale si applica a tutte le operazioni di ENERCOM.

Parte speciale 3

REATI IN DANNO

della PUBBLICA AMMINISTRAZIONE

REATI NEI RAPPORTI CON LA P.A. (artt. 24 e 25)

E REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (art. 25-decies del Decreto)

Le figure di reato che vengono in rilievo nei rapporti con la pubblica Amministrazione vengono qui di seguito indicate e brevemente illustrate:

- **Malversazione a danno dello Stato o dell'Unione Europea** (art. 316-bis c.p.): il reato consiste nell'utilizzare le somme ricevute a titolo di finanziamento e di contributo da parte dello Stato, di altro ente pubblico e dell'Unione Europea per scopi diversi da quelli a cui erano destinate, ovvero nel distrarle anche solo in parte, senza che rilevi che l'attività programmata si sia comunque svolta.
- **Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea** (art. 316-ter c.p.): il reato si configura allorché, utilizzando o presentando dichiarazioni o documenti falsi o attestanti cose non vere ovvero omettendo informazioni dovute si ottengono, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominati, concessi o erogati dallo Stato, da altri enti pubblici o dalla Unione europea.
  Peraltro tale reato si configura solo nei casi in cui la condotta non integri gli estremi del più grave reato di truffa aggravata per il conseguimento di erogazioni pubbliche di cui all'art. 640-bis c.p..
- **Concussione** (art. 317 c.p.): si verifica quando un pubblico ufficiale o un incaricato di un pubblico servizio abusa della sua qualità o dei suoi poteri e costringe o induce taluno a dare o a promettere indebitamente a sé o ad altri denaro o altre utilità.
- **Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio** (artt. 318 e 319 c.p.): si configura nel caso in cui un pubblico ufficiale riceva o ne accetti la promessa, per sé o per altri, denaro o altra utilità per omettere, ritardare o compiere un atto del suo ufficio o un atto contrario al suo dovere d'ufficio, in modo tale da favorire il soggetto che ha offerto denaro o altra utilità.
  L'attività del pubblico ufficiale può consistere sia in un atto dovuto (ad es. velocizzare una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ad es., il pubblico ufficiale accetta denaro per garantire l'aggiudicazione di una gara).
  L'elemento distintivo rispetto al reato di concussione è dato dall'accordo raggiunto tra corruttore e corrotto per il conseguimento di un vantaggio reciproco, mentre elemento essenziale della concussione è che il pubblico ufficiale o l'incaricato del pubblico servizio, abusando della propria qualità, costringono il privato a dare o promettere l'utilità.
- Circostanze aggravanti (art. 319-bis c.p.): la pena è aumentata se il fatto di cui all'art. 319 c.p. ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene.
- Corruzione in atti giudiziari (art. 319-ter c.p.): si ha allorché si corrompe un pubblico ufficiale - un magistrato, un cancelliere od altro funzionario - per favorire o danneggiare una parte in un procedimento giudiziario e, al fine di ottenere nel medesimo procedimento un vantaggio non espressamente previsto da norme di legge, anche a favore di una società che non sia parte nel detto procedimento.
- **Corruzione di persona incaricata di un pubblico servizio** (art. 320 c.p.): si realizza allorché un incaricato di pubblico servizio riceva (o ne accetti la promessa), per sé o per altri, denaro o altra utilità per omettere o ritardare un atto del suo ufficio ovvero per compiere un atto contrario al suo dovere d'ufficio.
- **Pene per il corruttore** (art. 321 c.p.): le pene stabilite negli artt. 318 comma 1, 319, 319-bis, 319 ter, e 320 c.p. in relazione alle ipotesi di cui agli artt. 318 e 319 c.p. trovano applicazione anche nei confronti di chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il danaro o altra pubblica utilità.
- **Istigazione alla corruzione** (art. 322 c.p.): tale reato si configura allorché venga offerto o promesso denaro o altra utilità ad un pubblico ufficiale o incaricato di pubblico servizio onde indurlo a compiere, omettere, ritardare ovvero a fare un atto contrario ai doveri del suo ufficio, ma tale offerta o promessa venga rifiutata.

- Concussione, corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.): si tratta dei reati sopra descritti di concussione e corruzione allorquando l'offerta o la promessa di denaro o altra utilità abbiano luogo nei confronti di:
  1) membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;
  2) funzionari e agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;
  3) persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;
  4) membri e addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;
  5) coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;
  6) persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali ovvero al fine di ottenere o di mantenere un'attività economica o finanziaria.
- **Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea** (art. 640, comma 2 n. 1, c.p.): si configura nel caso in cui siano posti in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato o ad altro Ente Pubblico o all'Unione Europea al fine di realizzare un ingiusto profitto. Tale fattispecie può realizzarsi ad esempio nel caso in cui, nel partecipare a una procedura di gara per la fornitura di energia, si forniscano alla P.A. informazioni non veritiere (es. documentazione artefatta), al fine di ottenere l'aggiudicazione della gara.
- **Truffa aggravata per il conseguimento di erogazioni pubbliche** (art. 640-bis c.p.): consiste nella truffa posta in essere per conseguire indebitamente erogazioni pubbliche. Il reato può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.
- **Frode informatica in danno dello Stato o di altro ente pubblico** (art. 640-ter c.p.): si configura nel caso in cui, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottiene un ingiusto profitto arrecando danno a terzi. Può realizzarsi in concreto qualora, ottenuto un finanziamento, venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente. È punibile a querela di parte.
- **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** (art. 377-bis c.p.): si configura ogniqualvolta vi sia una condotta diretta ad influenzare la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere, per mezzo di violenza, minaccia, offerta o promessa di denaro o di altra utilità, col fine di celare elementi "compromettenti" a carico di una determinata società, con evidente interesse della medesima. La norma intende dunque tutelare il corretto svolgimento dell'attività processuale contro ogni forma di indebita interferenza.
- La legge 6 novembre 2012, n. 190 contenente modifiche all'art. 25 ha introdotto tra i reati presupposto l'"induzione indebita a dare o promettere utilità" (art. 319-quater c.p.) "*Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da tre a otto anni. Nei casi previsti dal primo comma, chi dà o promette enaro o altra utilità è punito con la reclusione fino a tre anni.*"

Per l'individuazione dei livelli di rischio di ciascun reato come sopra indicato, nell'ambito della specificità delle attività svolte da ENERCOM (o l'esclusione dello stesso per le evidenti ragioni ivi riportate), si rimanda all'Analisi del Rischio allegata.

ENTI DELLA PUBBLICA AMMINISTRAZIONE

I reati oggetto della presente parte speciale contemplano come proprio presupposto l'instaurazione di rapporti con la Pubblica Amministrazione (PA) o lo svolgimento di attività che potrebbero implicare l'esercizio di un pubblico servizio.

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

Sono ritenuti appartenere alla Pubblica Amministrazione quegli enti che svolgano "tutte le attività dello Stato e degli altri enti pubblici".

Per semplicità di comprensione si riepilogano qui di seguito i caratteri distintivi degli enti della Pubblica Amministrazione.

Enti della Pubblica Amministrazione	
Ente della Pubblica Amministrazione	Qualsiasi ente che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi
Pubblica Amministrazione	Tutte le attività dello Stato e degli altri enti pubblici

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

- istituti e scuole di ogni ordine e grado e le istituzioni educative;
- enti ed amministrazioni dello Stato ad ordinamento autonomo, quali:
  a) Presidenza del Consiglio dei Ministri e Ministeri;
  b) Camera dei Deputati e Senato della Repubblica;
  c) Dipartimento Politiche Comunitarie;
  d) Autorità Garante della Concorrenza e del Mercato;
  e) Autorità per l'Energia Elettrica ed il Gas (AEEG);
  f) Autorità per le Garanzie nelle Comunicazioni;
  g) Banca d'Italia;
  h) Consob;
  i) Autorità Garante per la protezione dei dati personali;
  j) Agenzia delle Entrate;
  k) ISVAP: Istituto di Vigilanza sulle assicurazioni private e di interesse collettivo;
- Regioni;
- Province;
- Comuni;
- Comunità montane, e loro consorzi e associazioni;
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
- Unione Europea e istituzioni collegate;
- tutti gli enti pubblici non economici nazionali, regionali e locali, quali:
  a) INPS;
  b) CNR;
  c) INAIL;
  d) INPDAI;
  e) INPDAP;

f) ISTAT;
g) ENASARCO;
h) ISPESL (Istituto Sup. Prevenzione e Sicurezza sul Lavoro)
i) ASL;
j) ARPA;
k) UTF;
l) Uffici Metrici.

- Enti e monopoli di Stato;
- RAI.

Deve peraltro osservarsi che non tutte le persone fisiche che agiscono nella sfera e in relazione alla P.A. ricoprono i ruoli di "Pubblici Ufficiali" e di "Incaricati di Pubblico Servizio" essenziali perché possano configurarsi, nei loro confronti o per loro opera, le fattispecie criminose ex D.Lgs. 231/01.
A tal proposito, si richiama l'art. 357 c.p., ai cui sensi è considerato pubblico ufficiale "agli effetti della legge penale" colui il quale esercita "una pubblica funzione legislativa, giudiziaria o amministrativa" ed "è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi", ovvero la funzione amministrativa prevista da norme di diritto pubblico, rivolte cioè al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.
Secondo l'art. 358 c.p. invece "sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".
Costituiscono esempi di incaricati di pubblico servizio i dipendenti delle autorità di vigilanza che non concorrono a formare la volontà dell'autorità e che non hanno poteri autoritativi, i dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati, gli impiegati degli uffici pubblici, etc.

RAPPORTI CON DIPENDENTI DELLA PUBBLICA AMMINISTRAZIONE

Il Modello di ENERCOM è stato predisposto tenendo presenti, oltre alle prescrizioni del Decreto di riferimento, le Politiche aziendali definite dalla Presidenza in materia di Rapporti col Personale della Pubblica Amministrazione, così come meglio definite nel Codice Etico. Pertanto il Personale di ENERCOM è tenuto a conoscere e rispettare leggi e regolamenti che governano i rapporti tra Pubblica Amministrazione, Clienti e Fornitori.

Per il Personale di ENERCOM costituisce condotta contraria alla politica aziendale dare direttamente o indirettamente denaro o doni a dipendenti della Pubblica Amministrazione se con tale comportamento si viola una legge dello stato che proibisce tale pagamento o dono. Il principio è sancito nel "Codice Etico" laddove ENERCOM individua i principi comportamentali cui l'Azienda riconosce un valore etico e ove sono individuate le regole comportamentali in rispetto dei valori etici riconosciuti dall'Azienda. (v. Allegati).

PRINCIPALI ATTIVITÀ A RISCHIO-REATO

Sono definite aree a rischio-reato tutte quelle aree aziendali che per lo svolgimento della propria attività intrattengono rapporti con le PA. Tenuto conto della molteplicità dei rapporti che ENERCOM intrattiene con le Amministrazioni Pubbliche, sono state individuate le seguenti aree di attività ritenute più specificamente a rischio:

1. negoziazione/stipulazione e/o esecuzione di contratti con soggetti pubblici, partecipazione a procedure di gara o di negoziazione indette da enti pubblici per l'assegnazione di commesse (di fornitura o di servizi), o altre operazioni similari nell'ambito di un contesto competitivo, ovvero in cui, anche in presenza di un solo concorrente, l'ente pubblico avrebbe potuto selezionare anche altre imprese.
2. gestione di eventuali contenziosi giudiziali e stragiudiziali relativi all'esecuzione di contratti stipulati con soggetti pubblici;
3. definizione di contratti con enti pubblici per la gestione di adempimenti, verifiche, ispezioni;
4. gestione dei rapporti con soggetti pubblici per gli aspetti relativi alla sicurezza ed all'igiene del lavoro, all'assunzione di personale disabile, ai trattamenti previdenziali del personale e/o gestione dei relativi accertamenti/ispezioni;
5. intrattenimento di rapporti con esponenti della P.A. che abbiano competenze in processi legislativi, regolamentari o amministrativi riguardanti la società (ad es. Autorità per l'Energia Elettrica ed il Gas, CONSOB, Autorità Garante della Concorrenza e del Mercato, ecc.), quando tali rapporti (incluso l'invio di dati o informazioni) possano comportare l'ottenimento di vantaggi rilevanti per la società stessa, dovendosi escludere l'attività di mera informativa, partecipazione a eventi o momenti istituzionali e scambio di opinioni relativamente a particolari politiche o normative.

Costituiscono situazioni di particolare attenzione nell'ambito delle suddette aree di attività a rischio:
a) la partecipazione alle procedure di gara in associazione con un Partner (ad es. joint venture, anche in forma di ATI, consorzi, ecc.);
b) l'assegnazione, ai fini della partecipazione alle procedure di gara per la fornitura di energia, di uno specifico incarico di consulenza o di rappresentanza a un soggetto terzo.

Eventuali integrazioni delle suddette aree di attività a rischio potranno essere disposte dal Presidente di ENERCOM Srl al quale viene dato mandato di individuare le relative ipotesi e di definire gli opportuni provvedimenti operativi.

Le aree a "rischio-reato", identificate, hanno costituito il punto di riferimento nella definizione delle procedure di gestione da implementare ai fini dell'adeguamento dell'attuale sistema di controlli interno.

La tipologia delle procedure di controllo implementate sulle diverse aree a rischio-reato sono state definite tenendo in considerazione la rilevanza dei singoli punti di contatto con la PA e sono integrate con le Procedure ed Istruzioni Operative redatte per le attività di dettaglio del Sistema Gestione Qualità di ENERCOM (v. Elenco delle Procedure del Sistema Qualità e Sicurezza di ENERCOM negli Allegati).

REGOLE DI COMPORTAMENTO

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, amministratori, dirigenti e dipendenti – con riferimento alla rispettiva attività - sono altresì tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei seguenti documenti:
- il Codice Etico;
- le procedure operative volte a garantire la trasparenza nel processo di approvvigionamento;
- ogni altra normativa interna relativa al sistema di controllo interno in essere nella società;
- le procedure informative per l'assunzione e la formazione del personale;
- il sistema disciplinare di cui al CCNL applicabile;

Ai collaboratori esterni viene resa nota l'adozione del Modello e del Codice Etico da parte di ENERCOM, la cui conoscenza e il rispetto dei cui principi costituisce obbligo contrattuale a carico di tali soggetti.

Ai "Destinatari" di questo capitolo, amministratori, dirigenti e dipendenti che operano nelle aree di attività a rischio-reato nonché da collaboratori esterni e Partners, è fatto **espresso divieto** di tenere i seguenti comportamenti:

- dipendenti, collaboratori, consulenti e partner non devono porre in essere comportamenti che possano generare, anche solo potenzialmente, fattispecie di reato ai sensi del D.Lgs. 231/01;
- dipendenti, collaboratori, consulenti e partner devono evitare il determinarsi di qualsiasi situazione di conflitto d'interessi nei confronti della PA;
- in sede di trattativa d'affari o rapporto con la PA, dipendenti, collaboratori, consulenti e partner non devono tentare d'influenzare impropriamente le decisioni della controparte, ivi comprese quelle dei funzionari che trattano o prendono decisioni per conto della PA;
- i rapporti con la PA devono essere gestiti in modo unitario, nel senso che coloro che rappresentano l'Azienda nei confronti della PA devono ricevere un esplicito mandato;
- non sono ammesse pratiche di corruzione attiva o passiva o comportamenti collusivi di qualsiasi natura e sotto qualsiasi forma;
- non è consentito offrire denaro o compiere atti di cortesia commerciale (omaggi o forme d'ospitalità) a dirigenti, funzionari o dipendenti della PA o loro parenti, salvo che si tratti d'utilità d'uso di modico valore, che non possono essere in alcun modo interpretate come strumento per ricevere favori illegittimi;
- è proibito effettuare pagamenti, anche indiretti, a funzionari pubblici e a terzi in genere per ottenere trattamenti più favorevoli od influenzare un atto d'ufficio a determinare favori illegittimi (si considerano atti di corruzione sia i pagamenti illeciti ad enti o a loro dipendenti sia pagamenti effettuati tramite persone che agiscono per conto di tali enti); è vietato promettere opportunità d'impiego, vantaggi o altre utilità;
- nessun tipo di pagamento può esser effettuato in cash o in natura;
- le dichiarazioni rese a organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere rilasciato apposito rendiconto;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità.
- in sede di trattativa d'affari o rapporto con la PA, il personale incaricato non deve cercare d'influenzare impropriamente le decisioni della controparte, comprese quelle dei funzionari che trattano o prendono decisioni per conto della PA;
- nel caso specifico di gare con la PA si dovrà operare nel rispetto della legge e della corretta pratica commerciale;
- l'Azienda non dovrà farsi rappresentare, nei confronti della PA, da un consulente o da soggetto terzo, quando possono generarsi conflitti d'interesse;
- i compensi dei consulenti e dei partner devono essere determinati per iscritto;
- devono essere rispettati, da parte degli amministratori, i principi di trasparenza nell'assunzione di decisioni aziendali di rilevanza per i soci e terzi;
- devono essere adottate e rispettate apposite procedure che consentano l'esercizio del controllo da parte dei soci, organi sociali, società di revisione, e l'accesso rapido alle informazioni attribuite da leggi o regolamenti.
- per quanto concerne specificamente i rapporti con l'Autorità giudiziaria – considerata a tal fine quale parte della PA – che vedano coinvolti esponenti aziendali o altri destinatari (in relazione alle attività svolte per la società) è fatto obbligo ad ogni destinatario di non porre in essere atti di violenza, minaccia (o altre forme analoghe di coartazione) ovvero di non dare o di non promettere elargizioni in danaro o altre forme di utilità affinché il soggetto indagato/imputato:

- non presti una fattiva collaborazione al fine di rendere dichiarazioni veritiere, trasparenti e correttamente rappresentative dei fatti;
- 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

Lo svolgimento di attività a rischio con riferimento ai reati sopra richiamati nei rapporti con la Pubblica Amministrazione, di cui agli artt. 24 e 25 del Decreto deve essere debitamente documentata onde garantirne l'evidenza e trasparenza (v. allegata procedura).
L'OdV potrà predisporre rispetto alla procedura allegata ulteriori meccanismi di controllo per monitorare l'operazione in questione. Di tali ulteriori meccanismi di controllo verrà data evidenza scritta.

COMPITI DELL'ODV IN RIFERIMENTO ALLE ATTIVITÀ CON LA PA

E' compito dell'OdV:

a) Curare l'emanazione e l'aggiornamento di istruzioni standardizzate relative alle Attività delle aree "a rischio reato" ed, in genere, nei rapporti da tenere con la PA e ai limiti entro i quali non è necessaria l'utilizzazione di alcune voci del Modulo di Evidenza di cui alla citata procedura. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;

b) Verificare periodicamente – con il supporto delle altre funzioni competenti – il sistema di deleghe in vigore, raccomandando modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al responsabile dell'area;

c) Verificare periodicamente - con il supporto delle altre funzioni competenti - la validità d'opportune clausole standard finalizzate:
- all'osservanza da parte dei Collaboratori esterni e dei partner delle disposizioni del Decreto;
- alla possibilità di ENERCOM di effettuare efficaci azioni di controllo nei confronti dei "Destinatari" al fine di verificare il rispetto delle prescrizioni in esso contenute;
- all'attuazione di meccanismi sanzionatori (quali il recesso o la risoluzione dal contratto nei riguardi di Partner o di Collaboratori esterni) qualora si accertino violazioni delle prescrizioni;

d) Indicare al management le eventuali integrazioni ai sistemi di gestione finanziaria già presenti in ENERCOM, con l'evidenza degli accorgimenti opportuni a rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto

e) Esaminare eventuali segnalazioni provenienti dagli organi di controllo o da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute.

SANZIONI PER ILLECITI AMMINISTRATIVI

Le sanzioni per illeciti amministrativi sono indicate nel dettaglio alla Sezione II del D.Lgs. 231/01. Qui sono riportati gli art. 9 (Sanzioni amministrative) e art. 10 (Sanzione amministrativa pecuniaria).

Art. 9_Sanzioni amministrative

Le sanzioni per gli illeciti amministrativi dipendenti da reato sono:

a) la sanzione pecuniaria;
b) le sanzioni interdittive;
c) la confisca;
d) la pubblicazione della sentenza.

Le sanzioni interdittive sono:

a) l'interdizione dall'esercizio dell'attività;
b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
e) il divieto di pubblicizzare beni o servizi.

Art. 10_Sanzione amministrativa pecuniaria

Per l'illecito amministrativo dipendente da reato si applica sempre la sanzione pecuniaria. La sanzione pecuniaria viene applicata per quote in un numero non inferiore a cento né superiore a mille. L'importo di una quota va da un minimo di lire cinquecentomila (€ 258,23) ad un massimo di lire tre milioni (€ 1.549,37). Non è ammesso il pagamento in misura ridotta.

Parte speciale 4

REATI SOCIETARI

I REATI SOCIETARI (art. 25-ter del Decreto)

Vengono qui di seguito brevemente descritti i reati contemplati ed indicati all'art. 25-ter del Decreto (di seguito i "Reati Societari"), riuniti, per maggior chiarezza, in cinque tipologie differenti.

1. FALSITA' IN COMUNICAZIONI, PROSPETTI E RELAZIONI

• **False comunicazioni sociali** (art. 2621 c.c.) e **False comunicazioni sociali in danno della società, dei soci o dei creditori** (art. 2622 c.c.)

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

Peraltro la punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5% o una variazione del patrimonio netto non superiore all'1%.

In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscano in misura non superiore al 10% da quella corretta.

L'ipotesi di reato di cui all'art. 2622 c.c. si configura invece nel caso in cui, nell'intento di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, vengano esposti nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero vengano omesse informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, cagionando un danno patrimoniale alla società, ai soci o ai creditori.

Le due ipotesi di reato di cui agli articoli 2621 e 2622 c.c., prevedono una condotta che coincide quasi totalmente e si differenziano solo per il verificarsi (art. 2622 c.c.) o meno (art. 2621 c.c.) di un danno patrimoniale alla società, ai soci o ai creditori.

Entrambi i suddetti reati si realizzano: a) tramite l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero b) mediante l'omissione nei medesimi documenti di informazioni, la cui comunicazione è imposta dalla legge, riguardo alla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene.

La condotta (commissiva od omissiva) sopra descritta deve essere realizzata con l'intenzione di ingannare i soci o il pubblico e deve inoltre risultare idonea a trarre in errore i destinatari delle indicate comunicazioni sociali, essendo in definitiva rivolta a conseguire un ingiusto profitto a beneficio dell'autore del reato ovvero di terzi.

Si deve altresì osservare che:

- le informazioni false o omesse devono essere tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene;
- la responsabilità sussiste anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi;
- il reato di cui all'articolo 2622 c.c. è punibile a querela di parte, salvo che sia commesso in danno dello Stato, di altri enti pubblici, dell'Unione Europea o che si tratti di società quotate, nel qual caso è prevista la procedibilità d'ufficio.

Soggetti attivi del reato sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori.

• **Falso in prospetto** (art. 173-bis TUF): consiste nell'esporre false informazioni ovvero nell'occultare dati o notizie all'interno dei prospetti (per tali intendendosi i documenti richiesti ai fini dell'offerta al pubblico di prodotti finanziari o dell'ammissione alla quotazione nei mercati regolamentati, ovvero da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio) secondo modalità idonee ad indurre in errore i destinatari dei prospetti stessi.

Si precisa che deve sussistere l'intenzione di ingannare i destinatari dei prospetti e la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto.

• **Omessa comunicazione del conflitto di interesse** (art. 2629-bis c.c.): consiste nella violazione degli obblighi previsti dall'art. 2391, 1° co. c.c. da parte dell'amministratore di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea (ovvero di altri soggetti sottoposti a vigilanza), se dalla predetta violazione siano derivati danni alla società o a terzi.

L'art. 2391, 1° co. c.c. impone agli amministratori delle società per azioni di dare notizia agli altri amministratori e al collegio sindacale di ogni interesse che, per conto proprio o di terzi, abbiano in una determinata operazione 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.

2. TUTELA PENALE DEL CAPITALE SOCIALE

• **Indebita restituzione dei conferimenti** (art. 2626 c.c.): 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. La legge, cioè, non ha inteso punire anche i soci beneficiari della restituzione o della liberazione, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

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

La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio vale ad estinguere il reato.

Soggetti attivi del reato sono gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della ripartizione degli utili o delle riserve, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

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

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.): 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.

Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Il reato è punibile a querela di parte.
Soggetti attivi del reato sono, anche in questo caso, gli amministratori.
• **Formazione fittizia del capitale** (art. 2632 c.c.): è integrata dalle seguenti condotte:
1. formazione o aumento in modo fittizio del capitale sociale, anche in parte, mediante attribuzione di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale;
2. sottoscrizione reciproca di azioni o quote;
3. sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono gli amministratori ed i soci conferenti.
• **Indebita ripartizione dei beni sociali da parte dei liquidatori** (art. 2633 c.c.): 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.
I reato è perseguibile a querela della persona offesa e il risarcimento del danno ai creditori prima del giudizio estingue il reato.
Soggetti attivi del reato sono esclusivamente i liquidatori.

3. TUTELA PENALE DEL REGOLARE FUNZIONAMENTO DELLA SOCIETA'
• **Impedito controllo** (art. 2625 c.c.): consiste nell'impedire od ostacolare, mediante occultamento di documenti o con altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali.
Per tali ipotesi è prevista una sanzione amministrativa pecuniaria.
Le sanzioni sono maggiorate (con reclusione fino ad 1 anno raddoppiata per le società con titoli quotati in mercati regolamentati italiani o di altro stato dell'Unione europea) qualora tale condotta abbia cagionato un danno ai soci. In tal caso il reato è punibile solo a querela di parte.
L'illecito può essere commesso esclusivamente dagli amministratori.
• **Illecita influenza sull'assemblea** (art. 2636 c.c.): 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 costruito come un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta criminosa.

4. TUTELA PENALE CONTRO LE FRODI
• **Aggiotaggio** (art. 2637 c.c.): consiste nel diffondere notizie false ovvero nel realizzare operazioni simulate o altri artifici, concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero nell'incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o gruppi bancari.
Anche questo è un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta criminosa.

5. TUTELA PENALE DELLE FUNZIONI DI VIGILANZA
• **Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di Vigilanza** (art. 2638 c.c.): può essere realizzato con due condotte distinte:
1. 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 mediante l'occultamento, con altri mezzi fraudolenti, in tutto o in parte, 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 o amministrati dalla società per conto di terzi;

2. 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 del reato sono gli amministratori, i direttori generali, il dirigente preposto alla redazione dei documenti contabili societari, i sindaci e i liquidatori.
La norma è posta a tutela delle funzioni di vigilanza e si distingue dunque dal reato comune previsto dall'art. 170- bis del TUF, non compreso nell'elenco di cui all'art. 25-ter del Decreto, che sanziona il comportamento di "chiunque", fuori dai casi previsti dall'art. 2638 c.c., ostacoli le funzioni di vigilanza attribuite alle diverse autorità pubbliche a ciò deputate. La figura di reato risponde all'esigenza di coordinare ed armonizzare le fattispecie riguardanti le numerose ipotesi, esistenti nella disciplina previgente, di falsità nelle comunicazioni agli organi di vigilanza, di ostacolo allo svolgimento delle funzioni, ovvero di omesse comunicazioni alle autorità medesime. Viene così completata secondo il legislatore la tutela penale dell'informazione societaria, in questo caso nella sua destinazione alle autorità di vigilanza settoriali (non solo Consob, Banca d'Italia, Isvap, COVIP, ma anche Autorità garante della concorrenza e del mercato, Garante della privacy, Autorità per le Garanzie nelle Comunicazioni, Autorità per la Vigilanza sui Contratti Pubblici di Lavori, Servizi e Forniture etc.).
In particolare per quanto riguarda ENERCOM, deve ritenersi che la norma in questione riguardi gli obblighi di comunicazione nei confronti dell'Autorità per l'Energia Elettrica e il Gas.

6. CORRUZIONE TRA PRIVATI
• **Corruzione tra privati** (art. 2635 comma 3 c.c.): per la relativa trattazione si rinvia alla successiva PARTE SPECIALE 4-BIS.

Per l'individuazione dei livelli di rischio di ciascun reato come sopra indicato, nell'ambito della specificità delle attività svolte da ENERCOM, (o l'esclusione dello stesso per le evidenti ragioni ivi riportate) si rimanda all'Analisi del Rischio allegata.

PRINCIPALI AREE DI ATTIVITÀ A RISCHIO-REATO

Le attività svolte da ENERCOM nelle aree potenzialmente a rischio sono regolate da norme e leggi in vigore e comportamenti volontari con riferimento a:

1. formazione del bilancio, delle relazioni, dei prospetti e delle comunicazioni sociali previste dalle leggi;
2. rapporto con i soci, le società di revisione, il collegio sindacale;
3. rapporti con le Autorità di vigilanza;
4. operazioni sul capitale e destinazione dell'utile;
5. emissione di comunicati stampa ed informazione al pubblico.

Le informazioni riguardanti l'andamento economico, patrimoniale e finanziario di ENERCOM sono definite attraverso il bilancio civilistico predisposto su base annuale. La struttura del documento è conforme alle normative vigenti ed è sottoposto alla certificazione da parte di una Società esterna di Revisione.

Le regole ed aspetti di controllo tengono in considerazione la rilevanza dei punti di contatto con la PA.

La presente Parte, oltre agli specifici principi di comportamento relativi alle aree di rischio sopra indicate, richiama i principi generali di comportamento previsti dal Codice Etico adottato da ENERCOM alla cui osservanza sono tenuti tutti gli amministratori e dipendenti dell'Azienda.

PRINCIPI GENERALI DI COMPORTAMENTO – REATI SOCIETARI

Ai "Destinatari" di questo capitolo amministratori, dirigenti e dipendenti che operano nelle aree di attività a rischio-reato nonché da collaboratori esterni e Partners, è fatto ***espresso obbligo*** di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria dell'Azienda (Elenco delle Procedure del Sistema Qualità e Sicurezza di ENERCOM negli Allegati);
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, al fine di garantire la tutela del patrimonio degli investitori, ponendo la massima attenzione ed accuratezza nell'acquisizione, elaborazione ed illustrazione dei dati e delle informazioni relative ai prodotti finanziari, necessarie per consentire agli investitori di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria dell'Azienda e sull'evoluzione della sua attività, nonché sui prodotti finanziari e relativi diritti;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale e di agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- assicurare il regolare funzionamento dell'Azienda e degli organi sociali, garantendo ed agevolando ogni forma di controllo sulla gestione sociale previsto dalla legge;
- 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 da queste intraprese.

COMPITI DELL'ODV – REATI SOCIETARI

I compiti dell'OdV, in questo caso, sono:

a) per quanto riguarda il bilancio e le altre comunicazioni sociali, in ragione del fatto che il bilancio di ENERCOM è certificato da una società di revisione, i compiti dell'OdV si limitano a:

- Monitoraggio dell'efficacia delle procedure interne e delle regole di corporate governance per la prevenzione dei reati di false comunicazioni sociali;
- Esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari;
- Verifica dell'effettiva indipendenza della Società di Revisione.

b)per quanto riguarda le altre attività a rischio:

- Verifiche periodiche sul rispetto delle procedure interne e delle regole di corporate governance;
- Esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

L'OdV deve riportare i risultati della propria attività di vigilanza e controllo in materia di reati societari con cadenza annuale al CdA.

SANZIONI PER I REATI SOCIETARI

Le sanzioni per i reati societari sono indicate all'art. 3 Responsabilità amministrativa delle società del DL 11 aprile 2002, n. 61.

Le sanzioni sono sanzioni pecuniarie e sono previste in entità diverse per ogni tipologia di reato richiamata nel Decreto Legge e vanno da un range minimo di cento-centotrenta quote a un range massimo di duecento-cinquecento quote (1 quota € 258,23). Se l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

Parte speciale 4-bis

Reati di

CORRUZIONE TRA PRIVATI

REATI DI CORRUZIONE TRA PRIVATI (art. 25-ter lettera s-bis del Decreto)

LA TIPOLOGIA DEL REATO

La l. 6 novembre 2012 n. 190 ha introdotto nel nostro ordinamento una serie di novità finalizzate ad implementare la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione. Tra queste, ai fini del presente Modello, interessa la nuova formulazione dell'art. 2635 c.c., oggi intitolato "Corruzione tra privati".

Tale norma dispone:

"*Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, che, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società, sono puniti con la reclusione da uno a tre anni.*

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

Chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste.

Le pene stabilite nei commi precedenti sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.

Si procede a querela della persona offesa, salvo che dal fatto derivi una distorsione della concorrenza nella acquisizione di beni o servizi."

La norma punisce la condotta degli **amministratori,** dei **direttori generali,** del **dirigente preposto alla redazione dei documenti contabili societari,** dei **sindaci e** dei **liquidatori o soggetti sottoposti alla direzione o alla vigilanza di questi che, a seguito della dazione o anche solo della promessa di denaro o di altra utilità, per sé o per altri, compiono o omettono atti in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando un danno alla società**.

Una delle principiali novità introdotte dal nuovo articolo 2635 c.c. consiste nel fatto che la stessa pena è prevista anche per il soggetto c.d. corruttore, ossia colui che dà o promette denaro o altre utilità.

Il reato di corruzione tra privati previsto all'art. 25-ter, lettera s-bis, si perfeziona solo quando un soggetto compie o promette in concreto atti in violazione dei propri obblighi e per la società ne derivi un nocumento.

L'art. 2635 c.c., benché intitolato "Corruzione tra privati", trova applicazione **solamente nei rapporti tra società**. La norma infatti punisce le condotte corruttive che arrechino un danno al patrimonio sociale, e punisce pertanto la corruzione **solamente nel caso in cui determini** appunto **un nocumento al patrimonio sociale**, e non invece la corruzione in quanto tale.

Sotto il profilo della responsabilità amministrativa degli enti, la l. 190/2012 ha aggiunto la lettera s-bis) all'art. 25 ter del Decreto, che a sua volta **richiama il comma 3** del nuovo art. 2635 c.c.. Tale disposizione fa riferimento alla **sanzione prevista per il corruttore**, ossia chi dà o promette denaro o altre utilità. In altre parole, l'unica ipotesi cui è stata estesa la responsabilità amministrativa degli enti è quella della società corruttrice, i cui amministratori, direttori generali, dirigente preposto alla redazione dei documenti contabili societari, sindaci, liquidatori, o soggetti sottoposti alla direzione o alla vigilanza di questi, pongono in essere atti corruttivi.

La **condotta perpetrata** dal soggetto agente non è più solo limitata alla **violazione degli obblighi inerenti al proprio ufficio ma** è stata estesa **anche** alla **violazione degli obblighi di fedeltà**. L'elemento psicologico è il dolo che deve riflettersi su tutti gli elementi costitutivi della fattispecie. E' quindi necessario che i concorrenti nel reato abbiano inteso la dazione o promessa in relazione al successivo compimento di un atto, nella

consapevolezza della sua contrarietà agli obblighi d'ufficio (o di fedeltà) e con la volontà, almeno a titolo di dolo eventuale, di cagionare danno alla società.
Inoltre, affinché il reato si realizzi non è solo necessario che la dazione o promessa di denaro o di altra utilità sia diretta al soggetto agente ma è ora anche previsto che il beneficiario possa essere un soggetto terzo. L'applicazione della norma é stata estesa anche ai collaboratori dei soggetti "apicali".
L'art. 1, comma 77, della L. 190/2012 prevede l'inserimento nell'art. 25 ter, comma I, del D.Lgs. n. 231/2001 di una lettera s-bis concernente "il delitto di corruzione tra privati, nei casi previsti dal terzo comma dell'art. 2635 del codice civile" stabilendo una sanzione amministrativa da 200 a 400 quote.
La responsabilità dell'ente incontra quindi due limiti: il primo deriva dal regime di procedibilità essendo l'accertamento dell'illecito amministrativo precluso qualora il **reato sia perseguibile a querela** ed essa non venga presentata (art. 37 D.Lgs. n. 231/2001); il secondo consiste nella rilevanza attribuita solo a situazioni di **corruzione attiva**.

PRINCIPALI AREE DI ATTIVITÀ A RISCHIO-REATO

In via di principio, sono da considerarsi potenzialmente esposte a rischio tutte quelle attività aziendali che comportano il relazionarsi, in nome e per conto della Società, e anche in via indiretta o mediata, con società terze nell'ambito di un rapporto di tipo commerciale.
Le potenziali aree a rischio per la commissione dei reati in questione sono quelle che riguardano i **rapporti tra ENERCOM e società terze** con cui questa entra in contatto nello svolgimento della propria attività aziendale, quali a titolo esemplificativo gli agenti, i concessionari, i depositari, i fornitori, i consulenti, ecc. Nell'ambito di tali rapporti si potrebbe infatti astrattamente ipotizzare, da parte di dipendenti di ENERCOM, la promessa di una qualche utilità in cambio di prestazioni o servizi a condizioni di maggior favore.
Si tratta, com'è di tutta evidenza, di un rischio immanente nell'attività qualsiasi tipo di società.
Sono inoltre da considerarsi a rischio tutte quelle attività che, da un lato, potrebbero portare alla creazione dell'utilità che costituisce, in via di estrema semplificazione, il risultato ultimo nonché il fine dell'attività corruttiva. Si tratta quindi di tutte le attività inerenti al c.d. ciclo attivo, quali, a titolo esemplificativo, la definizione del prezzo di offerta di un bene o di un servizio, la definizione delle condizioni e dei termini di pagamento, della scontistica e della definizione di eventuali risoluzioni transattive in caso di contestazioni.
Sotto diverso profilo e tenuto conto dell'attività svolta da ENERCOM, sono soprattutto da considerarsi potenzialmente esposte a rischio tutte quelle attività attraverso le quali sarebbe possibile costituire la provvista o i fondi necessari per illecite dazioni o promesse di denaro. Si tratta quindi di **tutte le attività relative al c.d. ciclo passivo**, quali, a titolo esemplificativo, gli acquisti di beni e servizi, l'affidamento di consulenze e altre prestazioni professionali, la gestione del magazzino.
Ne consegue che risultano soggette al rischio tutte le aeree aziendali che hanno contatti e rapporti con amministratori, direttori generali, dirigenti preposti alla redazioni di documenti contabili societari, sindaci e liquidatori o anche con coloro che sono sottoposti alla direzione e vigilanza di uno dei suddetti soggetti (es. Direzione Amministrazione e Finanza, Direzione Commerciale, Ufficio Fornitori e Acquisti della Direzione Operativa).

Possono costituire occasioni di reato i rapporti tra privati inerenti la:
- negoziazione/stipulazione e/o esecuzione di contratti/convenzioni con soggetti privati, ai quali si deve pervenire mediante procedure di selezione;
- gestione delle attività di acquisizione e/o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie;
- predisposizione di atti contabili o societari, dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere;
- in generale rapporti con soggetti privati finalizzati alla cessione di beni o servizi.

Benché l'art. 25 ter del D.Lgs. n. 231/2001 richiami esclusivamente la fattispecie delittuosa prevista al terzo comma dell'art. 2635 c.c., così da far ritenere che la responsabilità dell'ente sorga soltanto nell'ipotesi ivi prevista ("*Chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste*"), si evidenzia che il modello 231 adottato da ENERCOM considera come sensibili anche i seguenti processi:

1. **acquisti di beni e servizi**: le attività e processi sensibili in particolare riguarderebbero la negoziazione/stipulazione e/o esecuzione di contratti/convenzioni con soggetti privati, la predisposizione delle offerte tecnico-economiche, la predisposizione degli ordini di acquisto, la valutazione delle richieste di ordine poiché trattasi di processi che, per loro natura, possono astrattamente consentire sia la concretizzazione del vantaggio derivante dall'accordo corruttivo che, dall'altro verso, la formazione della provvista di denaro necessaria all'esecuzione dell'attività corruttiva.
2. **gestione della c.d. omaggistica e delle spese di rappresentanza**, poiché trattasi di processi che, per loro natura, possono astrattamente e ipoteticamente costituire contropartita di accordi corruttivi.

Pertanto ENERCOM, senza alcuna estensione della fattispecie del reato di corruzione tra privati, richiama l'attenzione dei destinatari a quanto già previsto in relazione a tali processi sensibili in sede di Codice Etico e nelle procedure collegate.

Il rischio di verificazione dei suddetti reati (delitti) è considerato medio, tenuto anche conto di come nella storia di ENERCOM non si sono verificati episodi di coinvolgimento di dipendenti per il reato ex art. 2635 c.c., anche prima della riforma del 2012, posti in essere nell'interesse della società ovvero a suo vantaggio.
Si ritiene pertanto che possano essere individuate quali misure di prevenzione efficaci e sufficienti l'osservanza dei principi e delle disposizioni adottate dal Codice Etico, la stretta osservanza delle regole dettate dalle procedure aziendali applicabili, unitamente ad una rigorosa applicazione da parte di ENERCOM del sistema disciplinare.

REGOLE DI COMPORTAMENTO E PRESCRIZIONI RELATIVE AI REATI NEI RAPPORTI CON I PRIVATI

Mediante il proprio Codice Etico ENERCOM ha da tempo adottato e implementato una serie di regole di condotta volte alla prevenzione di qualsiasi evento corruttivo, tanto sul lato attivo (sotto specie di offerta di denaro o altre utilità a fini illeciti), quanto su quello passivo (sotto specie di accettazione di denaro o altre utilità a fini illeciti).
La regola generale che deve guidare il comportamento di tutti i Destinatari della presente Parte Speciale, così come sopra individuati, è la seguente:

- **nessuno dei dipendenti o di quanti agiscano in nome e per conto di ENERCOM può offrire, promettere o dare elargizioni in denaro o altra utilità ad alcuno, così come non può richiedere, acconsentire o accettare di ricevere elargizioni in denaro o altra utilità da alcuno**.

Il principio è del resto sintetizzato anche nel Codice Etico, laddove si richiede a tutti i dipendenti e a tutti coloro che agiscono in nome e per conto della Società di rispettare tutte le leggi in vigore. La correttezza sul mercato e con i concorrenti è infatti principio cardine della policy aziendale: ENERCOM mira a prevalere sui propri concorrenti sulla base della qualità e della competitività dei servizi resi. Non è consentito tentare di raggiungere tale risultato ricorrendo ad altri mezzi, meno che mai se illeciti.
I destinatari del Modello, cioè tutti coloro che operano per e con ENERCOM, inclusi i componenti degli organi sociali e in particolare quelli che, a qualunque titolo, intrattengano rapporti con soggetti terzi di natura privata, per conto o nel suo interesse, devono seguire i principi di comportamento di carattere generale indicati di seguito.
In via generale occorre tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge, del Codice Etico e delle altre procedure interne ed è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, la fattispecie di reato prevista dall'art. 25 comma 3 del D.Lgs. 231/2001. È altresì

proibito porre in essere comportamenti che determinino situazioni di conflitto di interesse nei confronti dei rappresentanti di detti soggetti privati.
In particolare, coerentemente con il rispetto dei principi etici che da sempre hanno guidato l'agire di ENERCOM, vengono qui di seguito elencati divieti e obblighi di fare che devono essere osservati dal personale nei rapporti con i privati.
Nei confronti dei privati è fatto divieto di:

- promettere o effettuare erogazioni in denaro per finalità diverse da quelle commerciali e/o di servizio;
- distribuire omaggi e regali con l'obiettivo di acquisire trattamenti di favore nella conduzione di qualsiasi attività. In particolare, è vietata qualsiasi forma di regalo a dirigenti e dipendenti, o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per ENERCOM. Gli omaggi sono consentiti esclusivamente nella misura in cui siano di modico valore o in quanto diretti a promuovere iniziative di carattere benefico o culturale, o l'immagine istituzionale di ENERCOM e in ogni caso devono essere singolarmente autorizzate secondo le procedure aziendali. I regali offerti - salvo quelli di modico valore - devono essere documentati in modo adeguato per consentire le verifiche da parte dell'OdV;
- promettere o concedere vantaggi di qualsiasi natura (come, a titolo di esempio, promesse di assunzione) in favore dei rappresentanti dei privati, o di loro familiari, al fine di influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per ENERCOM;
- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine istituzionale di ENERCOM e comunque non conformi alle specifiche procedure;
- effettuare prestazioni o pagamenti o riconoscere compensi in favore di collaboratori, fornitori, consulenti, partner o altri soggetti terzi operanti per conto di ENERCOM, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi o in relazione al tipo di incarico da svolgere o alle prassi vigenti;
- favorire, nei processi di acquisto, collaboratori, fornitori, consulenti o altri soggetti terzi in quanto indicati da rappresentanti dei privati, come condizione per lo svolgimento di successive attività;
- fornire o promettere di rilasciare informazioni e/o documenti riservati.

I divieti sopra rappresentati con i rappresentanti dei soggetti privati si intendono estesi anche ai rapporti indiretti (attraverso parenti, affini e amici o persone che comunque godano di "gradimento politico").
È altresì fatto divieto di tenere una condotta ingannevole che possa falsare la valutazione tecnico-economica relativamente alle prestazioni o ai servizi forniti, od omettere informazioni dovute, al fine di orientare a proprio favore le decisioni dei privati.
È inoltre fatto obbligo ai destinatari del presente Modello di attenersi alle seguenti prescrizioni:

- in caso di tentata corruzione da parte di un dirigente, dipendente, collaboratore o consulente del soggetto privato, il soggetto interessato deve: (i) non dare seguito alla richiesta; (ii) fornire tempestivamente informativa al proprio referente interno, il quale deve attivare formale informativa verso l'OdV;
- in caso di conflitti di interesse che sorgano nell'ambito dei rapporti con soggetti privati, il soggetto interessato deve fornire tempestivamente informativa al proprio referente interno, il quale a sua volta deve attivare formale informativa verso l'OdV;
- in caso di dubbi circa la corretta attuazione dei principi etico-comportamentali di cui sopra nel corso dello svolgimento delle attività operative, il soggetto interessato deve interpellare senza ritardo i responsabili o i referenti interni di ENERCOM e richiedere un parere all'OdV.

Per quanto riguarda tutte le attività inerenti gli acquisti di beni e servizi, l'Azienda ha provveduto a:
- definire nell'organigramma aziendale le funzioni coinvolte con adeguata stratificazione dei poteri decisionali e autorizzativi e distinzione dei ruoli tra i soggetti che partecipano al processo (richiesta della fornitura, effettuazione dell'acquisto, certificazione dell'esecuzione dei servizi; effettuazione del pagamento);
- stabilire le modalità per acquisire, archiviare e protocollare adeguatamente tutta la documentazione inerente ogni singola operazione (preventivi, ordini, contratti, documenti di trasporto, fatture e relative autorizzazioni al pagamento);
- definire i criteri di selezione e qualifica dei fornitori basati sui requisiti di professionalità, affidabilità, economicità.

- stabilire le modalità per verificare adeguatamente la corrispondenza tra gli importi versati, la documentazione acquisita a supporto e le prestazioni effettivamente ricevute.

Con riferimento a tutte le attività inerenti la gestione della c.d. omaggistica e le spese di rappresentanza si segnala che:

- la gestione degli omaggi non pubblicitari da parte di terzi è procedurata e comunque i clienti vengono invitati da ENERCOM a non inviare omaggi di nessun tipo;
- gli omaggi a favore di terzi possono essere solo di natura simbolica o comunque in quanto diretti a promuovere iniziative di carattere benefico o culturale, o l'immagine istituzionale di ENERCOM e in ogni caso devono essere singolarmente autorizzate secondo le procedure aziendali;
- le spese di rappresentanza (pranzi di lavoro, buffet per convegni) sono di entità limitata, sono previste a budget o debitamente autorizzate dalla Direzione Generale.

In aggiunta a quanto sopra, è prevista la seguente serie di misure volte non soltanto a prevenire la corruzione, ma anche a garantire il rispetto degli standard etici fissati per ENERCOM e a tutelare la sua reputazione. In particolare:

- Localizzazione del risk assessment
  Si deve individuare il potenziale rischio di commissione del reato di cui alla presente parte speciale per ogni singola unità di attività. Una corretta e appropriata valutazione del rischio consente infatti di ridurlo in maniera efficace.
- Due Diligence
  A seconda del rischio di commissione del reato individuato su base locale e per singola unità di attività, si deve procedere ad una due diligence preventiva in ogni caso di assunzione di nuovi dipendenti o di designazione di nuovi responsabili o altri ulteriori soggetti terzi che operano o opereranno in nome e per conto di ENERCOM.
- Adeguata tenuta dei libri sociali
  La prevenzione del rischio di corruzione passa necessariamente attraverso un'adeguata e appropriata conservazione, gestione e registrazione dei libri sociali. È quindi necessario che i libri sociali riflettano tutte le transazioni poste in essere dalla Società.
- Effettivo controllo interno e monitoraggio
  ENERCOM ha adottato un sistema di controllo interno dei conti della Società in ottemperanza a quanto prescritto dalla Autorità per l'Energia Elettrica e il Gas; l'accesso ai conti della Società è consentito solo a soggetti muniti di apposita delega; vengono effettuate periodiche verifiche sulla corrispondenza tra i beni effettivi della Società e quelli indicati nei libri sociali.
- Diffusione
  Una versione aggiornata del Modello di Organizzazione, Gestione e Controllo contenente i riferimenti alla normativa sulla Corruzione tra privati viene divulgata da ENERCOM a tutti i dipendenti e collaboratori tramite pubblicazione sul sito aziendale e affissione nelle bacheche delle sedi aziendali.

In relazione ad alcune fattispecie che più facilmente potrebbero agevolare la commissione di atti corruttivi, si dettano le seguenti regole di condotta che dipendenti e terzi che agiscono in nome e per conto di ENERCOM sono tenuti ad adottare.

(i) Fornitori

I fornitori hanno l'obbligo di rispettare i principi etici e le regole di comportamento adottati da ENERCOM e sintetizzati nella presente Parte Speciale e nel Codice Etico.

I processi di selezione dei fornitori e le regole per l'approvvigionamento delle merci sono fissate da ENERCOM con apposite procedure, che prevedono espressamente la ripartizione dei ruoli nella scelta dei fornitori, nel monitoraggio sul rispetto, da parte di questi, degli standard fissati dalla Società, nella formulazione degli ordinativi di merci e nella verifica sulle consegne e i pagamenti. Sono quindi analiticamente regolati i processi di gestione dei fornitori, il controllo degli approvvigionamenti e la gestione e verifica del magazzino.

(ii) Consulenti

La Società predilige avvalersi prevalentemente delle prestazioni di consulenti con cui sussiste un rapporto di lungo corso, in ragione del particolare vincolo di fiducia che deve sussistere con gli stessi.
ENERCOM provvede comunque alla verifica periodica circa la conservazione, nel tempo, dei necessari requisiti di correttezza e professionalità dei consulenti incaricati.
Identiche verifiche vengono compiute in caso di affidamento di incarichi a nuovi consulenti, con i quali ENERCOM non abbia in precedenza intrattenuto alcun rapporto.

(iii) Organizzazione di eventi di intrattenimento e di marketing

È consentita l'organizzazione di eventi di intrattenimento a condizione che siano connessi con la presentazione o con la promozione di un prodotto o servizio.
Allo stesso modo, è consentita la distribuzione di prodotti promozionali o di marketing ai clienti della Società, a condizione che i prodotti promozionali consegnati siano di quantità e importo ragionevoli e comunque sempre connessi al business aziendale. È altresì consentita l'organizzazione di eventi promozionali, a condizione che gli stessi siano indirizzati e coinvolgano la totalità dei possibili destinatari e non invece singoli e specifici soggetti selezionati.

(iv) Omaggi

Come già evidenziato, è vietata qualsiasi forma di regalo a controparti commerciali o a loro familiari o a persone che intrattengono con questi stretti rapporti personali, se non si caratterizzano per l'esiguità del valore o non sono volti a promuovere iniziative di carattere culturale o artistico, o ancora se non sono tesi a promuovere l'attività aziendale.
In ogni caso, i regali e gli omaggi sono sempre preventivamente approvati da ENERCOM. I regali offerti - con la sola eccezione di quelli di modico valore - devono essere documentati in modo adeguato per consentire le prescritte e necessarie verifiche.

COMPITI DELL'ODV – REATI DI CORRUZIONE TRA PRIVATI

I compiti dell'OdV, in questo caso, sono:

- Verifiche periodiche sul rispetto delle procedure interne;
- Esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

L'OdV deve riportare i risultati della propria attività di vigilanza e controllo in materia di reati ci corruzione tra privati con cadenza annuale al CdA.

SANZIONI PER I REATI DI CORRUZIONE TRA PRIVATI

Le sanzioni per i reati di corruzione tra privati sono unicamente sanzioni pecuniarie e vanno da un range minimo di 200 quote a un range massimo di 400 quote.
Se, in seguito alla commissione del reato, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

Parte speciale 5

TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

SALUTE E SICUREZZA – VIOLAZIONE DI NORME ANTINFORTUNISTICHE

La legge 3 agosto 2007 n.123 ha modificato il D.Lgs. n. 231/01 introducendo l'art. 25-septies, avente ad oggetto l'"omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro", che è stato successivamente modificato dal D.Lgs. 9 aprile 2008 n. 81. Tale articolo richiama le fattispecie di cui agli artt. 589 e 590 comma 3 del codice penale, con particolare riferimento alla violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute dei lavoratori.

In particolare:

1) con riferimento all'art. 589 c.p. (*Omicidio colposo*), qualora dalla violazione di norme antinfortunistiche derivi la morte di un lavoratore, il datore di lavoro (insieme eventualmente ad altri soggetti) può essere chiamato a rispondere a titolo di colpa per il mancato rispetto delle stesse.

2) con riferimento all'art. 590 c.p. (*Lesioni personali colpose*), qualora dalla violazione di norme antinfortunistiche derivino lesioni in danno di un lavoratore, il datore di lavoro (insieme eventualmente ad altri soggetti) può essere chiamato a rispondere a titolo di colpa per il mancato rispetto delle stesse.

Le fattispecie introdotte dalla L. 123/07 e modificate dal D.Lgs. 81/08 rappresentano reati di tipo colposo. *La responsabilità colposa*, in considerazione degli artt. 40 e 43 c.p., *attiene a quei soggetti che, pur non avendo voluto l'evento delittuoso, avevano l'obbligo giuridico di impedirlo mediante il rispetto di determinate norme di comportamento.*
In materia di norme antinfortunistiche e di tutela dell'igiene e della salute dei lavoratori l'"elusione fraudolenta" del modello organizzativo non rileva dunque quale esimente ai fini dell'esclusione della responsabilità amministrativa dell'ente.
Nei casi di reati di omicidio colposo e lesioni personali colpose commessi con violazione delle norme in materia di salute e sicurezza sul lavoro, la soglia concettuale di accettabilità, agli effetti esimenti del D.Lgs. n. 231/01, è infatti rappresentata dalla mera realizzazione di una condotta (non accompagnata dalla volontà dell'evento-morte/lesioni personali) violativa del modello organizzativo di prevenzione (e dei sottostanti adempimenti obbligatori prescritti dalle norme prevenzionistiche) nonostante la puntuale osservanza degli obblighi di vigilanza previsti dal D.Lgs. n. 231/01 da parte dell'apposito organismo (v. cap. III). Ciò in quanto l'elusione fraudolenta dei modelli organizzativi appare incompatibile con l'elemento soggettivo dei reati di omicidio colposo e lesioni personali colpose, di cui agli artt. 589 e 590 del codice penale, ovvero la colpa nella mancata osservanza di quanto previsto dalla normativa antinfortunistica.
Relativamente al rischio di comportamenti illeciti in materia di salute e sicurezza sul lavoro, il presente modello organizzativo non può dunque prescindere dalla vigente disciplina legislativa della prevenzione dei rischi lavorativi, che detta i principi e criteri essenziali per la gestione della salute e sicurezza sul lavoro in azienda, in particolare, del decreto legislativo n. 81/08 e successive modifiche. Tale complesso normativo costituisce un sistema di principi cogenti e adempimenti obbligatori la cui applicazione viene valutata idonea a ridurre ad un livello "accettabile", agli effetti esonerativi dello stesso D.Lgs. n. 231/01, le possibilità di condotte integranti gli estremi dei reati di omicidio o lesioni colpose gravi o gravissime commessi con violazione delle norme prevenzionistiche. La nozione di "accettabilità" in questione riguarda i rischi di condotte devianti dalle regole del modello organizzativo e non anche i sottostanti rischi lavorativi per la salute e la sicurezza dei lavoratori che, secondo i principi della vigente legislazione prevenzionistica, devono essere comunque integralmente eliminati in relazione alle conoscenze acquisite in base al progresso tecnico e, ove ciò non sia possibile, ridotti al minimo e, quindi, gestiti.

Di conseguenza ENERCOM, al fine di evitare l'accadimento di fatti integranti le fattispecie di reato indicate, impone a tutti i soggetti destinatari del Modello 231 il rispetto:

- della normativa vigente in materia di salute e sicurezza nei luoghi di lavoro

- della disciplina interna in materia di protezione e prevenzione dei rischi per i lavoratori

VALUTAZIONE DEI RISCHI NEI LUOGHI DI LAVORO

Riguardo al rischio di comportamenti integranti i reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme di salute e sicurezza sul lavoro, l'analisi si estende necessariamente alla totalità delle aree/attività aziendali, dovendo prendere in esame tutti i luoghi di svolgimento dell'attività della società.

E' interesse primario di ENERCOM, il rispetto di tutte le norme esistenti in tema di salute e sicurezza al fine di prevenire eventi in danno dei lavoratori.

E' interesse di ENERCOM imporre a tutti i soggetti che svolgono attività alle dipendenze ovvero in nome e per conto della stessa il rispetto delle norme esistenti in materia di salute e sicurezza nei luoghi di lavoro nonché il rispetto della disciplina interna elaborata a tutela dei lavoratori.

E' dunque obbiettivo di questo capitolo che tutti i destinatari del Modello 231 adottino regole di condotta conformi a quanto prescritto dalla legge al fine di prevenire il verificarsi dei Reati individuati all'art. 25-septies del D.Lgs. 231/01.

ENERCOM coordina pertanto il Modello 231 con la disciplina interna in tema di salute e sicurezza nei luoghi di lavoro, mediante rinvio a tutti i documenti, le regole, le disposizioni e le procedure elaborate dall'azienda in tema di *"Salute e Sicurezza nei luoghi di lavoro"*, con riferimento alla normativa esistente ed in particolare al D.Lgs. 81/08 e successive modifiche ed integrazioni (v. Elenco delle Procedure di ENERCOM negli Allegati).

In particolare sono richiamati:

1. Il Documento di Valutazione dei Rischi (DVR) ex artt. 17 e 28 D.Lgs. 81/08 emesso per ogni mansione aziendale.
2. Funzioni e compiti del Servizio di Prevenzione e Protezione e del Medico competente.
3. Le Regole per l'uso dei Dispositivi di Protezione Individuale.
4. Le Disposizioni in tema di sicurezza individuate per ciascuna mansione.
5. Le disposizioni relative all'uso delle attrezzature di lavoro e/o ai comportamenti da tenersi in caso di rapina o aggressione
6. Le disposizioni in tema di prevenzione degli incendi, di evacuazione dei lavoratori, di pronto soccorso.

Ogni violazione delle suddette norme e regolamenti sarà oggetto di valutazione ed eventuale sanzione da parte dell'Azienda, a prescindere da qualsiasi rilevanza penale dei comportamenti posti in essere.

COMPITI DELL'ODV_ SALUTE E SICUREZZA DEI LAVORATORI

E' compito dell'OdV:

a) Assicurare un sistema aziendale per l'effettuazione delle attività relative all'adempimento degli obblighi di legge in materia di salute e sicurezza sul lavoro;

b)Assicurare che la verifica, la valutazione, la gestione ed il controllo del rischio siano effettuate attraverso competenze tecniche e poteri necessari;

c) Assicurare l'emanazione e l'aggiornamento di istruzioni standardizzate relative alle Attività nelle aree "a rischio" per la sicurezza e la salute dei lavoratori;

d)Assicurare la tracciabilità di tutte le attività in applicazione al sistema aziendale in materia di sicurezza e la salute dei lavoratori;

e) Assicurare le attività di informazione e formazione del personale sui temi di salute e sicurezza nei luoghi di lavoro,

f) Effettuare periodicamente audit in tema di salute e sicurezza dei lavoratori;

g)Sanzionare la violazione di norme antinfortunistiche e tutela dell'igiene e della salute nei luoghi di lavoro.

SANZIONI PER VIOLAZIONE DI NORME ANTINFORTUNISTICHE

Le sanzioni per le violazioni relative a questo capitolo, sono dettagliate nel D.Lgs. n. 81/08 che prevede sanzioni, tra gli altri, a carico:

1. del datore di lavoro e il dirigente,
2. del preposto (persona che sovrintende alla attività lavorativa e garantisce l'attuazione delle direttive ricevute)
3. del medico competente;
4. del lavoratore.

All'art. 300 il D.Lgs. n. 81/08 introduce modifiche al decreto legislativo 8 giugno 2001, n. 231 e prevede:

In relazione al delitto di "*Omicidio colposo*" (art. 589 c.p.) commesso in violazione delle norme di sicurezza, ma solo per la violazione dell'art. 55 comma 2 (omessa valutazione dei rischi) si applica una sanzione pecuniaria in misura pari a 1.000 quote (1 quota € 258,23 quindi € 258.230) e sanzioni interdittive per una durata non inferiore a tre mesi e non superiore ad un anno.

In tutti gli altri casi si applica una sanzione pecuniaria in misura non inferiore a 250 quote e non superiore a 500 quote e sanzioni interdittive per una durata non inferiore a tre mesi e non superiore ad un anno.

In relazione al delitto di "*Lesioni gravi e gravissime*" (590, terzo comma, c.p.) commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non superiore a 250 quote e sanzioni interdittive per una durata non superiore a sei mesi.

Parte speciale 6

REATI INFORMATICI

E DELITTI IN VIOLAZIONE

DEL DIRITTO D'AUTORE

REATI INFORMATICI – TRATTAMENTO DEI DATI

DEFINIZIONI
Ai fini della presente parte speciale, si indicano le seguenti definizioni:
Credenziali: l'insieme degli elementi identificativi di un utente o di un account (generalmente User ID e Password).
Dati Informatici: qualunque rappresentazione di fatti, informazioni, o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione.
Delitti in Violazione del Diritto d'Autore: i reati di cui all'art. 25-nonies del Decreto.
Delitti Informatici: i reati di cui all'art. 24-bis del Decreto.
Documento/i Informatico/i: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Firma Elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
L.A. o Legge sul Diritto d'Autore: Legge 22 aprile 1941 n. 633 sul diritto d'autore.
Password: sequenza di caratteri alfanumerici o speciali necessaria per autenticarsi ad un sistema informatico o ad un programma applicativo.
Peer to Peer: meccanismo di condivisione di contenuti digitali tramite una rete di personal computer, di regola utilizzati per scambio di file con contenuti audio, video, dati e software.
Piano di Sicurezza: documento che definisce un insieme di attività coordinate che devono essere intraprese per implementare la politica di sicurezza del sistema.
Postazione di Lavoro: postazione informatica aziendale fissa oppure mobile in grado di trattare informazioni aziendali.
Sicurezza Informatica: l'insieme delle misure organizzative, operative e tecnologiche finalizzate a salvaguardare i trattamenti delle informazioni effettuati mediante strumenti elettronici.
Sistemi Informativi: l'insieme della rete, dei sistemi, dei data base e delle applicazioni aziendali.
Spamming: invio di numerosi messaggi indesiderati, di regola attuato attraverso l'utilizzo della posta elettronica.
Virus: programma creato a scopo di sabotaggio o vandalismo, in grado di alterare il funzionamento di risorse informatiche, di distruggere i dati memorizzati, nonché di propagarsi tramite supporti rimovibili o reti di comunicazione.

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI E DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE
Si trattano qui unitamente i reati contemplati dagli artt. 24-bis e 25-nonies del Decreto, in quanto:
- entrambe le fattispecie presuppongono un corretto utilizzo delle risorse informatiche;
- le aree di rischio risultano, in virtù di tale circostanza, in parte sovrapponibili;
- i principi procedurali mirano, in entrambi i casi, a garantire la sensibilizzazione dei destinatari in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

LE TIPOLOGIE DI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (art. 24-bis del Decreto)

• **Falsità in documenti informatici** (art. 491-bis c.p.): tutti i delitti relativi alla falsità in atti disciplinati dal codice penale (cfr. Capo III, Titolo VII, Libro II), tra cui sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico, pubblico o privato, avente efficacia probatoria (in quanto rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti).
In particolare, si precisa che si ha "falsità materiale" quando un documento viene formato o sottoscritto da persona diversa da quella indicata come mittente o sottoscrittore, con divergenza tra autore apparente e autore

reale del documento (contraffazione) ovvero quando il documento è artefatto (e, quindi, alterato) per mezzo di aggiunte o cancellazioni successive alla sua formazione.
Si ha, invece, "falsità ideologica" quando un documento non è veritiero nel senso che, pur non essendo né contraffatto né alterato, contiene dichiarazioni non vere. Nel falso ideologico, dunque, è lo stesso autore del documento che attesta fatti non rispondenti al vero.
I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali.
A titolo esemplificativo, integra il delitto di falsità in documenti informatici la condotta di chi falsifichi documenti aziendali oggetto di flussi informatizzati o la condotta di chi alteri informazioni a valenza probatoria presenti sui propri sistemi allo scopo di eliminare dati considerati "sensibili" in vista di una
possibile attività ispettiva.

- **Accesso abusivo ad un sistema informatico o telematico** (art. 615-ter c.p.): si realizza quando un soggetto si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza.

Il legislatore intende punire l'accesso abusivo ad un sistema informatico o telematico tout court, e dunque anche quando ad esempio all'accesso non segua un vero e proprio danneggiamento di dati: si pensi all'ipotesi in cui un soggetto acceda abusivamente ad un sistema informatico e proceda alla stampa di un documento contenuto nell'archivio del personal computer altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura).
Il reato si realizza altresì nell'ipotesi in cui il soggetto agente, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema, nonché, secondo il prevalente orientamento giurisprudenziale, qualora il medesimo abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.
Il delitto potrebbe pertanto essere astrattamente configurabile nell'ipotesi in cui un soggetto acceda abusivamente ai sistemi informatici di proprietà di terzi (outsider hacking), per prendere cognizione di dati riservati altrui nell'ambito di una negoziazione commerciale, o acceda abusivamente ai sistemi aziendali della società per acquisire informazioni alle quali non avrebbe legittimo accesso in vista del compimento di atti ulteriori nell'interesse della società stessa.

- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici** (art. 615-quater c.p.): si realizza qualora un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso di un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee a raggiungere tale scopo.

L'art. 615-quater c.p., pertanto, punisce le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.
I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche (quali badge o smart card).
Tale fattispecie si configura sia nel caso in cui il soggetto, in possesso legittimamente dei dispositivi di cui sopra (ad esempio, un operatore di sistema), li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi.
L'art. 615-quater c.p., inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.
Potrebbe rispondere del delitto, ad esempio, il dipendente della società che comunichi ad un altro soggetto la password di accesso alle caselle e-mail di un proprio collega, allo scopo di garantirgli la possibilità di controllare le attività svolte da quest'ultimo, quando da ciò possa derivare un determinato vantaggio o interesse per la società.

- **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico** (art. 615-quinquies c.p.): si realizza qualora qualcuno, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti, o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo

funzionamento, si procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici.
Tale delitto potrebbe, ad esempio, configurarsi qualora un dipendente si procuri un virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico aziendale in modo da distruggere documenti "sensibili" in relazione ad un procedimento penale a carico della società.
• **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche** (art. 617-quater c.p.): si configura qualora un soggetto fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisca o interrompa tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione.
Attraverso tecniche di intercettazione è infatti possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.
Il reato potrebbe configurarsi, ad esempio, con vantaggio concreto della società, nel caso in cui un dipendente impedisca una determinata comunicazione in via informatica al fine di evitare che un'impresa concorrente trasmetta i dati e/o l'offerta per la partecipazione ad una gara.
• **Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche** (art. 617-quinquies c.p.): si realizza quando un soggetto, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.
La condotta vietata è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, essendo sufficiente che le stesse abbiano una potenzialità lesiva.
Il reato si integra, ad esempio, a vantaggio della società, nel caso in cui un dipendente si introduca fraudolentemente presso la sede di una potenziale controparte commerciale al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche rilevanti in relazione ad una futura negoziazione.
• **Danneggiamento di informazioni, dati e programmi informatici** (art. 635-bis c.p.): si realizza quando un soggetto distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui.
Il danneggiamento potrebbe essere commesso a vantaggio della società laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte di un fornitore della società o al fine di contestare il corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell'ipotesi in cui vengano danneggiati dei dati aziendali "compromettenti".
• **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.): si realizza quando un soggetto commetta 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.
Si distingue dalla precedente figura di delitto poiché il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati al soddisfacimento di un interesse di natura pubblica.
Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora un dipendente compia atti diretti a distruggere documenti informatici aventi efficacia probatoria registrati presso enti pubblici (es. polizia giudiziaria) relativi ad un procedimento penale a carico della società.
• **Danneggiamento di sistemi informatici o telematici** (art. 635-quater c.p.): si realizza quando un soggetto mediante le condotte di cui all'art. 635-bis c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

Pertanto qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635-bis c.p..

- **Danneggiamento di sistemi informatici o telematici di pubblica utilità** (art. 635-quinquies c.p.): si configura quando la condotta di cui al precedente art. 635-quater c.p. è diretta a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

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

È bene tenere presente che in ogni caso la commissione di uno dei delitti informatici sopra descritti assume rilevanza, per le finalità di cui al Decreto, solo qualora la condotta, indipendentemente dalla natura aziendale o meno del dato/informazioni/programma/sistema informatico o telematico, possa determinare un interesse o vantaggio per ENERCOM.

Le sanzioni applicabili all'Ente nell'ipotesi di commissione dei delitti informatici possono essere di natura pecuniaria, da 100 a 500 quote (le stesse possono variare da un minimo di circa Euro 26.000 ad un massimo di circa Euro 800.000) e di natura interdittiva, che variano a seconda della fattispecie criminosa realizzata.

LE TIPOLOGIE DI DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE (art. 25-nonies del Decreto)

L'art. 25-novies contempla alcuni reati previsti dalla Legge sul Diritto d'Autore (e, in particolare, dagli artt. 171, 171-bis, 171-ter, 171-septies e 171-octies) quali, ad esempio, l'importazione, la distribuzione, la vendita o la detenzione a scopo commerciale o imprenditoriale di programmi contenuti in supporti non contrassegnati dalla SIAE; la riproduzione o il reimpiego del contenuto di banche dati; l'abusiva duplicazione, la riproduzione, la trasmissione o la diffusione in pubblico, di opere dell'ingegno destinate al circuito televisivo o cinematografico; l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa.

Da un'analisi preliminare è emersa l'immediata inapplicabilità alla società delle fattispecie di cui agli artt. 171-ter, 171-septies e 171-octies L.A.

Si provvede pertanto a fornire qui di seguito una breve descrizione delle due fattispecie di cui all'art. 25-nonies del Decreto ritenute prima facie rilevanti per la società, previste dagli artt. 171 comma 1 lett. a bis e comma 3, e 171 bis L.A.

- **Protezione del diritto d'autore e di altri diritti connessi al suo esercizio** (art. 171 co. 1 lett. a-bis e co. 3 L.A.): il Decreto prende in considerazione esclusivamente due fattispecie, ovvero: (i) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno protetta o di parte di essa; e (ii) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Nella prima ipotesi ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere lese le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete, nella seconda ipotesi il bene giuridico protetto non è, evidentemente, l'aspettativa di guadagno del titolare dell'opera, ma il suo onore e la sua reputazione.

Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora venissero caricati sul sito internet aziendale dei contenuti coperti dal diritto d'autore.

- **Protezione del diritto d'autore e di altri diritti connessi al suo esercizio** (art. 171 bis L.A.): la norma in esame è volta a tutelare il corretto utilizzo dei software e delle banche dati.

Per i software, è prevista la rilevanza penale dell'abusiva duplicazione nonché dell'importazione, distribuzione, vendita e detenzione a scopo commerciale o imprenditoriale e locazione di programmi "pirata".
Il reato in ipotesi si configura nel caso in cui chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla SIAE.
Il fatto è punito anche se la condotta ha ad oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.
Il secondo comma punisce inoltre chiunque, 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 ovvero esegue l'estrazione o il reimpiego della banca di dati ovvero distribuisce, vende o concede in locazione una banca di dati.
Sul piano soggettivo, per la configurabilità del reato è sufficiente lo scopo di lucro, sicché assumono rilevanza penale anche tutti quei comportamenti non sorretti dallo specifico scopo di conseguire un guadagno di tipo prettamente economico (come nell'ipotesi dello scopo di profitto).
Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora venissero utilizzati, per scopi lavorativi, programmi non originali ai fine di risparmiare il costo derivante dalla licenza per l'utilizzo di un software originale.

Le sanzioni applicabili all'Ente nell'ipotesi di commissione dei delitti in violazione del diritto d'autore possono essere di natura pecuniaria fino a 500 quote (e dunque fino ad un massimo di circa Euro 800.000) e di natura interdittiva, quali l'interdizione dall'esercizio dell'attività o la sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito per una durata non superiore ad un anno.

AREE A RISCHIO E ATTIVITÀ SENSIBILI

Le attività sensibili individuate per l'attività di ENERCOM, in riferimento ai Reati Informatici richiamati dall'art. 24-bis e dall'art. 25-novies unicamente per quanto attiene la non corretta diffusione di opere dell'ingegno protette e la non corretta diffusione o riproduzione di banche dati, sono le seguenti:

- Gestione e monitoraggio degli accessi ai sistemi informatici e telematici, nell'ambito della quale sono ricomprese le attività di:

  1. gestione del profilo utente e del processo di autenticazione;
  2. gestione del profilo utente autorizzato con accesso a informazioni commerciali sensibili;
  3. definizione delle condizioni di neutralità nella gestione delle infrastrutture aziendali;
  4. gestione e protezione della postazione di lavoro;
  5. gestione degli accessi verso l'esterno e verso altre società del gruppo;
  6. gestione e protezione delle reti da possibili intrusioni e da attacchi esterni;
  7. gestione degli output di sistema e dei dispositivi di memorizzazione;
  8. gestione della sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.);
  9. gestione degli applicativi in uso in azienda e relativi aggiornamenti.

- Tutte le attività aziendali svolte dai Destinatari tramite l'utilizzo dei Sistemi Informativi aziendali, del servizio di posta elettronica e dell'accesso ad Internet;
- Gestione dei Sistemi Informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT nonché la Sicurezza Informatica;
- Gestione dei flussi informativi elettronici con la pubblica amministrazione;
- Utilizzo di software e banche dati;

- Gestione dei contenuti del sito Internet.

ATTIVITÀ DI CONTROLLO NELLE AREE SENSIBILI

ENERCOM ha definito le policy aziendali, i principi generali di utilizzo, le regole di comportamento e di controllo riferiti agli strumenti informatici ed alle metodologie utilizzate che si sintetizzano nei seguenti punti:

Segregazione delle attività: è applicato il principio di separazione delle attività tra chi esegue, chi autorizza e chi controlla. Per tutte le attività gestite in ambito informatico sono stati creati profili di accesso ai diversi sistemi informativi in relazione alla mansione dell'utente ed ai compiti assegnati allo stesso.

Definizione di procedure/norme/regole: sono state definite disposizioni aziendali e procedure formalizzate per le attività informatiche e per la gestione dei dati idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività, per la sicurezza e riservatezza dei dati nonché modalità di archiviazione della documentazione e delle registrazioni rilevanti (Elenco delle Procedure del Sistema Qualità di ENERCOM negli Allegati).

Tracciabilità: Sono disciplinati i casi e le modalità della possibile cancellazione o distruzione di registrazioni effettuate su supporto informatico.

ENERCOM ha definito regole e procedure aziendali per prevenire la commissione di reati per mezzo di proprie infrastrutture con:

- L'attribuzione delle responsabilità e le autorizzazioni agli accessi;
- La gestione del rischio informatico riferito a: infrastrutture, hardware, software, documentazione, dati/informazioni, risorse umane;
- L'individuazione delle minacce, interne ed esterne, cui possono essere esposte le risorse con riferimento a: errori e malfunzionamenti, frodi e furti, danneggiamenti fisici, sovraccarico del sistema, mancato rispetto della legislazione vigente;
- L'applicazione di misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute.
- L'attuazione di un sistema che prevede la tracciabilità delle operazioni che possono influenzare la sicurezza dei dati critici.
- L'attuazione di attività di formazione e comunicazione relativa alla sicurezza e riservatezza dei dati volta a sensibilizzare tutto il personale dell'Azienda.

COMPITI DELL'ODV_ REATI INFORMATICI

E' compito dell'OdV o ente da questo delegato:

a) Assicurare un sistema aziendale di controllo dei sistemi informativi e di protezione dei dati aziendali e di gestione delle informazioni;

b) Assicurare che la verifica, la gestione ed il controllo dei sistemi informativi siano effettuati attraverso competenze tecniche e poteri necessari;

c) Assicurare l'emanazione e l'aggiornamento di istruzioni standardizzate relative alle Attività nelle aree "a rischio" per garantire la sicurezza e la protezione dei dati aziendali;

d) Assicurare le attività di informazione e formazione del personale sui temi di sicurezza e riservatezza dei dati aziendali;

e) Effettuare periodicamente audit in tema di rispetto delle regole aziendali dell'area dei sintemi informativi ed in particolare in tema di gestione dei dati.

SANZIONI PER VIOLAZIONE DI REATI INFORMATICI

Le sanzioni o pene per le violazioni relative a questo capitolo, sono dettagliate nelle leggi di riferimento art. 24-bis Legge 18 marzo 2008, n. 48 e art. 25-novies Legge 23 luglio 2009 n. 99 , art. 15 e prevedono:

- sanzioni pecuniarie di diversa entità in funzione della gravità del reato (da multe non inferiori a € 516 sino a quattrocento quote (una quota ha un valore minimo di € 258))
- sanzioni interdittive
- reclusione da uno a tre anni.

Parte speciale 7

REATI DI RICICLAGGIO

I C.D. REATI DI RICICLAGGIO (art. 25-octies)

Le figure di reato che vengono in rilievo in questa parte speciale sono state introdotte nel regime di responsabilità amministrativa ex D.Lgs. 231/01 dal D.Lgs. 231 del 2007, il c.d. "Decreto Antiriciclaggio" e vengono qui di seguito indicate e brevemente illustrate:

• **Ricettazione** (art. 648 c.p.): si configura nel caso in cui un soggetto, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta danaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farli acquistare, ricevere od occultare. È punita con la reclusione da 2 a 8 anni e con la multa da euro 516 a euro 10.329. La pena è diminuita quando il fatto è di particolare tenuità.
• **Riciclaggio** (art. 648-bis c.p.): si configura nel caso in cui un soggetto sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa. È punita con la reclusione da 4 a 12 anni e con la multa da euro 1.032 ad euro 15.493. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.
• **Impiego di denaro, beni o utilità di provenienza illecita** (art. 648-ter c.p.): si configura nel caso di impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto. È punita con la reclusione da 4 a 12 anni e la multa da euro 1.032 ad euro 15.493. La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.

La normativa italiana in tema di prevenzione dei Reati di Riciclaggio – in particolare il Decreto Antiriciclaggio – è rivolta ad ostacolare le pratiche di riciclaggio, vietando tra l'altro l'effettuazione di operazioni di trasferimento di importi rilevanti con strumenti anonimi e garantendo la ricostruibilità delle operazioni effettuate per mezzo dell'identificazione della clientela e della registrazione dei dati in appositi archivi.
Il Decreto Antiriciclaggio prevede i seguenti strumenti di contrasto del fenomeno del riciclaggio di proventi illeciti:
1. il divieto di trasferire denaro contante o libretti di deposito bancari o postali al portatore o di titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) in Euro o in valuta estera, a qualsiasi titolo tra soggetti diversi quando il valore dell'operazione è pari o superiori a Euro 5.000. Il trasferimento può tuttavia essere eseguito per il tramite di banche, istituti di moneta elettronica e Poste Italiane S.p.A.;
2. l'obbligo di adeguata verifica della clientela da parte di alcuni soggetti destinatari del Decreto Antiriciclaggio (elencati agli artt. 11, 12, 13 e 14 del Decreto Antiriciclaggio) in relazione ai rapporti e alle operazioni inerenti allo svolgimento dell'attività istituzionale o professionale degli stessi;
3. l'obbligo da parte di alcuni soggetti (elencati agli artt. 11, 12, 13 e 14 del Decreto Antiriciclaggio) di conservare, nei limiti previsti dall'art. 36 del Decreto Antiriciclaggio, i documenti o le copie degli stessi e registrare le informazioni acquisite per assolvere gli obblighi di adeguata verifica della clientela affinché possano essere utilizzati per qualsiasi indagine su eventuali operazioni di riciclaggio o di finanziamento del terrorismo o per corrispondenti analisi effettuate dall'UIF o da qualsiasi altra autorità competente;
4. l'obbligo di segnalazione da parte di alcuni soggetti (elencati agli artt. 10, comma 2, 11, 12, 13 e 14 del Decreto Antiriciclaggio) all'UIF, di tutte quelle operazioni, poste in essere dalla clientela, ritenute "sospette" o quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento al terrorismo.
I soggetti sottoposti agli obblighi di cui ai n. 2., 3., 4., sono:
1) gli intermediari finanziari e gli altri soggetti esercenti attività finanziaria. Tra tali soggetti figurano, ad esempio:
• banche;
• poste italiane;
• società di intermediazione mobiliare (SIM);

• società di gestione del risparmio (SGR);
• società di investimento a capitale variabile (SICAV).
2) I professionisti, tra i quali si indicano:
• i soggetti iscritti nell'albo dei ragionieri e periti commerciali;
• i notai e gli avvocati quando, in nome e per conto dei loro clienti, compiono qualsiasi operazione di natura finanziaria o immobiliare e quando assistono i loro clienti in determinate operazioni.
3) I revisori contabili.
4) Altri soggetti, intesi quali operatori che svolgono alcune attività il cui esercizio resta subordinato al possesso delle licenze, autorizzazioni, iscrizioni in albi o registri, ovvero alla preventiva dichiarazione di inizio di attività richieste dalle norme. Tra le attività si indicano:
• recupero di crediti per conto terzi;
• trasporto di denaro contante;
• gestione di case da gioco;
• offerta, attraverso internet, di giochi, scommesse o concorsi pronostici con vincite in denaro.
Stante dunque l'attività commerciale svolta, ENERCOM non rientra tra i soggetti destinatari del Decreto Antiriciclaggio; resta ad ogni modo la possibilità che esponenti della società, siano essi amministratori, dirigenti o dipendenti, commettano uno dei reati di riciclaggio.

L'art. 25-octies del Decreto potrebbe pertanto astrattamente trovare applicazione nei confronti di ENERCOM.

Per i reati di riciclaggio si applica la sanzione pecuniaria da 200 a 800 quote. Ove il denaro, i beni o le altre utilità provengano da delitto per cui è stabilita la pena della reclusione superiore nel massimo a 5 anni si applica la sanzione pecuniaria da 400 a 1000 quote. Considerato che l'importo di una quota può variare da circa Euro 258 a circa Euro 1.549, la sanzione pecuniaria può raggiungere la cifra di circa Euro 1,5 milioni. Per la commissione di tali reati si applicano inoltre le sanzioni interdittive previste dall'art. 9, comma 2, del Decreto, per una durata non superiore a 2 anni.

AREE A RISCHIO

In relazione ai reati sopra descritti, le aree valutate maggiormente a rischio risultano essere le seguenti:
1. rapporti con fornitori e partners;
2. flussi finanziari in entrata;
3. rapporti infragruppo;
Eventuali integrazioni delle suddette Aree a Rischio potranno essere disposte dal Presidente di ENERCOM, che ha mandato di individuare le relative ipotesi e definire gli opportuni provvedimenti operativi.

DESTINATARI DELLA PARTE SPECIALE E PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE

Obiettivo della presente Parte Speciale è che esponenti aziendali (amministratori, dirigenti o dipendenti), consulenti e partner, nella misura in cui possano essere coinvolti nello svolgimento di attività nelle aree a rischio, si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi dei reati di riciclaggio, pur tenendo conto della diversa posizione di ciascuno dei soggetti stessi nei confronti della società e, quindi, della diversità dei loro obblighi come specificati nel Modello.
Nell'espletamento di tutte le attività attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, gli esponenti aziendali – con riferimento alle operazioni di rispettiva competenza - devono in generale conoscere e rispettare tutte le regole, procedure e principi – da intendersi come attuativi ed integrativi del Modello - contenuti nei seguenti documenti, le cui modalità di approvazione e modifica rimangono quelle attualmente in vigore:

- il Codice Etico;
- il Regolamento interno per la qualificazione dei fornitori;
- la procedura aziendale che prevede l'analisi di tutti i soggetti che hanno rapporti con ENERCOM;
- ogni altra normativa interna relativa alla selezione e verifica delle controparti contrattuali;
- regole di corporate governance adottate dalla società.

Ai consulenti e ai Partners viene resa nota l'adozione del Modello e del Codice Etico da parte di ENERCOM, la cui conoscenza e il cui rispetto costituisce obbligo contrattuale a carico di tali soggetti.
In particolare, nell'espletamento delle attività considerate a rischio, gli esponenti aziendali, in via diretta, e i consulenti e i partner, tramite apposite clausole contrattuali, in relazione al tipo di rapporto in essere con ENERCOM, dovranno attenersi ai seguenti principi generali di condotta:
1. astenersi dal tenere condotte tali da integrare reati di riciclaggio;
2. astenersi dal tenere condotte che, pur non costituendo di per sé fattispecie di reato di riciclaggio, possano potenzialmente diventarlo;
3. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori/clienti/partners;
4. non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità, quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura;
5. non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
6. effettuare un costante monitoraggio dei flussi finanziari aziendali.

PRINCIPI PROCEDURALI SPECIFICI

Principi procedurali da osservare nelle singole operazioni a rischio
Con riferimento alle sopra individuate aree di rischio, vengono di seguito indicati i principi procedurali da implementarsi in specifiche procedure aziendali che gli esponenti aziendali sono tenuti a rispettare.

Con riferimento al rischio nei rapporti con fornitori e partners:
a) verificare l'attendibilità commerciale e professionale dei fornitori e partners commerciali/finanziari;
b) verificare che fornitori e partners non abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non cooperativi dal Gruppo di Azione Finanziaria contro il riciclaggio di denaro (GAFI); qualora Fornitori e Partner siano in alcun modo collegati ad uno di tali Paesi, sarà necessario che le decisioni relative ottengano l'espressa autorizzazione del Presidente, sentito l'OdV;
c) garantire trasparenza e tracciabilità degli accordi/joint venture con altre imprese per la realizzazione di investimenti;
d) verificare la congruità economica degli investimenti effettuati in joint venture (rispetto dei prezzi medi di mercato, utilizzo di professionisti di fiducia per le operazioni di due diligence, ecc.).

Con riferimento al rischio di flussi finanziari in entrata:
a) effettuare controlli formali e sostanziali dei flussi finanziari aziendali in entrata; tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio terrorismo ecc.), degli Istituti di credito utilizzati (sede delle banche coinvolte nelle operazioni) e di eventuali schermi societari e strutture fiduciarie utilizzate per eventuali operazioni straordinarie;
b) non accettare denaro e titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) per importi complessivamente superiori a euro 5.000, se non tramite intermediari a ciò abilitati, quali banche, istituti di moneta elettronica e Poste Italiane S.p.A.;
c) mantenere evidenza, in apposite registrazioni su archivi informatici, delle transazioni effettuate su conti correnti aperti presso stati in cui permangono regole di trasparenza meno restrittive per importi superiori, complessivamente, a euro 5.000.
Con riferimento al rischio nei rapporti infragruppo:

a) verificare il livello di adeguamento delle società controllate rispetto alla predisposizione di adeguati presidi antiriciclaggio.

ISTRUZIONI E VERIFICHE DELL'ORGANISMO DI VIGILANZA

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i reati di riciclaggio sono i seguenti:
a) proporre l'emanazione ed aggiornamento di istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle aree a rischio. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;
b) proporre la predisposizione di una procedura specifica per il monitoraggio delle controparti contrattuali diverse da partners e fornitori;
c) monitorare costantemente l'efficacia delle procedure interne già adottate dalla società e vigilare sull'efficacia di quelle di futura introduzione.

Parte speciale 8

ALTRI REATI

REATI DI FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO

L'art. 25-bis del D.Lgs. n. 231/01, introdotto dall'art. 6 della legge n. 350/2001, prevede, tra i reati presupposto per la punibilità dell'ente, i seguenti reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento:

- falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
- alterazione di monete (art. 454 c.p.);
- spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- falsificazione di valori di bollo, introduzione nello Stato acquisto o detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o valori di bollo (art. 460 c.p.);
- fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.);
- uso di valori di bollo contraffati o alterati (art. 464 c.p.);
- contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

Rispetto ai reati sopra elencati, tenuto conto del campo di operatività di ENERCOM, l'unico rischio di commissione che risulta astrattamente configurabile riguarda il reato presupposto di spendita di monete falsificate ricevute in buona fede (art. 457 c.p.). Tale fattispecie punisce chiunque spenda, o metta altrimenti in circolazione monete contraffatte o alterate, da lui ricevute in buona fede.
Sussiste infatti la possibilità che il personale ENERCOM addetto agli sportelli riceva inavvertitamente dalla clientela moneta falsificata.
Ai fini dell'integrazione dell'elemento soggettivo del reato in esame è peraltro necessario che l'autore si avveda o abbia quantomeno il dubbio della falsità della moneta che spende o mette altrimenti in circolazione e che abbia ricevuto in buona fede.
Ogni sportello è dotato di appositi dispositivi idonei a identificare l'eventuale falsità delle banconote ricevute.
Ne consegue che il rischio di commissione del reato in questione risulta essere modesto, in quanto limitato alla eventuale falsità della moneta metallica.
L'Azienda ha comunque in programma l'emanazione di adeguata informativa agli operatori sul comportamento da tenere nell'ipotesi che ci si accorga che venga presentata della moneta contraffatta (comunicato aziendale).

DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO (art. 25-bis.1, aggiunto dalla Legge 23 Luglio 2009, n.99, art. 15).

Le fattispecie criminose che assumono rilievo sono le seguenti:
Turbata libertà dell'industria o del commercio (art. 513 c.p.): quando si adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio, salvo che il fatto non costituisca più grave reato.
Frode nell'esercizio del commercio (art. 515 c.p.): quando nell'esercizio di un'attività commerciale, ovvero in uno spaccio aperto al pubblico, si consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile,

per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita, salvo che il fatto non costituisca più grave reato.
Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.).
Vendita di prodotti industriali con segni mendaci (art. 517 c.p.): quando si pongono in vendita o altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto.
Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517 ter c.p.).
Contraffazioni di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517 quater c.p.).
Illecita concorrenza con minaccia o violenza (art. 513 bis): quando nell'esercizio di un'attività commerciale, industriale o comunque produttiva, si compiono atti di concorrenza con violenza o minaccia. La condotta consiste nel porre in essere atti di concorrenza con violenza o minaccia nell'esercizio di un'attività commerciale nei confronti di altre aziende operanti nello stesso settore o zona, e cioè in una situazione di potenziale conflitto. Per concorrenza si intende quel regime nel cui ambito viene garantito ad ogni operatore economico la libertà di intervento e di iniziativa sui mercati. Di conseguenza, nella specie è punito chi opera sul piano economico con mezzi strumentali che, essendo caratterizzati da violenza o minaccia, compromettano la libertà d'iniziativa economica, determinando situazioni di privilegio non consentite o represse dall'ordinamento.
Frodi contro le industrie nazionali (art. 514): quando, ponendo in vendita o mettendo altrimenti in circolazione, sui mercati nazionali o esteri, prodotti industriali, con nomi, marchi o segni distintivi contraffatti o alterati, si cagioni un nocumento all'industria nazionale.

Con riguardo alle sopra elencate fattispecie di reato, attese le particolari modalità con cui le stesse debbono realizzarsi e considerata anche l'attività commerciale svolta da ENERCOM, si ritiene di poter escludere la sussistenza di rischi di commissione.

DELITTI CON FINALITÀ DI TERRORISMO O D'EVERSIONE DELL'ORDINE DEMOCRATICO (art. 25-quater, aggiunto dalla Legge 7 del 14 gennaio 2003 "Ratifica ed esecuzione della Convenzione internazionale per la repressione del finanziamento al terrorismo, fatta a New York il 9 dicembre 1999 e norme di adeguamento dell'ordinamento interno")

L'ente è soggetto a responsabilità anche nel caso di commissione, nel suo interesse o a suo vantaggio, di reati con finalità di terrorismo o di eversione dell'ordine democratico.

Sono previste sanzioni pecuniarie con il consueto meccanismo delle "quote", e per i casi più gravi sanzioni interdittive, sino alla interdizione definitiva dall'esercizio dell'attività

Le predette sanzioni trovano applicazione anche in relazione alla commissione di delitti che comunque violino quanto previsto dall'art. 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999. Sotto questo profilo, il catalogo dei Reati è dunque lasciato "aperto": non vi è, infatti, un'elencazione tassativa delle fattispecie, ma una previsione generica di delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali o in violazione di quanto previsto dall'art. 2 della Convenzione citata.

La principale fattispecie conosciuta dal nostro ordinamento è sicuramente il **delitto di associazione con finalità di terrorismo e di eversione dell'ordine democratico** previsto dall'art. 270-bis c.p., che punisce: 1) la promozione, costituzione, organizzazione, direzione o finanziamento di associazioni con finalità di terrorismo o di eversione dell'ordine democratico; 2) la partecipazione a tali associazioni.

Si ritiene di poter affermare che questa categoria di reati, alla luce del fatto che la società non avrebbe modo di trarre un interesse o vantaggi di sorta dalla commissione di questo genere di illeciti, non presenta rischi.

PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI (art. 25-quater-1, aggiunto dalla L. 9 gennaio 2006 n. 7, art. 8).

La società non ha alcun interesse e non potrebbe trarre alcun vantaggio dalla commissione di tale figura di reato, né del resto pare sussistere il rischio che esponenti aziendali lo commettano, attesa l'assenza nell'ambito delle strutture aziendali di strumentazioni idonee a consentire tali pratiche.

DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE (art. 25-quinquies, aggiunto dalla Legge n. 228/2003)

I reati "contro la personalità individuale" vengono qui di seguito elencati:

a. Pornografia minorile, art. 600 *ter*.
b. Detenzione di materiale pornografico, art. 600 *quater*
c. Pornografia virtuale, art. 600 *quater*.1.
d. Iniziative turistiche volte allo sfruttamento della prostituzione minorile, art. 600 *quinquies*

Si ritiene di poter affermare che la società, avuto riguardo al campo di operatività, non ha alcun interesse e non potrebbe trarre alcun vantaggio dalla commissione di tale figura di reato, e pertanto non sussistono rischi di commissione di tali illeciti.

ABUSI DI MERCATO (art. 25-sexies)

I reati presupposto di cui all'art. 25-sexies del D.Lgs. 231/01, sono i seguenti:

• **Abuso di informazioni privilegiate** (art. 184 D.Lgs. 58/1998):

1. quando, essendo in possesso di informazioni privilegiate in ragione della propria qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:

a) si acquista, si vende o si compiono altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;

b) si comunicano tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;

c) si raccomandano o si inducono altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a).

2. quando, essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose, si compie taluna delle azioni sopra indicate.

Il reato di Abuso di informazioni privilegiate appare configurabile ogniqualvolta uno dei soggetti indicati dalla norma sfrutti le informazioni di cui sia venuto in possesso, al fine di porre in essere una delle condotte tipizzate dal Legislatore. (Si pensi al caso in cui, a seguito della quotazione in borsa, un membro del Consiglio di Amministrazione compia operazioni su strumenti finanziari (non solo di compravendita, ma anche, ad esempio, di conferimenti in società in via di costituzione, ovvero di dazione di titoli a garanzia di fido), utilizzando le informazioni privilegiate di cui sia a conoscenza in virtù del ruolo ricoperto). Occorre peraltro rilevare come, nell'ambito di applicazione della norma, rifluiscano anche le negoziazioni compiute per interposta persona,

come quelle poste in essere tramite fiduciari o quelle realizzate formalmente a beneficio dei congiunti dell'insider.
Quanto alla condotta di tipping di cui al comma 1, lett. b) dell'art. 184 D.Lgs. n. 58/1998, è opportuno sottolineare come il divieto di comunicazione di informazioni privilegiate a terzi sia escluso quando avvenga nel "normale esercizio del lavoro, della professione, della funzione o dell'ufficio": non rivestirebbe pertanto rilevanza penale, ad esempio, la divulgazione delle notizie effettuate nel corso delle trattative di acquisizione o di fusione intercorrenti tra società quotate in borsa; ovvero realizzata mediante comunicati alla stampa specializzata.
In relazione alle condotte criminose poste in essere dagli azionisti, si ritiene comunemente che il reato possa essere integrato solo in quei casi in cui la partecipazione al capitale costituisca la causa del conseguimento dell'informazione privilegiata, posto che, ove ciò non avvenisse, l'azionista dovrebbe essere trattato alla stregua di qualsiasi altro investitore.
A titolo esemplificativo, l'azionista dovrebbe essere punito come insider qualora, reso edotto - in virtù del proprio possesso azionario - di un progetto che la società, ha intenzione di realizzare, effettuasse delle operazioni finanziarie avvantaggiandosi di tale informazione.
Per quanto concerne invece i cosiddetti temporary insiders, la norma sembra fare riferimento soprattutto ai consulenti ovvero ai membri di quegli organi (ad esempio Banca d'Italia o Consob) che possano venire a conoscenza dell'informazione privilegiata proprio nell'esercizio della propria attività.
• **Manipolazione del mercato** (art. 185. D.Lgs. 58/1998): quando si diffondono notizie false o si pongono in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, è punito con la reclusione da uno a sei anni e con la multa da euro ventimila a euro cinque milioni.

Stante l'ambito delle operazioni svolte da ENERCOM, che non ricomprendono il ricorso a "strumenti finanziari", devono ritenersi esclusi i rischi di commissione di tali reati.

REATI TRANSNAZIONALI (inseriti nella disciplina con la Legge n. 146 del 16 marzo 2006) E DI CRIMINALITÀ ORGANIZZATA (art. 24-ter, aggiunto dalla L. 15 luglio 2009, n. 94, art. 2, co. 29).

La Legge 146/2006 ha inserito nel numero dei reati un gruppo di reati definiti come "transnazionali" le seguenti fattispecie criminose:

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso (art. 416 bis c.p.);
- Associazione per delinquere finalizzata al contrabbando di tabacchi esteri (D.P.R. 473/1973, articolo 291 *quater*);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (D.P.R. 309/1990, art. 74);
- Riciclaggio (art. 648 bis c.p.);
- Impiego di denaro, beni od utilità di provenienza illecita (art. 648 ter c.p.);
- Traffico di migranti (D.Lgs. 286/1998 art. 12);
- Induzione a non rendere dichiarazioni (art. 377 bis c.p.);
- Favoreggiamento personale (art. 378 c.p.).

Stante l'ambito esclusivamente regionale dell'attività svolta e dei rapporti tenuti da ENERCOM, devono ritenersi esclusi i rischi di commissione di tali reati transnazionali.

Gran parte di essi tuttavia sono già stati presi in esame nelle precedenti parti speciali in quanto all'esito di successivi interventi del Legislatore sono divenuti rilevanti ai fini del Decreto anche se privi del carattere della transnazionalità.

Quanto ai restanti deve osservarsi che la L. 94/2009 ha introdotto nel novero dei reati presupposto l'associazione per delinquere, l'associazione di tipo mafioso, lo scambio elettorale politico mafioso (art. 416-ter c.p.), il sequestro di persona a scopo di rapina o estorsione (art. 630 c.p.), l'associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope, la illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo.

Anche per questi reati, avuto riguardo alle loro peculiarità si ritiene di poterne escludere il rischio.

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

Il comma 1 dell'art. 2 del D.Lgs. 16 luglio 2012, n. 109 ("Attuazione della direttiva 2009/52/CE che introduce norme minime relative a sanzioni e a provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare") ha introdotto nel corpo del D.lgs. 231/2001 l'articolo 25 duodecies che prevede la responsabilità degli enti per il delitto di cui all'articolo 22, comma 12 - bis, del decreto legislativo 25 luglio 1998, n. 286.
Tale norma sanziona il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, qualora:

- i lavoratori occupati siano in numero superiore a tre; oppure
- i lavoratori occupati siano minori in età non lavorativa; oppure
- i lavoratori occupati siano sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-bis del codice penale (ossia l'aver esposto i lavoratori a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro).

L'area a rischio di commissione del reato in questione è l'Ufficio Personale, con riferimento all'eventualità che l'azienda decida di ricorrere all'impiego di personale di cittadinanza non italiana.
Per questo reato, avuto riguardo alle procedure adottate dall'Ufficio personale, si ritiene che il rischio di commissione sia basso.

I principi di comportamento

Nell'espletamento della propria attività per conto di ENERCOM, i destinatari del Modello sono tenuti al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati dal Modello e, in particolare, dal Codice Etico.
A tutti i soggetti i destinatari del Modello, segnatamente, è fatto assoluto divieto:

- di tenere, promuovere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nell'articolo 25 duodecies del Decreto;
- di tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

I destinatari del Modello dovranno, inoltre, attenersi ai seguenti principi:

- considerare sempre prevalente la tutela dei lavoratori rispetto a qualsiasi considerazione economica;
- verificare al momento dell'assunzione e durante lo svolgimento di tutto il rapporto lavorativo che eventuali lavoratori provenienti da paesi terzi siano in regola con il permesso di soggiorno e, in caso di scadenza dello stesso, abbiano provveduto a rinnovarlo;
- nel caso in cui si faccia ricorso al lavoro interinale mediante apposite agenzie, assicurarsi che tali soggetti si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno e richiedere espressamente l'impegno a rispettare il Modello;
- assicurarsi con apposite clausole contrattuali che eventuali soggetti terzi con cui la Società collabora (fornitori, consulenti, ecc.) si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno e richiedere espressamente l'impegno a rispettare il Modello;

- devono essere rispettate le misure previste dalle procedure aziendali dirette alla prevenzione dell'impiego del lavoro irregolare e alla tutela dei lavoratori;
- non fare ricorso, in alcun modo, al lavoro minorile o non collaborare con soggetti che vi facciano ricorso.

L'azienda ha recentemente provveduto a modificare la procedura PRQS 01-03 integrandola con gli adempimenti di competenza dell'Ufficio Personale in caso di assunzione di personale straniero, in modo che sia garantita la verifica della regolarità del suo soggiorno.

Elenco degli allegati al "Modello 231"

Sono "Allegati" del presente Modello i seguenti documenti:

Allegati al Modello Organizzativo	Competenza in caso di modifiche
Allegato 1 Codice Etico di ENERCOM	Aggiornamento deliberato dal CdA di ENERCOM
Allegato 2 Organigramma funzionale	Aggiornamento a cura di RAQ su indicazioni del Presidente
Allegato 3 Composizione e Regolamento dell'OdV	Aggiornamento a cura di RAQ su indicazioni del Presidente
Allegato 4 Analisi Rischio Reato MOrg 231	Aggiornamento approvato dal Presidente sentito l'OdV
Allegato 5 Manuale Sistema Gestione Qualità	Aggiornamento a cura di RAQ e RSPP
Allegato 6 Elenco Procedure e Istruzioni Operative del Sistema Qualità	Aggiornamento deliberato dall'OdV su indicazioni del Resp. SGQ

Tutte le procedure adottate da ENERCOM per monitorare e gestire le aree di rischio, sono pubblicate sul sito Intranet Aziendale.

Fine documento