Modello di Organizzazione, Gestione e Controllo

ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

(Piano di prevenzione della corruzione ai sensi della legge 190/2012 e della delibera Civit 77/2013)

PARTE SPECIALE

Venis
Venezia Informatica e Sistemi S.p.A.

Versione: 3.0
Approvato con determinazione dell’Amministratore Unico il 22 dicembre 2016

PRIMA SEZIONE

PREMESSA

LA PARTE SPECIALE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo discende da un dettagliato lavoro diretto preliminarmente ad identificare, nel rispetto delle disposizioni di cui all'art. 6, comma 2 del Decreto Legislativo 8 giugno 2001, n. 231 (di seguito anche il "Decreto") e con riferimento alla specifica attività di Venis, le aree aziendali che possono essere considerate a rischio di commissione dei reati contemplati dal Decreto.

In generale, vengono considerate "aree a rischio" tutti quei settori di una società all'interno dei quali potrebbero essere commessi, nell'interesse o a vantaggio della società stessa, uno o più reati, tra quelli elencati agli articoli 24, 24 *bis* e *ter*, e 25, 25 *bis*, *bis* 1, *ter*, *quater*, *quater* 1, *quinquies*, *sexies*, *septies*, *octies*, *nonies*, *decies*, *undecies*, nonché nell'ulteriore articolo 25 *duodecies* del medesimo Decreto, nonché nella Legge 15 luglio 2009, n. 94 contenente le disposizioni in materia di sicurezza pubblica (art. 2 comma 29), nel D.P.R. 309/1990 – Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza (art. 74), nella Legge 18 marzo 2008, n. 48 – Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno (art. 7), nella Legge 23 novembre 2001 n. 409, recante Disposizioni urgenti in vista dell'introduzione dell'euro, nel Decreto n. 58 del 1998 – Testo Unico dell'Intermediazione Finanziaria, nel Decreto Legislativo 25 luglio 1998, n. 286 – Testo Unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero (articolo 12, comma 3, 3 *bis*, 3 *ter* e 5); nella Legge 14 gennaio 2003, n. 7 di ratifica della Convenzione di New York del 9 dicembre 1999, per la repressione del finanziamento del terrorismo (articolo 3); nella Legge 9 gennaio 2006, n. 7 – Disposizioni concernenti la prevenzione e il divieto delle pratiche di mutilazione genitale femminile (articolo 8); nella Legge 16 marzo 2006, n. 146 – Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea Generale il 15 novembre 2000 ed il 31 maggio 2001 (articoli 3 e 10); nella Legge 11 agosto 2003, n. 228 – Misure contro la tratta di persone – (articolo 5); nella Legge 18 aprile 2005, n. 62 – Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità Europee (articolo 9); nella Legge 3 agosto 2007, n. 231 e s.m.i. (articolo 64, comma 1, lett. f) – Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione – e nel recente D.L. 201/2011 (c.d. Manovra "Salva Italia" del governo Monti), convertito nella Legge 214/2011 con cui è stato ulteriormente ridotto il limite per la tracciabilità dei trasferimenti di denaro contante e dei titoli al portatore; nella legge 3 agosto 2007, n. 123 (art. 1) – Misure in tema di tutela della salute e della sicurezza sul lavoro e delega al Governo per il riassetto e la riforma della normativa in materia e successivo Decreto Legislativo 9 aprile 2008, n. 81, contenente il Testo Unico in materia di sicurezza; nella Legge n. 633 del 22 aprile 1941 (c.d. Legge sul diritto d'autore); nel D. Lgs. 7 luglio 2011 n. 121 – Attuazione della Direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della direttiva 2009/123/CE – che modifica la direttiva 2005/35/CE – relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per le violazioni); nel Decreto Legislativo 16 luglio 2012, n. 109, in attuazione della Direttiva 2009/52/CE circa l'impiego da parte di Enti di cittadini di Paesi terzi il cui soggiorno risulti

irregolare e nella L. 190/2012 in materia di prevenzione e repressione della corruzione e dell’illegalità nella pubblica amministrazione.

L’obiettivo della Parte Speciale del Modello è pertanto quello di fornire un quadro dettagliato della situazione aziendale con attenzione:

- alle aree “a rischio” individuate, unitamente alla descrizione dei processi, ai reati ipotizzabili e alle relative modalità attuative, nonché alle Funzioni aziendali interessate,
- al sistema di controllo, ovvero alle attività di controllo volte a contrastare la possibilità di realizzazione dei reati descritti,
- alle disposizioni riguardanti i flussi informativi specifici verso l’Organismo di Vigilanza (di seguito per brevità anche “O.d.V.”) al fine di agevolare l’attività di vigilanza e controllo sull’efficacia del Modello,
- ai documenti di riferimento,

nonché quello di fornire indicazioni in merito:

- al protocollo comportamentale da adottare con riferimento ad ogni area a rischio per evitare il generarsi di situazioni ambientali compatibili con i reati.

IL METODO UTILIZZATO

Il metodo di implementazione del presente Modello Organizzativo ha richiesto un lavoro di analisi su due livelli. Da un lato, si è proceduto all’attività di identificazione dei rischi-reato mediante l’osservazione, in concreto, del contesto aziendale di Venis, al fine di evidenziare dove e secondo quali modalità potrebbero verificarsi eventi pregiudizievoli, in considerazione degli obiettivi indicati dal Decreto; dall’altro si è proceduto alla progettazione e realizzazione del sistema di controllo unitamente alla indicazione di “protocolli comportamentali” (regole e procedure) da seguire nella formazione ed attuazione delle decisioni della Società, i quali, sono, a loro volta, funzionali all’eliminazione o, comunque, alla riduzione al minimo del rischio di commissione dei reati.

Il sistema di controllo ed i protocolli comportamentali di prevenzione previsti tengono conto, inoltre, della circostanza che, alla luce del Decreto, rileva anche il tentativo di reato. In questa ipotesi, peraltro, il Decreto prevede che le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) siano ridotte da un terzo alla metà, essendo esclusa l’irrogazione di sanzioni, ai sensi dell’ art. 26 del Decreto medesimo, solo nei casi in cui l’ente impedisca volontariamente il compimento dell’azione o la realizzazione dell’evento.

Con riferimento alla casistica dei reati contro la PA indicati negli articoli 24 e 25 del Decreto, le aree aziendali che sono state considerate rilevanti ai fini della possibilità di commissione dei reati, sono tutte quelle che hanno rapporti non soltanto diretti, ma anche indiretti, con la Pubblica Amministrazione.

In via preliminare ed a titolo meramente esemplificativo si chiarisce che quando la Società è chiamata a gestire attività afferenti l’esecuzione di progetti o la realizzazione di opere o servizi finanziati da risorse pubbliche, l’area “a rischio” viene individuata sia nei settori aziendali preposti alle verifiche delle condizioni previste per l’erogazione dei finanziamenti e/o contributi, sia in quei settori preposti alla realizzazione delle opere e/o dei progetti finanziati, sia nel settore incaricato della gestione dei flussi finanziari. Attività a rischio non sono, dunque, solo le attività di impresa, ma anche le attività strumentali allo svolgimento delle prime.

Una volta individuate le aree di attività a rischio, sia di impresa che “strumentali”, tipiche di un’azienda attiva nei settori di interesse per Venis, è stata effettuata un’analisi dell’effettivo contesto della Società, soprattutto in considerazione della sua natura di società *in house provider* del Comune di Venezia a partecipazione pubblica, al fine di delineare in modo specifico gli ambiti aziendali interessati dai reati in questione e di descrivere, in maniera più dettagliata, le eventuali modalità attuative di questi ultimi, muovendo dall’osservazione dell’insieme degli attuali processi operativi della Società.

Analogo procedimento è stato utilizzato per i reati di cui agli articoli 24 bis (delitti informatici e trattamento illecito dei dati), 25 bis (delitti contro la fede pubblica), 25 quater (delitti aventi finalità di terrorismo previsti dal codice penale e dalle leggi speciali ed i delitti, diversi dai precedenti, che siano comunque stati posti in essere in violazione di quanto previsto dalla Convenzione Internazionale di New York del 9 dicembre 1999 per la repressione del finanziamento al terrorismo), 25 quinquies (delitti contro la personalità individuale), per i reati di cui alla Legge 9 gennaio 2006, n. 7, inerenti le pratiche di mutilazione femminile, contemplati dall’art. 25 quater 1, nonché per i reati di cui all’art. 25 nonies (delitti in materia di violazione del diritto d’autore), 25 decies (induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria), 25 duodecies (impiego di cittadini di Paesi terzi il cui soggiorno è irregolare).

Per quanto riguarda, invece, i reati societari previsti dall’articolo 25 ter, l’individuazione delle “aree interessate” e delle modalità attuative ipotizzabili è stata perfezionata attraverso l’analisi della disciplina, legislativa e statutaria, degli organi sociali interessati, muovendo direttamente dalle ipotesi di reato contemplate dallo stesso articolo.

Analogamente si è proceduto per i delitti di criminalità organizzata previsti dall’art. 24 ter e per i reati transnazionali previsti dalla Legge n. 146/2006 di Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall’Assemblea Generale delle Nazioni Unite il 15 novembre 2000 ed il 31 maggio 2001.

Anche per quanto concerne i reati di cui all’art. 25 bis 1 (delitti contro l’industria e il commercio), 25 sexies ed i connessi illeciti amministrativi (abusi di mercato) e quelli di cui agli art. li 25 octies (ricettazione, riciclaggio e impiego di danaro, beni o utilità di provenienza illecita) e 25 undecies (reati ambientali), l’individuazione delle “aree interessate” e delle modalità attuative ipotizzabili è stata effettuata attraverso l’analisi della normativa rilevante e muovendo direttamente dalle ipotesi di reato contemplate dai predetti articoli.

Infine si osserva che, per quanto concerne, in particolare, i delitti di cui all’art. 25 septies : a) omicidio colposo commesso con violazione dell’articolo 55, comma 2, del D. Lgs. n. 81/2008, attuativo dell’articolo 1 della Legge delega n. 123/2007 (ovverosia commesso con violazione degli obblighi relativi ad attività non delegabili dal Datore di Lavoro); b) omicidio colposo commesso con violazione delle disposizioni del D. Lgs. n. 81/2008, attuativo dell’articolo 1 della Legge delega n. 123/2007 e c) lesioni personali gravi o gravissime commesse con violazione delle disposizioni contenute nel D. Lgs. n. 81/2008, attuativo dell’articolo 1 della Legge delega n. 123/2007 (indistintamente, quelle contenenti obbligazioni inerenti attività delegabili e non dal datore di lavoro), la mappatura delle “aree interessate” e l’individuazione della tipologia di modalità attuative ipotizzabili è stata effettuata attraverso l’individuazione delle prescrizioni funzionali ad evitare che si verifichino eventi pregiudizievoli per la salute e l’integrità fisica del lavoratore, (contenute nelle prescrizioni legislative ed aziendali in materia) e mediante l’individuazione – sia in termini fisici (localizzazione) che di funzioni – dei soggetti che, per espressa previsione di legge ovvero in virtù di quanto previsto dalle disposizioni organizzative dell’azienda sono tenuti al rispetto o debbono far rispettare le anzidette prescrizioni.

SECONDA SEZIONE

PARTE PRIMA – REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

(artt. 24 e 25 del Decreto)

Aree a rischio

Con riferimento specifico ai reati previsti dagli articoli 24 e 25 del Decreto – i quali rilevano, secondo l'ordinamento italiano, se commessi nei confronti della Pubblica Amministrazione sia italiana che estera – al fine di rendere maggiormente comprensibile in cosa consista il rischio di commissione del reato, è preliminarmente necessario precisare cosa debba intendersi, ai sensi della legge penale, per "pubblico ufficiale" e per "incaricato di pubblico servizio".

Sul punto, si richiama l'articolo 357, c.p., secondo il quale sono pubblici ufficiali "*coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti 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*".

Per quanto attiene alla nozione di "*pubblica funzione amministrativa*", l'articolo 357, comma 2, c.p., specifica che si tratta di una funzione disciplinata da "*norme di diritto pubblico*", ovverosia da quelle norme volte al perseguimento di uno scopo pubblico ed a tutela di un interesse pubblico .

In conformità al secondo comma dell'articolo 357, c.p. – incentrato sul profilo oggettivo della natura della funzione esercitata - rientra, anche la figura del "pubblico ufficiale straniero", da individuarsi in: (i) qualsiasi persona che esercita una funzione legale, amministrativa o giudiziaria in un Paese straniero; (ii) qualsiasi persona che esercita una funzione pubblica per un Paese straniero ovvero per un ente pubblico di un Paese straniero; (iii) qualsiasi funzionario o agente di un'organizzazione internazionale pubblica, quale, ad esempio, i funzionari della Comunità Europea.

Agli effetti dell'articolo 358, c.p., 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 questa ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale*".

La giurisprudenza ha inoltre elaborato una serie di indici rivelatori del carattere "pubblicistico" dell'ente. In particolare, si fa riferimento ai seguenti indici:

- la sottoposizione ad un'attività di controllo e di indirizzo a fini sociali nonché ad un potere di nomina e revoca degli amministratori da parte dello Stato o di altri enti pubblici;
- la presenza di una convenzione e/o concessione con la pubblica amministrazione;
- l'apporto finanziario da parte dello Stato.

Sulla base di quando sopra riportato, l'elemento discriminante per indicare se un soggetto rivesta o meno la qualità di "incaricato di un pubblico servizio" è rappresentato, dunque, non dalla natura giuridica dell'ente, ma

dalle funzioni affidate al soggetto, le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale. Da quanto detto, discende che l'incaricato di pubblico servizio può essere descritto come la persona che, a qualunque titolo, presta un pubblico servizio (ovvero un'attività disciplinata da norme di diritto pubblico in funzione della cura di interessi pubblici o del soddisfacimento di bisogni di interesse generale) pur essendo privo di poteri formali di natura deliberativa, autorizzativa o certificativa (tipici della pubblica funzione amministrativa) mirati alla cura dei suddetti interessi e bisogni.

Residuando inevitabilmente, nell'individuazione di entrambe le figure, evidenti margini di incertezza, Venis, in funzione della prevenzione di tale rischio-reato, valuta caso per caso se i soggetti con i quali entra in rapporto possano essere qualificati o meno come incaricati di pubblico servizio.

Il presupposto fondamentale per la configurazione dei reati sopra descritti consiste nell'instaurazione di rapporti diretti ed indiretti con la Pubblica Amministrazione nonché lo svolgimento ed esercizio di attività, da parte di personale Venis, nella qualità di eventuali incaricati di pubblico servizio (ad es. nell'espletamento di gare ad evidenza pubblica nelle procedure per le quali Venis assume la funzione di stazione appaltante).

In tal senso, pertanto, Venis ha definito come aree a rischio tutte quelle aree aziendali che per lo svolgimento della propria attività intrattengono rapporti con le Pubbliche Amministrazioni.

Si rileva inoltre che vengono definite aree di supporto tutte quelle aree di attività aziendale che gestiscono strumenti di tipo finanziario e/o mezzi sostitutivi. Si tratta, quindi, di aree di attività che pur non istaurando rapporti diretti con la Pubblica Amministrazione, possono supportare la commissione di reati.

*

Nel procedere all'individuazione dei reati di cui agli articoli 24 e 25 del decreto, occorre dar conto delle recenti novità apportate in materia dalla Legge n. 190 del 6 novembre 2012 (*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalita' nella pubblica amministrazione*).

In forza della nuova disciplina **all'art. 25, comma 3 del D. Lgs. 231/2001** è stato inserito il richiamo al nuovo art. 319-quater, che la Legge n. 190 ha aggiunto al nostro Codice Penale. Tale articolo configura come autonomo, rispetto al passato, il reato di concussione per induzione e stabilisce la punibilità ANCHE del privato che perfeziona la dazione dell'indebito.

Ai sensi del nuovo art. 319-quater, infatti "*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 denaro o altra utilità è punito con la reclusione fino a tre anni*".

Ciò significa che l'imprenditore che fosse indotto, per effetto dell'abuso di potere del funzionario pubblico, a versare o a promettere a quest'ultimo denaro o altra utilità e che, precedentemente, era considerato vittima del reato di concussione (con possibilità, quindi, di chiedere un risarcimento del danno non solo all'autore del reato, ma anche alla Pubblica Amministrazione di appartenenza), oggi è punito come correo dell'amministrazione o del pubblico funzionario.

All'art. 25-ter, comma 1 del D. Lgs. 231/2001, viene poi aggiunta la lettera s-bis) che richiama il nuovo delitto di **corruzione tra privati** nei casi di cui al nuovo **terzo comma** dell'art. 2635 c.c. (ovvero limitatamente a "*chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma*").

Ai sensi del nuovo art. 2635 c.c.:

"1. 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.
2. 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.
3. Chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste.
4. 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.
5. Si procede a querela della persona offesa, salvo che dal fatto derivi una distorsione della concorrenza nella acquisizione di beni o servizi".

Le innovazioni non sono di poco conto in un sistema giuridico come il nostro in cui il fenomeno corruttivo è sempre stato prevalentemente concepito nell'ambito dei pubblici poteri. Invero, anche il Codice Penale disciplina i reati di corruzione nel titolo dedicato ai reati contro la Pubblica Amministrazione.

Ulteriore elemento di novità rispetto al passato è rappresentato dalla rilevanza conferita alla violazione degli "obblighi di fedeltà" oltre agli "obblighi inerenti al proprio ufficio.

*

Passando alla specifica individuazione delle **aree a rischio,** con riferimento ai reati commessi in danno della Pubblica Amministrazione (di cui agli artt. 24 e 25 del Decreto), si segnalano i seguenti relativi **processi operativi**:

1) Vendita di beni e servizi alla Pubblica Amministrazione - Negoziazione, stipulazione e/o esecuzione di contratti e di convenzioni di concessioni con l'ente locale di riferimento;

2) Acquisizioni con ruolo pubblicistico - Negoziazione, stipulazione e/o esecuzione di contratti e di convenzioni di concessioni, in qualità di stazione appaltante, nel rispetto delle disposizioni previste nel D. Lgs. n. 163/2006 e nel D.P.R. n. 207/2010 e s.m.i recanti "Codice degli Appalti pubblici" e "Regolamento di Attuazione";

3) Gestione dei rapporti con soggetti pubblici per l'ottenimento di autorizzazioni, licenze, provvedimenti amministrativi necessari allo svolgimento delle attività aziendali per l'installazione di impianti e attività strumentali;

4) Finanza agevolata - Richiesta e ottenimento di finanziamenti, contributi, erogazioni da parte di amministrazioni pubbliche; attività di gestione dei finanziamenti stessi per l'esecuzione di grandi opere e/o di progetti finanziati;

5) Gestione dei rapporti con i soggetti pubblici per gli aspetti che riguardano gli adempimenti, verifiche e ispezioni relativi alla produzione di rifiuti ed emissioni inquinanti.

6) Gestione amministrativa degli obblighi previdenziali e fiscali del personale dipendente e dei collaboratori. Gestione dei relativi accertamenti, delle ispezioni;

7) Altri rapporti con lo Stato, le Regioni, gli Enti Locali ed altre amministrazioni pubbliche italiane ed estere, nonché con Autorità di Vigilanza Regolamentazione e Garanzia;

8) Procedimenti giudiziali con la Pubblica Amministrazione;

9) Gestione di procedimenti giudiziali con soggetti terzi non pubblici.

Sono stati individuati, altresì, alcuni **processi strumentali** che impattano indirettamente sui reati previsti dal Decreto. Si tratta dei processi di gestione delle provviste. Precisamente, i processi di supporto analizzati sono:

10) Approvvigionamento di beni e servizi;

11) Conferimento di contratti di consulenza o prestazioni professionali;

12) Finanza dispositiva - Gestione dei pagamenti e delle risorse finanziare;

13) Selezione e assunzione del personale e gestione delle risorse umane;

14) Accordi transattivi;

15) Spese di rappresentanza e gestione omaggistica;

16) Sponsorizzazioni;

17) Liberalità.

Fermi restando i principi di comportamento a cui attenersi nello svolgimento dell'attività aziendale in generale e nei rapporti con la Pubblica Amministrazione (di seguito anche "PA") in particolare, dettagliatamente individuati nel documento "Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione", da ritenersi validi con riferimento a tutte le aree a rischio di commissione dei reati contro la PA, la rilevanza, nel complesso delle attività di Venis, delle funzioni proprie delle aree a rischio sopra considerate, rende quanto mai opportuno procedere all'analisi separata di ogni singola area.

1) "VENDITA DI BENI E SERVIZI ALLA PUBBLICA AMMINISTRAZIONE – NEGOZIAZIONE, STIPULAZIONE E/O ESECUZIONE DI CONTRATTI E DI CONVENZIONI DI CONCESSIONI CON L'ENTE LOCALE DI RIFERIMENTO"

1.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività svolte per la fornitura di beni e servizi (talvolta con realizzazione di opere infrastrutturali) a favore di soggetti pubblici sulla base di contratti o di convenzioni di concessioni.

Pur essendo attualmente Venis una Società controllata dal Comune di Venezia che opera per e nell'interesse esclusivo degli azionisti (quindi non opera sul mercato delle gare pubbliche) l'analisi del presente processo viene fatta, per completezza, tenendo conto di entrambe le fattispecie, offerta e partecipazione a gara.

Il processo si articola nelle seguenti fasi:

- Preparazione dell'offerta con il soggetto pubblico, nel caso di trattative private;

- Preparazione dell'offerta e partecipazione alla gara, nel caso di evidenza pubblica o negoziazione;
- Stipulazione ed esecuzione contrattuale e collaudo/verifica;
- Fatturazione, gestione del credito, incassi ed eventuali contestazioni.

1.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Truffa aggravata a danno dello Stato, di altro Ente Pubblico o dell'Unione Europea (art. 640, comma 2, n. 1, c.p.); corruzione (artt. 318, 319, 319 *bis* e 320, 322, c.p.); frode informatica a danno dello Stato (articolo 640-*ter*, c.p.).

Il reato di **truffa aggravata** si configura nel caso in cui, per realizzare un ingiusto profitto, siano poste in essere condotte artificiose ed idonee ad indurre in errore la Pubblica Amministrazione, con conseguente danno a suo carico.

Tale reato può realizzarsi, ad esempio, laddove, nella predisposizione da parte dei soggetti e degli Uffici competenti, di documenti di gara si forniscano informazioni non veritiere o si adotti una condotta ingannevole idonea a recare un danno patrimoniale allo Stato (ad es., sovrastimando i beni/servizi offerti o rendicontando prestazioni non fornite).

Occorre considerare che a seguito della riforma di cui alla L. 190 del 6 novembre 2012, si è avuto un inasprimento generalizzato delle pene per alcuni dei reati contro la Pubblica Amministrazione (abuso d'ufficio, peculato, corruzione e concussione).

Per quanto di nostro interesse, perché espressamente contemplato dal D. lgs. 231/2001, occorre in particolare considerare la modifica della struttura del reato di corruzione impropria (ovvero la corruzione per atto di ufficio) oggi chiamata "corruzione per l'esercizio della funzione" (art. 318 e 320 c.p.).

Con la modifica si estende la punibilità all'incaricato di pubblico servizio equiparando *in toto* la sua figura a quella del pubblico ufficiale (art. 320 c.p.) e sanzionando non solo la retribuzione ma **qualsiasi forma** di utilità promessa o ottenuta. Non viene più richiesta, pertanto, la qualifica di pubblico impiegato per l'ipotesi di cui all'art. 319 c.p. (corruzione per atto contrario ai doveri d'ufficio).

Il nuovo articolo 318 c.p., inoltre prevede una fattispecie corruttiva di carattere generale, non più vincolata al compimento di un atto predeterminato del funzionario pubblico, ma che si estende a sanzionare un generico asservimento della funzione (*il pubblico ufficiale che, **per l'esercizio delle sue funzioni o dei suoi poteri**, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa è punito con la reclusione da uno a cinque anni*).

Essendo poi stata eliminata l'ipotesi della corruzione impropria susseguente (che in passato non prevedeva la punibilità per il privato), non vi è più differenza, dal punto di vista della punibilità, tra chi paga, offre o promette e il pubblico funzionario.

Ad oggi, pertanto, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto

contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità (essendo rimasto invariato il testo dell’art. 319 c.p. – c.d. corruzione propria - al di là dell’inasprimento della pena che va oggi da quattro a otto anni di reclusione).

L’elemento tipico del reato, non è più soltanto la “illecita negoziazione” di un atto amministrativo ma un più generico assoggettamento della funzione a scopi non legittimi, a fronte della indebita percezione di denaro e/o altra utilità.

Tale reato può realizzarsi nel caso di promessa, offerta, concessione da parte dei soggetti e degli Uffici competenti della Società o anche da parte di terzi, quali agenti, collaboratori esterni, soggetti appositamente incaricati, all’amministrazione aggiudicatrice, per se stessa o per un terzo, di danaro o di altro vantaggio, al fine, ad esempio, favorire l’aggiudicazione del contratto e influire sull’esito del collaudo.

Il reato di **frode informatica** si configura nel caso di creazione di un’anomalia di funzionamento o di distruzione di informazioni nell’ambito di un sistema o di un software della Società, contenente dati rilevanti per la Pubblica Amministrazione, al fine di procurarsi un vantaggio ingiusto con conseguente danno a carico della Pubblica Amministrazione.

Tale reato può, dunque, verificarsi nel caso di interventi non legittimi, attuati in qualsiasi modo, su programmi e sistemi informatici, da parte degli Uffici e dei soggetti competenti, al fine di sottrarre tali dati al controllo della PA oppure al fine di manipolarli, ad esempio per favorire l’aggiudicazione di un contratto. Il reato potrebbe essere altresì commesso alterando il funzionamento di sistemi o intervenendo sui dati, per procurare un ingiusto profitto alla Società (anche ad es. nel caso di contratti riguardanti l’installazione/gestione di software per conto della PA).

1.c) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell’Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l’Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza, Bilancio
- la Funzione Acquisti, Gare e Contratti
- la Funzione Tecnologie, Servizi e Sviluppo
- il Responsabile del Procedimento
- la Funzione Comunicazione

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

1.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- La segregazione delle responsabilità mediante l'esistenza di attori diversi operanti nelle seguenti fasi/attività dei processi:
    - Preparazione dell'offerta o definizione negoziata delle specifiche,
    - Gestione Albo Fornitori per le sub-forniture,
    - Esecuzione contrattuale,
    - Fatturazione;
- Sottoscrizione, da parte del responsabile dell'offerta, di specifica dichiarazione di rispetto dei principi etico-comportamentali adottati dalla Società[1] da allegare ai documenti di partecipazione a gare/trattative private con PA;
- Il conferimento di specifiche procure ai responsabili delle unità organizzative coinvolte al fine di dotarli del potere di rappresentanza della Società;
- Effettuazione di verifica di congruenza fra quanto contrattualizzato, quanto collaudato/attestato e quanto fatturato alla PA;
- Tracciabilità della documentazione eventualmente richiesta e consegnata all'ente di riferimento, degli atti e delle fonti informative nelle singole fasi del processo con specifico riferimento ad impiego di risorse e tempi;
- Selezione ed utilizzo di sub-fornitori da Albo Fornitori qualificati;
- Inserimento, in caso di partecipazione a Raggruppamenti Temporanei di Imprese (RTI), da parte delle società che aderiscono al Raggruppamento, della clausola riportata in nota[2], che costituirà parte integrante e essenziale degli accordi/intese tra le parti;

[1] La dichiarazione standard da utilizzare è la seguente: La Società dichiara che, in tutte le attività svolte ai fini della partecipazione alla gara di appalto/trattativa privata, sono state rispettate le disposizioni contenute nel Modello di Organizzazione, Gestione e Controllo adottato dalla Società ai sensi del Decreto, nel Codice Etico che ne costituisce parte integrante e sostanziale e nel Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, adottati dalla Società. La Società si impegna altresì all'osservanza di dette disposizioni in tutte le fasi di negoziazione con la Pubblica Amministrazione che dovessero intervenire successivamente alla presentazione dell'offerta.

[2] "Le Parti dichiarano reciprocamente e garantiscono che, nelle operazioni ed attività del Raggruppamento, si impegnano al rispetto delle normative vigenti al fine di non porre in essere alcuna azione pregiudizievole nei confronti dei terzi in genere, ed in particolare dell'Ente Appaltante.
Le Parti si impegnano a porre in essere ogni azione affinché il Raggruppamento, nei propri rapporti commerciali e di affari, ottemperi ai seguenti principi fondamentali:
- utilizzo legittimo della Immagine o nome delle Parti, senza trarne per il Raggruppamento o per ciascuna di esse, vantaggi commerciali non giustificati;
- corretta gestione e uso delle informazioni riservate o confidenziali ricevute da terzi;
- adozione di pratiche commerciali e contrattuali nel pieno rispetto dei canoni di correttezza.

In particolare le Parti, nel rispetto di quanto previsto dal Decreto, con riferimento alle operazioni ed attività di interesse del Raggruppamento, dichiarano di aver già provveduto all'adozione del Modello Organizzativo richiesto da tale normativa, o si impegnano, qualora non abbiano già provveduto all'adozione del citato Modello Organizzativo, ad adottare un Modello Organizzativo che recepisca i principi di seguito evidenziati.

- Devono inoltre essere definite adeguate modalità di escalation autorizzativa per la gestione delle eventuali deroghe ai principi sopra riportati.

1.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- *Predisposizione e trasmissione documentazione di gara/offerta*
    - in sede di raccolta/redazione della documentazione tecnico-amministrativa e trasmissione dei documenti di partecipazione alla gara o in sede di trattative e definizione delle clausole contrattuali; la fattispecie a rischio ricorre, in particolare, nel caso in cui tali comportamenti siano diretti a rappresentare alla PA informazioni non vere e/o non complete o ad eludere obblighi di legge;

- *Scelta del contraente da parte PA e stipulazione del contratto*
    - in sede di verifica della rispondenza ai requisiti del bando ed individuazione del vincitore della gara e stipulazione del contratto; la fattispecie a rischio può ricorrere, in particolare, nel caso in cui tali comportamenti siano utilizzati per indurre i citati rappresentanti a favorire la posizione della Società (ad es., le Funzioni aziendali di vendita si impegnano a scegliere, in modo immotivato, eventuali sub-fornitori di “gradimento” dei rappresentanti della PA);

Per tali finalità le Parti che sottoscrivono il presente atto si impegnano - con riferimento alle operazioni ed iniziative di interesse del Raggruppamento- a svolgere le attività di propria competenza nel rispetto delle normative vigenti e dei comuni principi di etica professionale, ed in particolare all'osservanza delle seguenti forme di condotta:

- improntare la propria attività a principi di trasparenza, correttezza e lealtà;
- promuovere una competizione leale, rifuggendo e stigmatizzando il ricorso a comportamenti illegittimi o comunque scorretti per raggiungere obiettivi economici;
- perseguire l'eccellenza della performance in termini di qualità, informando i propri comportamene a correttezza;
- mantenere con le Pubbliche Autorità locali, nazionali e sopranazionali relazioni ispirate alla piena e fattiva collaborazione, nel rispetto delle reciproche autonomie;
- non erogare contributi, vantaggi o altre utilità ai partiti politici ed alle organizzazioni sindacali, o a loro rappresentanti o candidati;
- non promettere vantaggi o altre utilità o effettuare erogazioni in denaro per finalità diverse da quelle istituzionali,
- non effettuare spese di rappresentanza con finalità diverse dalla mera promozione dell'immagine aziendale;
- non promettere o concedere omaggi o regalie non di modico valore,
- non fornire o promettere informazioni e/o documenti riservati;
- non favorire, nei processi d'acquisto, fornitori, sub-fornitori e consulenti indicati da rappresentanti della Stazione Appaltante;
- non esibire documenti/dati falsi od alterati,
- non tenere una condotta ingannevole che possa indurre la Stazione Appaltante in errore nella valutazione tecnico-economica dei prodotti e servizi offerti/forniti,
- non omettere informazioni dovute, al fine di orientare a proprio favore le decisioni della Stazione Appaltante;
- non ottenere e/o modificare informazioni a vantaggio dell'azienda, accedendo in maniera non autorizzata ai sistemi informativi della Pubblica Amministrazione o abusando della posizione di fornitore della Pubblica Amministrazione;
- non corrispondere ad alcuno, direttamente o attraverso terzi -ivi comprese /e imprese collegate o controllate, i propri collaboratori e consulenti - somme di denaro o altra utilità a titolo di Intermediazione o simili, volte a facilitare la conclusione di determinati atti da parte della PA.;
- non versare ad alcuno, a nessun titolo somme di denaro o altra utilità finalizzate a rendere meno onerosa l'esecuzione e la gestione degli affidamenti della PA rispetto agli obblighi assunti.

- *Esecuzione del contratto*

  - in sede di gestione contrattuale: la fattispecie a rischio può ricorrere, in particolare, nel caso in cui tali comportamenti siano finalizzati ad agevolare gli interessi della Società (ad es., acquisto di beni e servizi destinati ad utilizzi non direttamente correlabili all'oggetto contrattuale e prestazioni previste e non rese);

  - in sede di gestione di sistemi di Information & Communication Technology (ICT) per conto della PA: la fattispecie a rischio ricorre, in particolare, nel caso in cui tali comportamenti siano finalizzati ad alterare i sistemi stessi o ad intervenire sui dati a vantaggio della Società (ad es., per ottenere informazioni riservate inerenti a gare);

  - in sede di gestione di possibili modifiche o integrazioni del contratto: la fattispecie a rischio può ricorrere, in particolare, nel caso in cui tali comportamenti siano utilizzati per indurre i rappresentanti della PA a favorire la posizione della Società;

- *Collaudo/verifica del bene/servizio oggetto del contratto*

  - in sede di contatti preventivi e successivi al collaudo/verifica con i rappresentanti della PA: la fattispecie a rischio può ricorrere, in particolare, nel caso in cui tali comportamenti siano finalizzati ad indurre questi ultimi a favorire la posizione della Società;

  - in sede di collaudo/verifica da parte della PA: la fattispecie a rischio può ricorrere, in particolare, nel caso in cui tali comportamenti siano diretti ad influenzare, nell'interesse della Società, il giudizio dei collaudatori;

  - in sede di gestione di eventuali contestazioni con la PA: la fattispecie a rischio ricorre, in particolare, nel caso in cui tali comportamenti siano utilizzati per eludere obblighi di legge e per favorire gli interessi della Società;

- *Gestione del credito*

  - in sede di contestazione su esistenza ed ammontare del credito; la fattispecie a rischio può ricorrere, in particolare, nel caso in cui tali comportamenti siano utilizzati per indurre i rappresentanti della PA a favorire la posizione della Società.

1.F) FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni interessate devono comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco contratti/ordini di vendita di beni/servizi stipulati;

Flusso 2: elenco contestazioni in corso che la PA ha formalmente inoltrato alla Società oltre all'indicazione delle principali attività svolte per l'ente di riferimento.

1.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione
- Procedura organizzativa VAQ-CO-MP-02 "La procedura dei Contratti in Venis"
- Procedura organizzativa VAQ-AC-MP-01 "Albo dei fornitori in Venis"
- Procedura organizzativa VAQ-AC-MP-02 "Gli approvvigionamenti in Venis"
- Procedura organizzativa VAQ-AC-MP-04 "Gestione Gare"

2) "ACQUISIZIONI CON RUOLO PUBBLICISTICO – NEGOZIAZIONE, STIPULAZIONE ED ESECUZIONE DI CONTRATTI E DI CONVENZIONI DI CONCESSIONI, IN QUALITÀ DI STAZIONE APPALTANTE, NEL RISPETTO DELLE DISPOSIZIONI PREVISTE NEL DECRETO LEGISLATIVO 163/06, RECANTE CODICE DEI CONTRATTI PUBBLICI"

2.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività svolte, quale stazione appaltante per conto della Pubblica Amministrazione, per acquisire, tramite negoziazione, stipulazione ed esecuzione di contratti e di convenzioni in concessioni, forniture di beni e/o servizi mediante trattative private o con procedure ad evidenza pubblica. Il processo fa riferimento anche all'attività di gestione operativa delle commesse pubbliche.

Il processo si articola nelle seguenti fasi:

- Recepimento delle esigenze della PA;
- Individuazione dei criteri tecnico-economico-giuridici dell'appalto (in funzione dei quali si opera mediante trattativa privata o procedura ad evidenza pubblica) e redazione del capitolato tecnico;
- Individuazione e scelta del fornitore;
- Esecuzione contrattuale e collaudo.

2.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (art. 318, 319, 319-*bis*, e 320, c.p.); concussione (articolo 317 c.p.) e concussione per induzione (art. 319-*quater*); truffa aggravata in danno dello Stato, di altro Ente Pubblico e dell'Unione Europea (articolo 640, comma 2, n. 1, c.p.); malversazione a danno dello Stato (art. 316 *bis*).

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità (essendo rimasto invariato il testo dell'art. 319 c.p. – c.d. corruzione propria - al di là dell'inasprimento della pena).

Nel caso di specie, il reato potrebbe configurarsi nell'ipotesi di promessa, offerta, concessione di danaro o altra utilità da parte degli Uffici o dei soggetti responsabili dell'esecuzione delle opere e dei lavori alle amministrazioni competenti, affinché queste consentano che la Società non ottemperi agli obblighi, legislativi e contrattuali, relativi ad esempio all'attuazione del piano di esecuzione dei lavori. In particolare, avuto riguardo ai rapporti tra la PA e la Società in qualità di concessionario di costruzione e/o di gestione di opere pubbliche, si specifica che il reato di corruzione potrebbe configurarsi sia dal lato passivo (c.d. "corruzione passiva"), ovverosia laddove esponenti aziendali della Società, accettino, nell'ambito della gestione delle attività sopra indicate, per loro stessi o anche per terzi, danaro o altro vantaggio al fine di favorire l'affidamento dei lavori ad un determinato soggetto, che dal lato attivo, nel caso di promessa, offerta, concessione, diretta o indiretta, alla PA, per se stessa o per un terzo, di danaro o di altro vantaggio al fine di conservare il ruolo di stazione appaltante ovvero per altro indebito vantaggio (corruzione c.d. "attiva").

Il reato di **concussione** si verifica, oggi, nel caso in cui gli esponenti aziendali, in qualità di pubblici funzionari o di incaricati di pubblico servizio, abusino della loro posizione di "soggetto pubblico" per **"costringere"** taluno a dare o promettere a sé o ad altri, indebitamente, danaro o altra utilità, esercitando una "pressione psichica" sul privato.

Tale impostazione consegue alle innovazioni apportate in materia dalla L. 190/2012, alla quale è seguita la riformulazione dell'art. 317 del codice penale (che, come è agevole verificare, oggi non contiene più il riferimento all'"induzione", ma soltanto alla "costrizione" di alcuno a dare o promettere denaro o altre utilità).

La riforma, invero, ha reso la fattispecie di **concussione per induzione** un'autonoma forma di reato, contemplata dal nuovo art. 319-quater del Codice Penale con una modificazione consistente dell'originaria impostazione del nostro sistema penale che raggruppava in un'unica norma e sottoponeva alla stessa sanzione "*il costringere e l'indurre alcuno a dare o promettere indebitamente denaro od altra utilità*" (precedente formulazione dell'art. 317 c.p. - Concussione).

La nuova disciplina, a differenza dell'impostazione precedente, sancisce la punibilità anche del privato che perfeziona la dazione dell'indebito.

La sanzione pecuniaria a carico dell'impresa può arrivare sino ad Euro 1.200.000 (*unmilioneduecentomila/00*).

Nel caso di specie, il reato in questione potrebbe essere commesso da esponenti aziendali nel caso di richiesta a terzi di prestazioni non dovute, nell'interesse o a vantaggio della Società, sfruttando i poteri derivanti dal ruolo di "stazione appaltante" per conto della Pubblica Amministrazione.

Laddove Venis svolga il ruolo di concessionario di costruzione e/o di gestione di opere pubbliche, per conto o nell'interesse della Pubblica Amministrazione, il reato in questione si verificherebbe, ad esempio, nel caso di raggiungimento di un accordo con una società affidataria di lavori, al fine di consentire a quest'ultima di svolgere prestazioni fittizie, o per un valore di mercato inferiore a quello contrattualmente previsto, in cambio, ad esempio, di danaro o di altro vantaggio, con conseguente danno alla Pubblica Amministrazione.

E' chiaro, comunque, che il reato di concussione, rispetto alle altre figure criminose, è suscettibile di

un'applicazione piuttosto residuale.

Avuto riguardo alla nozione di pubblico ufficiale e di incaricato di pubblico servizio ed, in particolare, ai soggetti che possono rivestire questa funzione, si rimanda a quanto esposto nel paragrafo **A. Aree a rischio** della presente Parte Speciale.

Il reato di **truffa aggravata** si configura nel caso in cui, per realizzare un ingiusto profitto, siano poste in essere condotte artificiose ed idonee ad indurre in errore la Pubblica Amministrazione, con conseguente danno a suo carico.

In particolare, nel caso che ci occupa, il reato di truffa aggravata potrebbe essere commesso laddove, ad esempio, a seguito della conduzione non corretta dell'appalto (artifizio o raggiro concordato con la società appaltatrice) venissero ingannevolmente sovrastimati i beni ed i servizi offerti con conseguente danno patrimoniale alla PA..

Il reato di **malversazione** a danno dello Stato si configura nel caso di mancata destinazione di fondi pubblici allo scopo per il quale sono stati ottenuti.

Con riferimento all'attività di Venis il reato si potrebbe verificare laddove siano stati richiesti dei finanziamenti per la gestione di una determinata commessa ed i finanziamenti ottenuti (ad es. per lo sviluppo di una rete cittadina) siano stati destinati anche parzialmente a scopi diversi (ad es. consulenze, attività di supervisione) da quelli dichiarati nella domanda volta ad ottenere i fondi agevolati.

2.c) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l'Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti
- la Funzione Tecnologie, Servizi e Sviluppo
- il Responsabile del Procedimento
- la Funzione Comunicazione
- gli Incaricati della Progettazione
- la Direzione Lavori

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché

collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

2.D) SISTEMA DI CONTROLLO

Il sistema di controllo attivato in questo processo si basa sugli elementi qualificanti della **chiara e formalizzata separazione di ruolo** nelle fasi chiave del processo, della **tracciabilità degli atti** e della partecipazione di **membri esterni indipendenti**.

In particolare, gli elementi specifici di controllo sono:

- Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
    - Acquisizione dell’incarico,
    - Definizione delle specifiche (capitolato tecnico e d’oneri),
    - Gestione della gara d’appalto/negoziazione,
    - Effettuazione del collaudo;
- Nel caso di affidamento diretto è necessario procedere con l’espletamento di adeguata attività selettiva fra diversi offerenti e di obiettiva comparazione delle offerte (sulla base di criteri oggettivi e documentabili).
- Nel caso di Gara d’Appalto è necessaria:
    - l’esistenza di criteri tecnico-economici o giuridici per la qualificazione dei fornitori (ad es. Albo Fornitori, Consip o MEPA);
    - l’esistenza di una commissione di almeno tre membri, con responsabilità di valutazione e scelta del fornitore;
    - l’esistenza di una griglia valutativa (con elementi tecnici ed economici), preventivamente definita, da applicare alle offerte pervenute;
- Il conferimento di specifiche procure ai responsabili delle unità organizzative coinvolte al fine di dotarli del potere di rappresentanza della Società;
- Modalità strutturate per l’effettuazione delle prove di verifica da effettuare in sede di collaudo;
- Tracciabilità delle singole fasi del processo e in particolare della documentazione inerente alla procedura di scelta del contraente, eseguita in qualità di stazione appaltante, nel rispetto del Codice dei contratti pubblici;
- Devono inoltre essere definite adeguate modalità di escalation autorizzativa per la gestione delle eventuali deroghe ai criteri sopra definiti.

2.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo ed in particolare nelle seguenti attività:

- *Recepimento esigenze della PA e individuazione criteri tecnico-economici dell'appalto*
  - in sede di incontri con i rappresentanti della PA volti all'affidamento dell'incarico di stazione appaltante, quando tali comportamenti siano finalizzati a favorire la posizione della Società;
  - in sede di predisposizione della documentazione necessaria all'appalto, quando tali comportamenti siano finalizzati a favorire determinati fornitori (attraverso appositi capitolati tecnici o informazioni riservate) o ad assecondare indebite pressioni della PA.
- *Scelta del contraente ed esecuzione del contratto*
  - in fase di aggiudicazione dell'appalto, quando tali comportamenti siano finalizzati a favorire determinati fornitori indicati dalla PA;
  - in fase di esecuzione del contratto, quando tali comportamenti siano finalizzati a disattendere le clausole contrattuali (ad es. ritardi e penali).
- *Collaudo e ispezioni/controlli/verifiche*
  - in sede di collaudo da parte dell'apposita commissione e/o di ispezioni/controlli/verifiche da parte della PA, quando si tenda ad influenzarne il giudizio nell'interesse della Società e ad eventuale svantaggio della PA.

2.F) FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Il Responsabile della Funzione Acquisti quale stazione appaltante deve comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco contratti che conferiscono il ruolo di stazione appaltante;

Flusso 2: elenco situazioni gestite con modalità di escalation (in deroga);

Flusso 3: elenco degli appalti effettuati con importo inferiore (entro 5%) alla soglia di spesa oltre la quale è prescritta l'evidenza pubblica, oltre all'elenco delle principali attività svolte in qualità di stazione appaltante.

2.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei rapporti con la Pubblica Amministrazione

- Procedura organizzativa VAQ-CO-MP-02 "La procedura dei Contratti in Venis"
- Procedura organizzativa VAQ-AC-MP-01 "Albo dei fornitori in Venis"
- Procedura organizzativa VAQ-AC-MP-02 "Gli approvvigionamenti in Venis"
- Procedura organizzativa VAQ-AC-MP-04 "Gestione Gare"

3) "GESTIONE DEI RAPPORTI CON SOGGETTI PUBBLICI PER L'OTTENIMENTO DI AUTORIZZAZIONI, LICENZE, PROVVEDIMENTI AMMINISTRATIVI NECESSARI ALL'INSTALLAZIONE DI IMPIANTI E ATTIVITÀ STRUMENTALI"

3.A) DESCRIZIONE DEL PROCESSO

I processi relativi ad autorizzazioni e concessioni si riferiscono alle attività svolte per l'ottenimento di:

- autorizzazioni per l'installazione di impianti (ad es. scavi in suolo pubblico);
- provvedimenti amministrativi per lo svolgimento di attività strumentali impiantistiche.

con attenzione anche alla cura di adempimenti quali comunicazioni, dichiarazioni, deposito di atti e documenti e alla successiva gestione del rapporto con la PA.

Tali processi presentano uno sviluppo sostanzialmente analogo, articolato nelle seguenti fasi:

- Contatto con il soggetto pubblico per la rappresentazione dell'esigenza;
- Inoltro della richiesta, con eventuale negoziazione di specifiche tecnico-progettuali e di clausole contrattuali;
- Rilascio dell'autorizzazione o stipulazione del contratto;
- Gestione dei rapporti in costanza di autorizzazione o esecuzione contrattuale, con conclusiva verifica e/o collaudo;
- Gestione di ispezioni/accertamenti e/o dell'eventuale contenzioso.

3.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articoli 318, 319, 319 bis e 320, c.p.); truffa aggravata a danno dello Stato, di altro Ente pubblico o dell'Unione Europea (articolo 640, comma 2, n. 1, c.p.); frode informatica a danno dello Stato (articolo 640 ter, c.p.)

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per

l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

Nel caso di specie, il reato può configurarsi, in particolare, nel caso di promessa, offerta, concessione diretta o indiretta da parte degli Uffici o dei soggetti competenti della Società all'amministrazione aggiudicatrice, per se stessa o per un terzo, di danaro o di altro vantaggio al fine:

(i) di velocizzare una pratica burocratica;

(ii) di far omettere uno dei passaggi del procedimento autorizzatorio o concessorio e, più in generale,

(iii) di favorire il rilascio di concessioni ed autorizzazioni, la stipulazione del contratto o l'esito dell'ispezione.

Il reato di **truffa aggravata** si configura nel caso in cui, per realizzare un ingiusto profitto, quale, ad esempio, l'aggiudicazione di una concessione o il rilascio di un'autorizzazione, siano poste in essere condotte artificiose ed idonee al fine di indurre un erroneo convincimento nella Pubblica Amministrazione, ad esempio, circa il possesso di determinati requisiti.

Tale reato si verifica, ad esempio, nel caso di predisposizione, da parte dei soggetti o degli Uffici competenti della Società, di documentazione falsa contenente requisiti di idoneità tecnica non veritieri, al fine di favorire il rilascio di concessioni ed autorizzazioni oppure in una condotta ingannevole che rechi danno patrimoniale allo Stato (ad es. nel caso in cui nelle convenzioni per scavi, nelle quali è previsto un pagamento a misura, si dichiari un lavoro quantitativamente inferiore a quello effettivamente realizzato per dover corrispondere un minore importo).

Il reato di **frode informatica** si configura nel caso di distruzione, manipolazione di dati informatici della Società, rilevanti per la Pubblica Amministrazione, al fine di indurla in errore circa l'esistenza di determinati requisiti.

Tale reato potrebbe essere commesso nel caso di interventi non legittimi, attuati in qualsiasi modo, parte degli Uffici e dei soggetti competenti su programmi e sistemi informatici, al fine di sottrarre o di manipolare dati rilevanti per la Pubblica Amministrazione e di facilitare ed ottenere l'assegnazione di una concessione o il rilascio di un'autorizzazione.

3.c) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l'Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti

- la Funzione Tecnologie, Servizi e Sviluppo
- il Responsabile del Procedimento (eventualmente in relazione a ciascun contratto pubblico)
- gli Incaricati della Progettazione
- la Direzione Lavori

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nell’area di attività a rischio precedentemente individuata.

3.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **separazione di ruolo** nelle fasi chiave del processo e della **tracciabilità degli atti**. In particolare, gli elementi specifici di controllo sono di seguito rappresentati:

- la segregazione delle responsabilità, con attenta divisione dei ruoli, tra le aree/soggetti che svolgono le attività di:
    - presa di contatto con il soggetto pubblico per la richiesta di informazioni,
    - redazione dei modelli e/o documenti,
    - di presentazione dei modelli e/o documenti,
    - di gestione dei rapporti con i soggetti pubblici;
- l’esistenza di sistemi di verifica (ad es. la compilazione di schede informative, l’indizione di apposite riunioni) per perseguire il rispetto dei canoni di integrità, trasparenza e correttezza del processo;
- conferimento, ove necessario, di una procura, ai responsabili delle unità organizzative coinvolte al fine di dotarli del potere di rappresentare l’azienda dinanzi alla Pubblica Amministrazione;
- autorizzazione del vertice aziendale, o di altra funzione dallo stesso delegata, per la consegna di documentazione al soggetto pubblico;
- indicazione delle modalità di gestione di eventuali contestazioni;
- accertamento della congruenza fra quanto autorizzato, quanto realizzato e quanto dichiarato alla PA ai fini del pagamento dei corrispettivi previsti;
- tracciabilità degli atti e delle fonti informative nelle singole fasi dei processi con specifico riferimento ad impiego di risorse e tempi e della documentazione eventualmente richiesta e consegnata al soggetto pubblico;

- formalizzazione degli eventuali rapporti con soggetti esterni (consulenti, terzi rappresentanti o altro) incaricati di svolgere attività a supporto della Società, prevedendo nei contratti una specifica clausola che li vincoli al rispetto dei principi etico-comportamentali adottati dalla Società[3];

- Selezione ed utilizzo di fornitori da Albo Fornitori (pubblici o della Società) qualificati e modalità operative finalizzate a valutazione anche nei confronti dei professionisti esterni di cui ci si avvale.

- devono, inoltre, essere definite adeguate modalità di escalation autorizzativa per la gestione delle eventuali deroghe ai principi sopra esposti.

3.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- in sede di predisposizione e presentazione della documentazione necessaria, quando tali comportamenti siano utilizzati per influire nella stipulazione del contratto o nel rilascio dell’autorizzazione;

- in sede di ispezioni/accertamenti da parte della PA, quando tali comportamenti siano finalizzati ad influenzare, nell’interesse della Società, il giudizio/parere dei rappresentanti pubblici intervenuti.

3.F) FLUSSI INFORMATIVI VERSO L’ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni interessate al rilascio di autorizzazioni da parte della PA, alla stipula di contratti di concessione e alla firma di convenzioni, devono presentare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco provvedimenti ottenuti e contratti stipulati, con l’indicazione:

- dell’ente/ufficio competente,

- dei riferimenti del referente della Pubblica Amministrazione contattato (nome, cognome, qualifica e incarico ricoperto);

Flusso 2: elenco contestazioni e contenziosi in corso promossi dalla PA, oltre all’indicazione delle principali iniziative/attività svolte.

3.G DOCUMENTI DI RIFERIMENTO

- Codice Etico

[3] Il testo standard della clausola è riportato nel Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, nota 1.

- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione

4) "FINANZA AGEVOLATA – RICHIESTA E OTTENIMENTO DI FINANZIAMENTI, CONTRIBUTI, EROGAZIONI DA PARTE DI AMMINISTRAZIONI PUBBLICHE; ATTIVITÀ DI GESTIONE DEI FINANZIAMENTI STESSI PER L'ESECUZIONE DI GRANDI OPERE E/O DI PROGETTI FINANZIATI"

4.A) DESCRIZIONE DEL PROCESSO

Il processo si compone delle attività di:

- Individuazione delle fonti di finanziamento, di cui si può beneficiare;
- Predisposizione delle operazioni di richiesta/istruttoria per l'ottenimento di finanziamenti, contributi ed erogazioni da parte di pubbliche amministrazioni;
- Approvazione della richiesta e stipulazione del contratto;
- Acquisizione e gestione del finanziamento agevolato (a titolo di acconto[4] e/o saldo);
- Verifiche ed ispezioni da parte dell'Ente finanziatore;
- Rendicontazione dell'attività.

4.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articoli 318 e 319, 319 bis, 320, c.p.); truffa aggravata per il conseguimento di erogazioni pubbliche (640 bis); malversazione a danno dello Stato o dell'Unione Europea (316 bis c.p.); indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (316 ter c.p.).

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

Nel caso di specie, il reato si verificherebbe, ad esempio, in caso di promessa, offerta o concessione, da parte degli Uffici coinvolti nella procedura di richiesta dei fondi, all'amministrazione competente, per se stessa o per un terzo, di somme di danaro o di altri vantaggi, al fine di indurre quest'ultima a rilasciare finanziamenti, erogazioni e contributi alla Società stessa o a terzi ovvero ad emettere o ritardare verifiche o altri atti dovuti.

[4] La richiesta di erogazione a titolo di acconto avviene, di norma in conformità con le regole definite dall'ente finanziatore, sulla base di semplice dichiarazione a firma del Legale Rappresentante dell'azienda richiedente, senza specifico obbligo di rendicontazione.

Il reato di **truffa aggravata per il conseguimento di erogazioni pubbliche** si configura nel caso in cui, al fine di conseguire contributi, finanziamenti, mutui agevolati, siano poste in essere condotte artificiose ed idonee ad indurre un erroneo convincimento nella Pubblica Amministrazione, con conseguente danno all'erario.

Le modalità di condotta tipiche del reato di **indebita percezione di erogazioni ai danni dello Stato** sono, in questo caso, molto simili a quelle del reato di truffa aggravata. La condotta materiale di questa fattispecie delittuosa è costituita dalla presentazione di documenti falsi, dall'omissione di informazioni obbligatorie, dal rilascio di autorizzazioni alla presentazione di domande di finanziamento senza verificare la sussistenza o meno dei requisiti richiesti, per conseguire, indebitamente, contributi o finanziamenti comunque denominati, concessi o erogati dallo Stato, da enti pubblici o dalle Comunità Europee.

Nel caso di specie, con riferimento all'attività di Venis, entrambi i reati si verificherebbero nel caso di predisposizione artificiosa di documentazione contenente informazioni non veritiere circa il possesso dei requisiti tecnici, la tipologia di progetto da realizzare, la situazione finanziaria, da parte dei soggetti e degli Uffici competenti, al fine di indurre l'amministrazione competente ad erogare il finanziamento.

Il reato di **malversazione a danno dello Stato** si configura nel caso di mancata destinazione dei fondi allo scopo per il quale sono stati ottenuti.

Nel caso di specie, il reato si verificherebbe nel caso di destinazione delle somme ottenute da parte dei soggetti e degli Uffici competenti a scopi diversi da quelli dichiarati nella domanda volta ad ottenere i fondi, agevolati o meno.

Avuto riguardo all'intera area critica in commento, si segnala che il reato di "frode nelle sovvenzioni" è uno dei più diffusi, riguardando, in generale, tutti i fenomeni di "indebita captazione" ovvero di "illecita utilizzazione dei fondi".

4.c) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l'Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti
- la Funzione Tecnologie, Servizi e Sviluppo
- il Responsabile del Procedimento

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

4.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **separazione di ruolo** nelle fasi chiave del processo, della **tracciabilità degli atti e** nella effettuazione di specifiche **attività di riscontro degli avanzamenti progettuali**. In particolare, gli elementi specifici di controllo sono di seguito rappresentati:

- individuazione di attori con responsabilità distinte e operanti nelle diverse fasi/attività di:
    - Individuazione delle fonti di finanziamento, di cui si può beneficiare, e presa di contatto con il soggetto pubblico per la richiesta di informazioni;
    - predisposizione della documentazione per la richiesta di finanziamenti, contributi ed erogazioni da parte di pubbliche amministrazioni (ad es. redazione dei modelli e/o documenti);
    - presentazione della documentazione;
    - Successiva gestione dei rapporti con i soggetti pubblici (ad es. nella fase di stipulazione del contratto);
    - Realizzazione dell'attività oggetto di finanziamento;
    - Collaudo delle realizzazioni o certificazione dell'esecuzione di lavori/prestazioni;
    - Predisposizione dei rendiconti dei costi.

con attenta divisione dei ruoli e delle responsabilità.

Inoltre, con specifico riferimento alla fase di richiesta del finanziamento/contributo/erogazione:

- conferimento di specifiche procure ai responsabili delle unità organizzative coinvolte;
- autorizzazione del vertice aziendale, o di altra funzione dallo stesso delegata, per la consegna di documentazione al soggetto pubblico;
- tracciabilità degli atti e delle fonti informative nelle singole fasi dei processi con specifico riferimento ad impiego di risorse e tempi e della documentazione eventualmente richiesta e consegnata al soggetto pubblico;
- circolazione di informazioni di dettaglio alle Funzioni sopra indicate con riguardo alla destinazione prevista dei finanziamenti, come evidenziata in sede di relativa domanda;
- formalizzazione degli eventuali rapporti con soggetti esterni (consulenti, terzi rappresentanti o altro) incaricati di svolgere attività a supporto della Società, prevedendo nei contratti una specifica clausola che li vincoli al rispetto dei principi etico-comportamentali adottati dalla Società[5];

[5] Il testo standard della clausola è riportato nelProtocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, nota 1.

- previsione di sistemi di verifica (ad es. la compilazione di schede informative, l’indizione di apposite riunioni) per perseguire il rispetto dei canoni di integrità, trasparenza e correttezza del processo

Con specifica attenzione alla fase di esecuzione dell’opera/progetto finanziato:

- Assegnazione della responsabilità di presidio unitario delle attività tecnico-realizzative per ogni progetto finanziato;
- Definizione, per ogni progetto, di un piano di informazione, verso tutte le strutture coinvolte, circa le regole di attuazione degli interventi finanziati e della loro successiva gestione;
- Effettuazione del collaudo delle realizzazioni o certificazione dell’esecuzione di lavori/prestazioni;
- Esistenza di riconciliazione fra dati tecnici ed amministrativi e di connessa verifica di finanziabilità delle spese esposte;
- Effettuazione di verifica di congruenza degli stati di avanzamento del progetto con il piano finanziario definito dal contratto;
- Esistenza di un organismo di controllo, costituito da personale tecnico ed amministrativo per monitorare lo stato di avanzamento del progetto, in conformità con le regole di attuazione definite, con interventi di verifica in corso d’opera;

4.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- *Approvazione della concessione del finanziamento contributo*
    - in sede di incontri con i rappresentanti degli Istituti finanziari e/o della PA nel corso della istruttoria, quando tali comportamenti siano mirati al superamento di vincoli o criticità ai fini della concessione del finanziamento agevolato/contributo;
    - in sede di presentazione della documentazione prescritta dalla normativa per la concessione del finanziamento agevolato/contributo, quando tali comportamenti (ad es. dichiarazioni false circa agevolazioni ottenute) siano utilizzati per indurre i rappresentanti di tali Enti a favorire la Società;
    - in sede di approvazione della concessione del finanziamento agevolato/contributo, quando tali comportamenti siano finalizzati a poter disporre di particolari privilegi o ad agevolare, tramite iniziative non trasparenti e non formalizzate sul piano aziendale, gli interessi della Società;
- *Acquisizione e gestione di eventuali erogazioni a titolo di anticipo/acconto*
    - in sede di emissione dei provvedimenti di erogazione, da parte degli Organi competenti: quando tali comportamenti siano finalizzati ad agevolare gli interessi della Società;

- in sede di adempimenti degli obblighi di legge/normativi e convenzioni per il conseguimento degli anticipi/acconti previsti dalla legge, quando tali comportamenti siano diretti a rappresentare - agli Istituti Finanziari ed alla PA - informazioni non veritiere e/o non complete o ad eludere obblighi di legge/normativi;

- *Realizzazione del progetto*
  - in sede di attuazione degli interventi finanziati, quando tali comportamenti siano diretti ad evitare, anche in parte, l’osservanza degli adempimenti di legge/amministrativi;
  - in sede di utilizzo di finanziamenti agevolati/contributi, quando tali comportamenti siano diretti a destinare i fondi ricevuti a finalità differenti, da quelle prescritte da leggi/normative di concessione;
  - in sede di ispezioni/controlli/verifiche da parte degli Organismi specifici, quando tali comportamenti siano finalizzati ad influenzare, nell’interesse della Società, il giudizio/parere di tali Organismi;
- *Consuntivazione e rendicontazione dei costi del progetto*
  - in sede di predisposizione degli stati avanzamento lavori, quando tali comportamenti (es., presentazione di documenti di consuntivazione e rendicontazione non corretti e non veritieri) siano utilizzati per agevolare la posizione della Società;
  - in sede di ispezioni/controlli/verifiche, da parte degli addetti degli Istituti Finanziari e/o della PA, quando tali comportamenti siano finalizzati ad influenzare, nell’interesse della Società, il giudizio/parere di tali addetti.

4.F) FLUSSI INFORMATIVI VERSO L’ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni interessate all’erogazione di contributi/finanziamenti devono presentare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco finanziamenti richiesti ed ottenuti, con l’indicazione:

- dell’ente/ufficio competente,
- dei riferimenti del referente della Pubblica Amministrazione contattato (nome, cognome, qualifica e incarico ricoperto);

Flusso 2: elenco risultanze delle verifiche/ispezioni effettuate dalla PA.

4.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico

- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione

5) "GESTIONE DEI RAPPORTI CON I SOGGETTI PUBBLICI PER GLI ASPETTI CHE RIGUARDANO GLI ADEMPIMENTI, VERIFICHE E ISPEZIONI RELATIVI ALLA PRODUZIONE DI RIFIUTI ED EMISSIONI INQUINANTI"

5.A) DESCRIZIONE DEL PROCESSO

Il processo è composto dalle attività necessarie a garantire il rispetto delle normative in materia di tutela ambientale ed a certificare l'attuazione degli adempimenti in materia di rifiuti, emissione di fumi o la produzione di inquinamento acustico e/o elettromagnetico agli organismi pubblici preposti ai controlli.

Il processo si articola sostanzialmente in due fasi:

- Gestione degli adempimenti:
    - per inquinamento acustico/elettromagnetico,
    - relativi allo smaltimento rifiuti;
- Gestione di ispezioni e verifiche.

5.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articoli 318, 319, 319 bis e 320, c.p.); truffa aggravata a danno dello Stato, di altro Ente pubblico o dell'Unione Europea (articolo 640, comma 2, n. 1, c.p.)

Va evidenziato che, per le attività da essa svolte in tema di predisposizione e messa in opera di reti informative e sistemi applicativi, tale da comportare l'uso o sviluppo di apparati soggetti a particolari tutele di smaltimento sia in ragione della tipologia di beni (rifiuti di apparecchiature elettriche ed elettroniche – RAEE) sia in ragione delle tutele dovute in tema di sicurezza dei dati personali con relativi obblighi di trattamento specifico dello smaltimento ai sensi del Provvedimento del Garante per la Tutela dei Dati Personali del 13 ottobre 2008, le responsabilità in materia nella Società coinvolgono diverse Funzioni interne, demandate a vario titolo anche ad interagire direttamente con organismi esterni deputati ad alcune specifiche funzioni di trattamento o smaltimento.

Con riguardo ai sistemi trasmissivi senza filo passibili di inquinamento elettromagnetico, personale della Società può risultare coinvolto a diverso titolo nello sviluppo talvolta con apparati wireless per reti di accesso o di trasporto di segnali, motivo per il quale riveste particolare importanza il controllo e rispetto delle norme sulle certificazioni degli apparati ed omologazione di impianti.

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o

abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

Nel caso di specie, il reato di corruzione potrebbe verificarsi, ad esempio, sia nelle fasi di gestione degli adempimenti sia nell'ambito di ispezioni e verifiche, nel caso di promessa, offerta o concessione, da parte degli Uffici coinvolti o dei soggetti competenti della società, di denaro o altro vantaggio al fine di perseguire illecitamente finalità per le quali non sussistano i requisiti, fra le quali il rilascio di autorizzazioni, il rilascio di certificazione attestante la conformità alle prescrizioni di legge, la mancata irrogazione di sanzioni, etc.

Il reato di **truffa aggravata** si configura nel caso in cui, per realizzare un ingiusto profitto, quale, ad esempio, l'aggiudicazione di una concessione o il rilascio di un'autorizzazione, siano poste in essere condotte artificiose ed idonee al fine di indurre un erroneo convincimento nella Pubblica Amministrazione.

Nel caso di specie il reato di truffa a danno dello Stato potrebbe configurarsi ove, a seguito di decisioni o provvedimenti degli organi di controllo fondati su documentazioni false e/o alterate predisposte dagli Uffici coinvolti o condotte volutamente subdole/artificiose poste in essere dagli stessi Uffici, derivasse un danno patrimoniale alla PA (ad es. l'onere sostenuto per bonifiche ambientali a seguito dell'inosservanza delle normative in materia) con ingiusto profitto per la Società.

5.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l'Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti
- la Funzione Tecnologie, Servizi e Sviluppo
- la Direzione Lavori

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

5.D) IL SISTEMA DI CONTROLLO

Il sistema di controllo si basa sull'elemento qualificante della **tracciabilità delle fasi del processo** e sulla **separazione di ruolo**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- segregazione delle responsabilità tra le aree/soggetti che svolgono le attività di:
    - presa di contatto con il soggetto pubblico per la richiesta di informazioni,
    - di redazione dei modelli e/o documenti,
    - di presentazione dei modelli e/o documenti,
    - di gestione dei rapporti con i soggetti pubblici;
- tracciabilità delle singole attività (documentazione a supporto, verbalizzazione delle decisioni, intestazione/formalizzazione dei documenti) demandate alle funzioni coinvolte;
- verifica della corrispondenza delle dichiarazioni/certificazioni presentate all’Azienda con la documentazione tecnica di supporto, anche con riferimento a certificazioni e omologazione di apparati o impianti;
- protocollo dei flussi documentali fra le Funzioni dell’Azienda e gli organi della PA deputati al rilascio di autorizzazioni e/o di certificazione attestante la conformità alle prescrizioni di legge o deputati all’effettuazione di ispezioni e verifiche.

5.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo ed in particolare nelle seguenti attività:

- in sede di incontri formali e informali, per indurre i rappresentanti dell’Amministrazione a favorire il rilascio delle certificazioni/autorizzazioni;
- in sede di predisposizione della documentazione necessaria, per influire nella scelta del rilascio delle certificazioni/autorizzazioni;
- in sede di ispezioni e verifiche, per influenzare, nell’interesse della Società, il giudizio/parere degli Organismi di controllo.

5.F) FLUSSI INFORMATIVI VERSO L’ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni coinvolte nella fase di ispezione e verifica devono comunicare, con periodicità definita, quanto segue:

Flusso 1: elenco ispezioni e verifiche in corso, per inquinamento acustico/elettromagnetico e per rifiuti.

5.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione

6) "GESTIONE AMMINISTRATIVA DEGLI OBBLIGHI PREVIDENZIALI E FISCALI DEL PERSONALE DIPENDENTE E DEI COLLABORATORI. GESTIONE DEI RELATIVI ACCERTAMENTI, DELLE ISPEZIONI"

6.A) SVOLGIMENTO DEL PROCESSO

Il processo si riferisce alle attività svolte per l'adempimento degli obblighi legislativi in materia di trattamenti previdenziali del personale dipendente e dei collaboratori (gestione delle agevolazioni contributive e assistenziali, gestione delle dichiarazioni e liquidazione di imposte, tasse, canoni, etc.).

Il processo si articola nelle seguenti fasi:

- Determinazione degli importi da versare (sulla base delle retribuzioni e dei compensi) e predisposizione delle dichiarazioni prescritte dalla legge (Emens, F24, CUD, 770, ecc.);
- Approvazione delle dichiarazioni per gli Enti;
- Invio (prevalentemente telematico) dei moduli e versamento dei relativi importi;
- Visite ispettive (eventuali).

6.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articolo 318 c.p. e 319, c.p.); truffa aggravata in danno dello Stato, di altro Ente pubblico o dell'Unione Europea (articolo 640, comma 2, n. 1, c.p.); frode informatica ai danni dello Stato (articolo 640 ter, c.p.).

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

Nel caso in esame, il reato potrebbe essere commesso laddove venissero promessi, offerti, concessi danaro o altre utilità, in modo diretto o indiretto, a funzionari di enti ed amministrazioni competenti, da parte dei soggetti e degli Uffici competenti della Società, durante lo svolgimento di ispezioni e controlli, al fine di evitare l'applicazione di una sanzione, di negoziare l'applicazione di una sanzione pecuniaria di minor valore, di ritardare l'esito di una indagine.

La **truffa aggravata** si configura nel caso di condotte artificiose finalizzate ad indurre erronei convincimenti nei funzionari della Pubblica Amministrazione ed a conseguire un profitto ingiusto.

Nel caso in esame, la truffa potrebbe essere commessa qualora venissero sottoposti o inoltrati alla Pubblica Amministrazione documenti falsi, artefatti, incompleti (ad es., invio di moduli DM10 artatamente non corretti), al fine di indurre in errore i funzionari delle amministrazioni competenti, per evitare, ad esempio, l'applicazione di sanzioni amministrative , procurando un ingiusto profitto per la Società ed cagionando un danno patrimoniale alla PA.

Il reato di **frode informatica** si configura nel caso di creazione di un'anomalia di funzionamento o di distruzione dei dati di un software della Società, contenente dati rilevanti per la Pubblica Amministrazione, al fine di sottrarli al suo controllo.

Nell'ipotesi in esame, il reato di frode informatica potrebbe essere commesso nel caso di interventi non legittimi, attuati in qualsiasi modo, su programmi e sistemi informatici, da parte degli Uffici e dei soggetti competenti della Società, al fine di sottrarre o di manipolare dati rilevanti per la Pubblica Amministrazione, evitando l'applicazione di una sanzione o favorendo l'applicazione di una sanzione minore.

6.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l'Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza, Bilancio e Amministrazione del Personale

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

6.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **tracciabilità** degli atti. In particolare, gli elementi specifici di controllo sono di seguito rappresentati:

- Verifica di conformità fra dati forniti dai sistemi di amministrazione del personale e dati dichiarati;
- Tracciabilità degli atti e delle fonti informative nelle singole fasi del processo.

6.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione in tutte le fasi del processo ed in particolare nelle seguenti attività:

- *Determinazione degli importi e predisposizione delle dichiarazioni*
    - in sede di raccolta della documentazione e predisposizione della dichiarazione quando tali comportamenti siano diretti a rappresentare alla PA informazioni non vere e/o non complete o ad eludere obblighi di legge;
- *Visite ispettive da parte della PA*
    - in sede delle suddette visite, quando tali comportamenti siano finalizzati ad influenzare, nell'interesse della Società, le relative risultanze (producendo un danno patrimoniale per la PA).

6.F) FLUSSI INFORMATIVI CON L'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni coinvolte nelle fasi eventuali di ispezione e verifica devono comunicare, con periodicità definita, quanto segue:

Flusso 1: elenco ispezioni e verifiche in corso

6.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione

7) "ALTRI RAPPORTI CON LO STATO, LE REGIONI, GLI ENTI LOCALI ED ALTRE AMMINISTRAZIONI PUBBLICHE ITALIANE ED ESTERE , NONCHÉ CON AUTORITÀ DI VIGILANZA REGOLAMENTAZIONE E GARANZIA"

7.A) DESCRIZIONE DEL PROCESSO

I processi riguardano i rapporti diversi da quelli considerati nelle precedenti aree a rischio, con lo Stato, le Regioni, gli Enti Locali ed altre amministrazioni pubbliche (di seguito dette anche nel complesso "le altre amministrazioni pubbliche"), italiane ed estere, nonché con Autorità di Vigilanza, di Regolazione e di Garanzia.

In particolare si fa riferimento ai casi di :

- richieste di autorizzazioni/licenze/concessioni diverse da quelle previste nella precedente area **A.3,** in particolare per la gestione di offerta di servizi di telecomunicazioni;

- istruttorie, ispezioni, indagini campionarie e controlli nei confronti della Società, da parte di Ministeri ed altre amministrazioni competenti (ad es. Autorità Garante per la Privacy, Autorità Garante delle Comunicazioni, Ministero dello Sviluppo Economico, Ministero delle Finanze, Enti Previdenziali, Ministero dell'Ambiente, Ministero della Sanità, Autorità Garante della Concorrenza e del Mercato, etc.);

- agli obblighi di informativa specifici nei confronti di Autorità Indipendenti/Organismi di Vigilanza quali l'Osservatorio sui lavori pubblici – sezioni regionali e sezione centrale – e l'Autorità di Vigilanza sui Contratti Pubblici (AVCP).

Tali processi presentano uno sviluppo sostanzialmente analogo, che si può considerare sinteticamente articolato nelle seguenti fasi:

- Istruttoria interna e predisposizione documentale;

- Presentazione della richiesta di provvedimento o trasmissione degli atti o rappresentazione della posizione dell'Azienda;

- Gestione del rapporto in costanza d'autorizzazione/benestare, comprese verifiche ed ispezioni ed eventuale contenzioso.

7.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articolo 318, 319, 319 bis, 320, c.p.); truffa aggravata a danno dello Stato, di altro Ente pubblico o dell'Unione Europea (articolo 640, comma 2, n. 1, c.p.).

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

Nel caso in esame, il reato potrebbe essere compiuto mediante la promessa, l'offerta, la concessione diretta o indiretta, da parte dei soggetti e degli Uffici competenti della Società, a funzionari dei Ministeri o delle Autorità, per se stessi o per un terzo, di danaro o di altro vantaggio, al fine di influenzare posizioni e decisioni dei predetti soggetti in merito ad eventuali istruttorie, accertamenti contributivi, indagini o controlli in corso ovvero al fine di ottenere indebitamente decisioni o provvedimenti favorevoli.

Il reato di **truffa aggravata** si configura nel caso in cui, per realizzare un ingiusto profitto, siano poste in essere condotte artificiose idonee ad indurre in errore la Pubblica Amministrazione, con conseguente danno all'erario.

Tale reato potrebbe essere compiuto nel caso di elaborazione di falsi, di predisposizione artefatta di documenti anche contabili da parte dei soggetti e degli Uffici competenti della Società, al fine di ottenere indebiti favori o di negoziare sanzioni minori, con conseguente danno per l'Erario.

7.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell’Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l’Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti
- la Funzione Tecnologie, Servizi e Sviluppo
- il Responsabile del Procedimento

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

7.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave del processo e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
    - Predisposizione di dati/informazioni/documenti da fornire alle Autorità,
    - Presentazione di dati/informazioni/documenti alle altre amministrazioni pubbliche;
- esistenza di direttive sulle modalità di condotta operativa da adottare nei contatti formali ed informali intrattenuti con le amministrazioni pubbliche e le Autorità (ad es. la compilazione di schede informative, l’indizione di apposite riunioni) per perseguire il rispetto dei canoni di integrità, trasparenza e correttezza del processo;
- formalizzazione degli eventuali rapporti con soggetti esterni (consulenti legali, terzi rappresentanti o altro) incaricati di svolgere attività a supporto della Società, prevedendo nei contratti una specifica clausola che li vincoli al rispetto dei principi etico-comportamentali adottati dalla Società[6];
- definizione dettagliata dei ruoli e delle responsabilità in merito alla gestione dei contatti/rapporti con le amministrazioni pubbliche e con le Autorità di settore. In particolare prevedere che i contatti con gli

[6] Il testo standard della clausola è riportato nel Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, nota 1.

interlocutori istituzionali e con le Autorità avvengono esclusivamente tramite referenti o responsabili di Funzioni che abbiano ricevuto esplicito mandato dal vertice della Venis

- conferimento di specifiche procure, ai responsabili delle unità organizzative coinvolte al fine di dotarli del potere di rappresentare l’azienda, ove necessario, dinanzi alle altre amministrazioni pubbliche ed alle Autorità;

- l’autorizzazione del vertice aziendale, o di altra funzione dallo stesso delegata, per la consegna di documentazione richiesta e/o consegnata alle altre amministrazioni pubbliche ed alle Autorità,

- Rendicontazione dei rapporti formali con rappresentanti della amministrazioni pubbliche[7] e tracciabilità degli atti e delle fonti documentali che ne stanno alla base.

7.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al Presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- *Istruttoria interna e presentazione*

    - in sede di rapporti con Organismi di Vigilanza/Ministero dello Sviluppo Economico, volti alla definizione e rappresentazione della posizione della Società: la fattispecie a rischio può ricorrere, in particolare, nel caso in cui tali comportamenti siano utilizzati per indurre a favorire gli interessi della Società (ad es. mediante la fornitura di dati/informazioni non veritieri);

    - nel corso della fase istruttoria promossa da AGCOM/Ministero dello Sviluppo Economico a fronte di domande e istanze per il conseguimento di puntuali autorizzazioni; la fattispecie a rischio può ricorrere, in particolare, nel caso in cui tali comportamenti siano mirati al superamento di vincoli o criticità ai fini del rilascio dei citati provvedimenti da parte della PA;

- *Gestione del rapporto*

    - nel corso della gestione delle autorizzazioni/licenze: la fattispecie a rischio ricorre, in particolare, nel caso in cui tali comportamenti siano finalizzati ad evitare, anche in parte, l’osservanza degli adempimenti di legge/amministrativi o, comunque, a poter disporre di particolari privilegi;

    - in sede di adempimenti conseguenti agli obblighi di legge/normativi e di attività di gestione in genere; la fattispecie a rischio ricorre, in particolare, nel caso in cui tali comportamenti siano diretti a rappresentare alle Istituzioni Pubbliche dati/informazioni non corretti, con la finalità di perseguire “posizioni privilegiate” nell’interesse della Società o di eludere obblighi di legge/normativi;

    - in sede di ispezioni/controlli/verifiche da parte di Organismi di Vigilanza/Ministero dello Sviluppo Economico: la fattispecie a rischio può ricorrere, in particolare, nel caso in cui tali

[7] Con il termine “rappresentanti della PA” si intendono anche i soggetti (es. consulenti; società private, etc.) che operano su mandato/per conto di un Ente della PA.

comportamenti siano finalizzati a influenzare, nell'interesse della Società, il giudizio/parere dei citati Autorità/Organismi/Ministero;

- in sede di conciliazione/contenzioso: la fattispecie a rischio può ricorrere, in particolare, nel caso in cui tali comportamenti siano finalizzati a influenzare le decisioni dell'Organo giudicante.

7.F) FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni coinvolte nella gestione dei rapporti istituzionali ed Autorità devono comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco delle richieste e dei relativi provvedimenti ottenuti per licenze, concessioni e autorizzazioni, per la gestione dei servizi di telecomunicazioni.

Flusso 2: elenco delle eventuali istruttorie ed ispezioni/controlli in corso, oltre all'indicazione delle principali iniziative/attività svolte nei confronti delle amministrazioni pubbliche o delle Autorità.

7.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione

8) "PROCEDIMENTI GIUDIZIALI CON LA PUBBLICA AMMINISTRAZIONE"

8.A) DESCRIZIONE DEL PROCESSO

Il processo concerne tutte le attività di gestione dei contenziosi (incluse le fasi di pre-contenzioso) civili, penali ed amministrativi con la Pubblica Amministrazione – derivanti da contratti stipulati dalla Società con soggetti pubblici e da altri rapporti con la PA[8].

Il processo si articola nelle seguenti fasi:

- Accertamento preliminare e pre-contenzioso;
- Apertura del contenzioso;
- Gestione del procedimento;
- Conclusione con sentenza.

[8] Per gli altri tipi di contenzioso, cfr. il successivo paragrafo A.9 Area a rischio "Procedimenti giudiziali con soggetti terzi non pubblici".

8.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articolo 318, 319, 319 bis, e 320, c.p.), corruzione in atti giudiziari (art. 319 ter, c.p.) e truffa aggravata a danno dello Stato, di altro Ente pubblico o dell'Unione Europea (articolo 640, comma 2, n. 1, c.p.) .

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

Nel caso in esame esso potrebbe essere commesso nei confronti di rappresentanti della Pubblica Amministrazione quale controparte del contenzioso, al fine di ottenere illecitamente decisioni giudiziali e/o stragiudiziali favorevoli.

Il reato di **corruzione in atti giudiziari** si configura quando le condotte tipiche del reato di corruzione siano poste in essere per favorire o danneggiare una parte in un processo, con l'eventuale aggravante dell'ingiusta condanna di qualcuno.

Nel caso di specie esso potrebbe essere commesso nei confronti di Giudici competenti a giudicare sul contenzioso di interesse di Venis (compresi gli ausiliari e i periti d'ufficio) nell'ipotesi di promessa, offerta, concessione di danaro o di altro vantaggio al fine di influenzare le loro decisioni.

Il reato di **truffa aggravata** si configura nel caso in cui, per realizzare un ingiusto profitto siano poste in essere condotte artificiose ed idonee al fine di indurre un erroneo convincimento nella Pubblica Amministrazione.

Nel caso di specie, il reato di truffa aggravata a danno dello Stato potrebbe configurarsi ove, a seguito della decisione espressa dall'Organo Giudicante, fondata su prove documentali false e/o alterate o condotte volutamente subdole/artificiose, derivasse un danno patrimoniale nei confronti della PA, con ingiusto profitto per la Società.

8.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l'Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti

- la Funzione Tecnologie, Servizi e Sviluppo

- il Responsabile del Procedimento

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni , legali e procuratori e partner operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

8.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **tracciabilità** e della puntuale **registrazione della documentazione**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Tracciabilità delle fasi operative, degli atti e delle fonti informative, con riguardo anche a tempi e risorse coinvolte;

- Protocollo dei documenti aziendali ufficiali diretti (tramite legali esterni e periti di parte) ai Giudici– compresi i Periti d’ufficio dagli stessi designati – competenti a giudicare sul contenzioso di interesse di Venis, e/o ai rappresentanti della Pubblica Amministrazione quale controparte del contenzioso;

- Verifica delle attività svolte al fin di garantire che le stesse siano adeguatamente documentate e che la documentazione sia conservata in apposito archivio, con divieto di cancellare o distruggere arbitrariamente i documenti archiviati;

- Valutazione di congruità formale dei flussi documentali e di esperibilità delle azioni funzionali al procedimento.

8.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al Presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo ed in particolare nelle seguenti attività:

- in sede di incontri formali e informali, anche a mezzo di legali esterni e periti di parte, per indurre Giudici (compresi gli ausiliari e i Periti d’ufficio), nonché i rappresentanti della Pubblica Amministrazione quale controparte del Contenzioso, a favorire gli interessi della Società;

- nel corso delle fasi del procedimento, anche a mezzo di legali esterni e periti di parte, per ottenere il superamento di vincoli o criticità ai fini della tutela degli interessi della Società;

- in sede di ispezioni/controlli/verifiche da parte degli Organismi pubblici o periti d’ufficio, per influenzarne il giudizio/parere nell’interesse della Società, anche a mezzo di legali esterni e periti di parte;

- in sede di decisione del contenzioso, per influenzare le posizioni della Pubblica Amministrazione quale controparte del contenzioso e le decisioni dell'Organo giudicante, anche a mezzo di legali esterni e periti di parte.

8.F) FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Il Responsabile della Funzione interessata deve comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco contenziosi civili, penali, amministrativi in corso e conclusi con la Pubblica Amministrazione.

8.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei rapporti con la Pubblica Amministrazione.

9) "PROCEDIMENTI GIUDIZIALI CON SOGGETTI TERZI NON PUBBLICI"

9.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce a tutte le attività di gestione dei contenziosi civili, penali ed amministrativi (incluse le fasi di precontenzioso) con soggetti terzi non pubblici.

I processo si articola nelle seguenti fasi:

- Pre-contenzioso;
- Apertura del contenzioso;
- Gestione del procedimento;
- Conclusione con sentenza.

9.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione in atti giudiziari (articolo 319 ter, c.p.).

Il reato di **corruzione in atti giudiziari** si configura quando le condotte tipiche del reato di corruzione siano poste in essere per favorire o danneggiare una parte in un processo, con l'eventuale aggravante dell'ingiusta condanna di qualcuno.

Nel caso di specie, il reato si potrebbe verificare nel caso di promessa, offerta, concessione da parte dei soggetti e degli Uffici competenti della Società a magistrati, cancellieri, per se stessi o per un terzo, di danaro o di altro vantaggio, al fine di influenzare le loro decisioni, nell'ambito di un procedimento di cui la Società sia parte.

9.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l'Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti
- la Funzione Tecnologie, Servizi e Sviluppo
- il Responsabile del Procedimento

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori e procuratori esterni e partner operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

9.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli stessi elementi qualificanti previsti per i procedimenti giudiziali con la PA, ovvero la **tracciabilità** e la puntuale **registrazione della documentazione**.

In particolare dovrà prevedersi.

- la tracciabilità delle fasi operative, degli atti e delle fonti informative, con riguardo anche a tempi e risorse coinvolte;
- il protocollo dei documenti aziendali ufficiali diretti (tramite legali esterni e periti di parte) ai Giudici– compresi i Periti d'ufficio dagli stessi designati – competenti a giudicare sul contenzioso di interesse di Venis;
- la verifica delle attività svolte al fin di garantire che le stesse siano adeguatamente documentate e che la documentazione sia conservata in apposito archivio, con divieto di cancellare o distruggere arbitrariamente i documenti archiviati;

- la valutazione di congruità formale dei flussi documentali e di esperibilità delle azioni funzionali al procedimento.

9.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al Presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo ed in particolare nelle seguenti attività:

- in sede di incontri formali ed informali, anche a mezzo di legali esterni e periti di parte, per indurre Giudici (compresi gli ausiliari e i periti d'ufficio) a favorire gli interessi della Società;
- nel corso delle fasi del procedimento (ivi compreso il *tentativo facoltativo di conciliazione* nelle cause di lavoro) anche a mezzo di legali esterni e periti di parte, per ottenere il superamento di vincoli o criticità ai fini della tutela degli interessi della Società;
- in sede di ispezioni/controlli/verifiche da parte degli Organismi pubblici o periti d'ufficio, per influenzarne il giudizio/parere nell'interesse della Società, anche a mezzo di legali esterni e periti di parte;
- in sede di decisione del contenzioso, per influenzare le decisioni dell'Organo giudicante, anche a mezzo di legali esterni e di periti di parte.

9.F) FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Il Responsabile della Funzione interessata deve comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco contenziosi civili, penali, amministrativi in corso e conclusi.

9.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione.

* * *

Conformemente a quanto precedentemente illustrato, si procede di seguito alla trattazione separata delle ulteriori aree a rischio rappresentate dai processi strumentali che vengono direttamente in rilievo con riferimento ai reati previsti dal Decreto e che si riportano sotto per pronto riferimento:

10) Approvvigionamento di beni e servizi;

11) Conferimento di contratti di consulenza o prestazioni professionali;

12) Selezione e assunzione del personale e incentivazione delle politiche retributive

13) Finanza dispositiva - Gestione dei pagamenti e delle risorse finanziare

14) Accordi transattivi

15) Spese di rappresentanza e gestione omaggistica

16) Sponsorizzazioni

17) Liberalità

10) "APPROVVIGIONAMENTI DI BENI E SERVIZI"

10.A) DESCRIZIONE DEL PROCESSO

Il processo di acquisizione di beni e servizi si articola nelle seguenti fasi:

- Pianificazione fabbisogni;
- Individuazione dei criteri tecnico-economico-giuridici della fornitura o appalto (in funzione dei quali si opera mediante trattativa privata o procedura ad evidenza pubblica);
- Individuazione e scelta del fornitore;
- Predisposizione della richiesta d'acquisto;
- Redazione, verifica, autorizzazione ed emissione della richiesta d'acquisto;
- Gestione operativa del contratto/ordine (esecuzione prestazioni/consegna beni);
- Gestione delle fatture passive: ricevimento, rilascio benestare, contabilizzazione e pagamento.

10.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articoli 318, 319, 319 bis e 320, c.p.).

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o

abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

Nel caso in esame il processo di pianificazione degli approvvigionamenti, comprensivo delle fasi sopra individuate, nonché quello di gestione delle fatture passive, se condotti in modo anomalo da parte dei soggetti e degli Uffici competenti della Società, potrebbe costituire un potenziale supporto per la commissione del reato di corruzione, mediante la creazione di fondi “neri”, attraverso contratti stipulati a prezzi superiori rispetto a quelli di mercato ovvero mediante la scelta di fornitori particolarmente graditi alla Pubblica Amministrazione.

10.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell’Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l’Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti
- la Funzione Tecnologie, Servizi e Sviluppo
- il Responsabile della Trattativa/Procedimento

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

10.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave del processo, della **tracciabilità degli atti** e della **valutazione** complessiva delle forniture.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
  - Identificazione dei bisogni,
  - Richiesta della fornitura,
  - Definizione delle specifiche (Capitolato tecnico e d’oneri),
  - Effettuazione dell’acquisto,

- Certificazione dell’esecuzione dei servizi/consegna dei beni (rilascio benestare),
- Effettuazione del pagamento;

- Esistenza di criteri tecnico-economici per la qualificazione dei fornitori:
  - la selezione di potenziali fornitori (qualificazione o Albo Fornitori),
  - la validazione della fornitura e dei beni/servizi forniti,
  - la valutazione complessiva dei fornitori;
- Nel caso di affidamento diretto:
  - Espletamento di adeguata attività selettiva fra diversi offerenti e di obiettiva comparazione delle offerte (sulla base di criteri oggettivi e documentabili);
- Nel caso di gara d’appalto:
  - Esistenza di una commissione di almeno tre membri con responsabilità di valutazione e scelta del fornitore e di una griglia valutativa (con elementi tecnici ed economici) preventivamente definita;
  - Esistenza di livelli di approvazione per la formulazione delle richieste di acquisto e per la certificazione della fornitura/erogazione;
  - Esistenza di livelli autorizzativi (in coerenza con il sistema di procure aziendale) per la stipulazione dei contratti e l’approvazione delle relative varianti/integrazioni;
  - Trasparenza delle norme aziendali con riferimento alle singole fasi del processo acquisitivo:
    - precisa individuazione dei soggetti responsabili,
    - valutazione delle richieste di approvvigionamento,
    - verifica che le richieste arrivino da soggetti autorizzati,
    - determinazione dei criteri che saranno utilizzati nelle varie fasi del processo e per esprimere le valutazioni sulle offerte tecniche ed economiche.
- Tracciabilità delle singole fasi del processo con riguardo ad atti e documenti, tempi e risorse impiegate per consentire la ricostruzione delle fonti informative, delle responsabilità e le motivazioni delle scelte;
- Devono, inoltre, essere definite modalità di escalation autorizzativa per le attività d’acquisizione gestite in deroga ai requisiti sopra esposti (ad es. mancata comparazione fra offerte alternative, etc.).

10.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al Presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo. Inoltre:

- prevedere procedure organizzative aziendali specifiche per la regolamentazione dei processi di approvvigionamento;
- la scelta della modalità di approvvigionamento da adottare (es. pubblicazione del bando) deve essere formalizzata e autorizzata;
- le principali fasi della gara (apertura delle offerte tecniche, definizione del parere tecnico, apertura delle offerte economiche) devono essere verbalizzate e vi devono partecipare soggetti con interessi contrapposti (sia approvvigionamenti che unità richiedente);
- devono essere definiti criteri di rotazione delle persone coinvolte nel processo di approvvigionamento;
- devono esistere idonei sistemi di monitoraggio e formalizzazione di report da sottoporre ad un adeguato livello gerarchico per il monitoraggio (ad esempio numero di gare, fornitore vincitore, commissione aggiudicatrice, importo ed ente richiedente il fornitore unico, ecc.).

10.F) FLUSSI INFORMATIVI VERSO L’ORGANISMO DI VIGILANZA

Il Responsabile della Funzione Acquisti deve comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco degli acquisti effettuati richiesti dalle Funzioni Aziendali extra processi operativi.

10.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione
- Procedura organizzativa VAQ-CO-MP-02 “La procedura dei Contratti in Venis”
- Procedura organizzativa VAQ-AC-MP-01 “Albo dei fornitori in Venis”
- Procedura organizzativa VAQ-AC-MP-02 “Gli approvvigionamenti in Venis”
- Procedura organizzativa VAQ-AC-MP-04 “Gestione Gare”

11) "CONFERIMENTO DI CONTRATTI DI CONSULENZA O PRESTAZIONI PROFESSIONALI"

11.A) DESCRIZIONE DEL PROCESSO

Il processo riguarda l'assegnazione di incarichi per consulenze e prestazioni professionali[9] a soggetti terzi e pertanto si configura, pur nella specificità dell'oggetto contrattuale, come un processo d'acquisizione, articolato nelle seguenti fasi:

- Definizione del Piano di periodo;
- Elaborazione della richiesta di consulenza/prestazione professionale;
- Verifica, approvazione ed emissione della richiesta di consulenza/prestazione professionale;
- Scelta della fonte d'acquisto e contrattualizzazione;
- Gestione operativa del contratto;
- Rilascio benestare, contabilizzazione e pagamento dei corrispettivi.

11.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articolo 318, 319, 319 bis e 320, c.p.).

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

In questo quadro, una gestione non trasparente delle procedure volte all'assegnazione a terzi di incarichi di consulenza o di altre prestazioni professionali, da parte dei soggetti e degli Uffici competenti, potrebbe costituire una modalità strumentale per la commissione del reato di corruzione.

In particolare, si fa riferimento alla possibilità che la gestione dei predetti incarichi sia resa funzionale alla creazione di fondi occulti da utilizzare, indebitamente, a favore della Pubblica Amministrazione (si pensi al riconoscimento di compensi superiori a quelli di mercato o privi di causale) oppure alla possibilità che vengano favoriti professionisti o società "graditi" alla Pubblica Amministrazione, al fine di ottenere indebiti vantaggi.

[9] Per consulenze si intendono le prestazioni di contenuto specialistico rese da terzi per professionalità non presenti nell'Azienda ovvero ad integrazione delle professionalità esistenti.

11.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell’Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l’Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti
- la Funzione Tecnologie, Servizi e Sviluppo
- la Funzione Comunicazione

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

11.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sui due elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave del processo, della **tracciabilità degli atti**, a garanzia della trasparenza delle scelte effettuate e del servizio ricevuto.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
    - Elaborazione della richiesta di consulenza/prestazione professionale,
    - Verifica, approvazione ed emissione della richiesta di consulenza/prestazione professionale,
    - Definizione contrattuale,
    - Certificazione dello svolgimento dell’attività professionale richiesta (rilascio benestare),
    - Corresponsione del corrispettivo;
- Previsione ed utilizzo di idonei schemi contrattuali adeguatamente formalizzati;
- Previsione di meccanismi di verifica idonei a comprovare l’esistenza dei necessari requisiti professionali, economici ed organizzativi del consulente/professionista a garanzia degli standard qualitativi necessari o richiesti e per consentire una valutazione complessiva del servizio reso;
- Per consulenze/prestazioni professionali svolte da soggetti terzi incaricati di rappresentare la Società nei confronti della PA deve essere prevista una specifica clausola che li vincoli all’osservanza dei principi

etico-comportamentali adottati da Venis il cui testo è riportato nel Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione;

- Esistenza di livelli di approvazione per l’elaborazione delle richieste di consulenza/prestazione professionale e per la certificazione/validazione del servizio reso;

- Esistenza di livelli di approvazione per l’emissione delle richieste di consulenza/prestazione professionale;

- Tracciabilità delle singole fasi del processo (documentazione a supporto, livello di formalizzazione), per consentire, la ricostruzione delle responsabilità, delle motivazioni delle scelte e delle fonti informative.

Devono, inoltre, essere definite modalità operative e connessi meccanismi di escalation autorizzativa per eventuali deroghe ai principi sopra riportati, laddove ritenuto necessario, ad esempio per esigenze di riservatezza e tempestività.

11.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al Presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo. Inoltre:

- prevedere un’adeguata attività selettiva fra diversi offerenti e di obiettiva comparazione delle offerte (sulla base di criteri oggettivi e documentabili). Gli incarichi devono essere conferiti sulla base dell’Albo Consulenti gestita dalla Funzione Acquisti Gare e Contratti. L’inserimento/eliminazione dall’Albo deve essere motivato e documentato e basato su criteri oggettivi;

- ogni richiesta/stipulazione dei contratti per consulenza/prestazione professionale deve essere espressamente autorizzata in coerenza con il sistema di procure aziendale e prevedere precisi limiti di spesa coerenti con i preventivi richiesti, vincoli e responsabilità;

- devono esistere documenti giustificativi degli incarichi conferiti con motivazione, attestazione di inerenza e congruità, approvati dal superiore gerarchico e debitamente archiviati.

11.F) FLUSSI INFORMATIVI VERSO L’ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni interessate devono comunicare, con periodicità definita, quando indicato:

Con riferimento alle singole unità organizzative:

Flusso 1: piano annuale Consulenze/Prestazioni professionali e relativi aggiornamenti;

Flusso 2: elenco incarichi gestiti in deroga ai principi standard.

Flusso 3: consuntivo attività di consulenza/prestazioni professionali suddivise per fornitore.

11.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione
- Procedura organizzativa VAQ-AC-MP-01 "Albo dei fornitori in Venis"
- Procedura organizzativa VAQ-AC-MP-02 "Gli approvvigionamenti in Venis"
- Regolamento per il Conferimento incarichi professionali

12) "SELEZIONE E ASSUNZIONE DEL PERSONALE E GESTIONE DELLE RISORSE UMANE"

12.A) DESCRIZIONE DEL PROCESSO

Il processo di selezione e assunzione del personale è composto da tutte le attività necessarie alla costituzione del rapporto di lavoro. Il processo viene attivato per tutti i segmenti professionali di interesse, nel rispetto delle norme e del regolamento aziendale e si articola, sostanzialmente, nelle seguenti fasi:

- Attività di selezione del personale: acquisizione e gestione dei *curricula vitarum*; espletamento della selezione;
- formulazione dell'offerta ed assunzione;
- Amministrazione del personale e pagamento delle retribuzioni;
- Formazione del personale per quanto riguarda l'attuazione del Modello Organizzativo.

12.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articoli 318, 319, 319 bis e 320 c.p.).

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

Nel caso di specie, il reato potrebbe essere commesso nel caso di promessa, offerta, concessione da parte dei soggetti e degli Uffici competenti della Società ovvero da parte di altri soggetti per conto di questi ultimi, a pubblici ufficiali o ad incaricati di pubblico servizio, per se stessi o per un terzo, di un impiego lavorativo, al fine di indurre tali funzionari all'erogazione di favori ed alla indebita concessione di vantaggi relativamente dello

svolgimento delle attività aziendali.

Inoltre, irregolari procedure di erogazione delle retribuzioni e dei benefit connessi, che coinvolgono direttamente o indirettamente, funzionari della PA (ad es. assenza di accertamento dei presupposti formali e sostanziali per la liquidazione di somme relative a trasferte, rimborsi spese, premi, incentivi; assenza totale di controllo delle carte di credito aziendali utilizzate; attribuzione a terzi di benefit aziendali, buoni pasto, buoni benzina, etc.), possono costituire supporto per la commissione del reato di corruzione.

12.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell’Organigramma Venis allegato alla Parte Generale del presente Modello.

Potenzialmente, se si fa in particolare riferimento ad eventuali irregolari procedure di erogazione delle retribuzioni e dei benefit connessi, può trattarsi di tutte le funzioni previste nell’organigramma, ovvero:

- l’Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Tecnologie, Servizi e Sviluppo
- la Funzione Comunicazione, Sviluppo Personale e Qualità

Sono altresì interessati eventuali collaboratori esterni e partner operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

12.D) SISTEMA DI CONTROLLO

Essendo Venis una società *in house provider* del Comune di Venezia a partecipazione al pubblica, essa procede all’assunzione del proprio personale dipendente mediante procedura concorsuale. Ne consegue che il sistema di controllo non può basarsi che sugli elementi qualificanti del **puntuale rispetto della normativa vigente in materia** e sulla **tracciabilità della documentazione** comprovante i requisiti di concorso.

Stante quanto sopra esposto, gli elementi specifici di controllo possono essere così sintetizzati:

- Nella fase di “Selezione”:
    - Idonea pubblicazione e diffusione del bando di concorso secondo la normativa vigente,
    - Previsione, di norma, nel bando di concorso, di distinte modalità di valutazione, “‘attitudinale” e “tecnica”, del candidato,
    - Assegnazione della responsabilità di tali valutazioni a una commissione di soggetti distinti,
    - Prevedere la sottoscrizione formale delle suddette valutazioni da parte dei componenti la commissione, a garanzia della tracciabilità delle scelte effettuate;

- Nella fase ‘Formulazione dell’offerta e assunzione”:
    - procedere alla scelta in base alla graduatoria definita,
    - in sede di sottoscrizione della lettera di assunzione, verificare l’esistenza della documentazione accertante il corretto svolgimento delle fasi precedenti.

12.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al Presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo. Inoltre:

- nell’elaborazione del bando, con particolare riferimento all’indicazione dei requisiti attitudinali e tecnici dei candidati, attenersi scrupolosamente alla normativa vigente in materia;
- porre particolare attenzione alla raccolta e conservazione/archiviazione della documentazione comprovante i requisiti concorsuali;
- prevedere idonei sistemi di verifica del corretto svolgimento delle varie fasi concorsuali

12.F) FLUSSI INFORMATIVI VERSO L’ORGANISMO DI VIGILANZA

La Funzione Risorse Umane deve comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco dei concorsi indetti e delle assunzioni effettuate.

12.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione
- Regolamento in materia di Reclutamento e Selezione del Personale

13) "FINANZA DISPOSITIVA – GESTIONE DEI PAGAMENTI E DELLE RISORSE FINANZIARE"

13.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività riguardanti i flussi monetari e finanziari in uscita destinati all'assolvimento delle obbligazioni di varia natura delle unità operative.

I flussi suddetti si articolano sostanzialmente in due macro-gruppi:

- Flussi di natura **ordinaria**, connessi ad attività/operazioni correnti (ad es., acquisti di beni, servizi, oneri finanziari, fiscali e previdenziali, stipendi e salari);

- Flussi di natura **straordinaria**, connessi alle operazioni di tipo finanziario (ad es., sottoscrizioni e aumenti di capitale sociale, finanziamenti alla Società, cessioni di credito, operazioni in valuta estera e sui derivati-swap, futures, etc.).

Il processo si articola nelle seguenti fasi:

- Pianificazione del fabbisogno finanziario periodico e comunicazione – debitamente autorizzata – alla Funzione Finanza e Bilancio;

- Predisposizione (da parte della Funzione Finanza e Bilancio) delle disponibilità finanziarie, alle date e presso gli sportelli bancari;

- Richiesta dell'ordine di pagamento;

- Destinazione dell'importo, conformemente alle indicazioni delle Funzioni interessate.

- Autorizzazione al pagamento da parte della Funzione delegata.

13.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articoli 318, 319 e 320 c.p.).

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

Il processo di finanza dispositiva costituisce una delle modalità strumentali attraverso cui, in linea di principio, può essere commesso il reato di corruzione in quanto potrebbe agevolmente rappresentare il supporto per la costituzione di disponibilità finanziarie (c.d. "fondi neri") destinabili, da parte degli Uffici competenti della Società ovvero da altri soggetti per conto di questi ultimi, al pubblico ufficiale o all'incaricato di pubblico servizio al fine di indurli all'erogazione di favori ed alla indebita concessione di vantaggi relativamente dello svolgimento delle attività aziendali.

13.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell’Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l’Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

13.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave del processo, della **tracciabilità degli atti** e dei **livelli autorizzativi** da associarsi alle operazioni.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
    - Richiesta dell’ordine di pagamento,
    - Effettuazione del pagamento,
    - Controllo/riconciliazioni a consuntivo;
- Esistenza di livelli autorizzativi sia per la richiesta, che per l’ordine di pagamento, articolati in funzione della natura dell’operazione (ordinaria/straordinaria) e dell’importo;
- Devono esistere documenti giustificativi delle risorse finanziarie utilizzate con motivazione, attestazione di inerenza e congruità, validati dal superiore gerarchico e archiviati per garantire la tracciabilità degli atti e delle singole fasi del processo (con specifico riferimento all’annullamento dei documenti che hanno già originato un pagamento);
- Devono, inoltre, essere definite modalità operative e connessi meccanismi di escalation autorizzativa per eventuali deroghe ai principi sopra riportati, laddove ritenuto necessario, ad esempio per esigenze di tempestività.

13.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al Presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo. Inoltre:

- Prevedere un flusso informativo sistematico che garantisca il costante allineamento fra procure, deleghe operative e profili autorizzativi con particolare attenzione a limiti di spesa, vincoli e responsabilità;
- Prevedere e diffondere specimen di firma in relazione ai livelli autorizzativi definiti per la richiesta;
- Effettuare periodica attività di riconciliazione dei conti intrattenuti con banche;

Eventuali modalità non standard (relative sia a operazioni di natura ordinaria che straordinaria) devono essere considerate ‘in deroga” e soggette, pertanto, a criteri di autorizzazione e controllo specificamente definiti riconducibili a:

- Individuazione del soggetto che può richiedere l’operazione;
- Individuazione del soggetto che può autorizzare l’operazione;
- Indicazione, a cura del richiedente, della motivazione;
- Designazione (eventuale) della risorsa abilitata all’effettuazione dell’operazione attraverso procura *ad hoc*.

13.F) FLUSSI INFORMATIVI VERSO L’ORGANISMO DI VIGILANZA

Flusso 1: Elenco delle Funzioni Aziendali che possono richiedere flussi monetari e/o finanziari da effettuarsi con modalità non standard.

Flusso 2: Elenco dei flussi monetari e/o finanziari non standard realizzati nel periodo.

Flusso 3: Elenco dei flussi monetari e/o finanziari realizzati nel periodo.

13.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione.

14) "ACCORDI TRANSATTIVI"

14.A) DESCRIZIONE DEL PROCESSO

A norma del Codice Civile, la transazione è il contratto mediante il quale le parti, facendosi reciproche concessioni, prevengono una lite che può sorgere tra loro o pongono fine a una lite già cominciata.

Il processo in esame concerne pertanto tutte le attività necessarie a prevenire o dirimere una controversia con soggetti terzi.

Le controversie possono derivare sia da un rapporto contrattuale, sia da responsabilità extracontrattuali (ad es. insorgere della lite a seguito di danni provocati da terzi all'Azienda e viceversa).

Il processo si articola nelle seguenti fasi:

- Analisi dell'evento da cui deriva la controversia;
- Esame dell'esistenza dei presupposti per addivenire alla transazione;
- Svolgimento delle attività finalizzate alla definizione e formalizzazione della transazione (ad es. contatti e incontri con la controparte);
- Redazione, stipula ed esecuzione dell'accordo transattivo.

14.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articoli 318, 319 e 320 c.p.).

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

Il processo che porta alla definizione di un accordo transattivo costituisce una delle modalità strumentali attraverso cui può essere commesso il reato di corruzione. Invero esso potrebbe rappresentare una potenziale modalità di predisposizione di mezzi finanziari utili (cd "fondi neri") e destinabili, da parte delle Funzioni competenti della Società ovvero da altri soggetti per conto di questi ultimi, al pubblico ufficiale o all'incaricato di pubblico servizio al fine di indurli all'erogazione di favori ed alla indebita concessione di vantaggi relativamente dello svolgimento delle attività aziendali.

14.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l'Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti
- la Funzione Tecnologie, Servizi e Sviluppo
- la Funzione Sviluppo Personale (con riferimento alle cause di lavoro)

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori e procuratori legali esterni e partner operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

14.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **separazione di ruolo** fra le fasi chiave del processo e della **tracciabilità delle fasi** a garanzia delle scelte effettuate alla base dell'accordo transattivo.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di responsabilità differenziate fra:
    - Gestione operativa del processo aziendale legato all'accordo transattivo,
    - Gestione della trattativa e formalizzazione dell'accordo transattivo;
- Esistenza di livelli autorizzativi per la stipulazione ed esecuzione degli accordi transattivi;
- Tracciabilità del processo mediante la conservazione ed archiviazione della documentazione relativa alle singole fasi (richiesta, gestione, formalizzazione ed esecuzione dell'accordo), con attenzione particolare anche ai tempi ed alle risorse coinvolte;
- Devono essere, inoltre, previste modalità di *escalation* autorizzativa per la gestione delle eventuali deroghe (con particolare riferimento al superamento delle soglie di cui al paragrafo successivo).

14.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al Presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo. Inoltre:

- Definire specifici parametri da seguire nella decisione di privilegiare il ricorso ad accordi transattivi in alternativa alla gestione della controversia in sede giudiziale.
- Prevedere una divisione dei possibili accordi transattivi sulla base di soglie economiche e stabilire una precisa corrispondenza tra i livelli autorizzativi richiesti con riferimento ad ogni soglia economica.

Inoltre, in caso di ricorso a professionalità esterne prevedere:

- criteri specifici di selezione di procuratori o professionisti esterni (ad esempio, capacità tecnica, esperienza, requisiti soggettivi di professionalità e onorabilità, referenze qualificanti, politica di prezzo) e delle modalità di gestione e controllo dell’operato di tali professionisti;
- la verifica circa la mancanza di cause di incompatibilità del professionista esterno per la difesa della Società;
- strumenti di monitoraggio delle attività effettivamente svolte dal professionista esterno allo scopo di verificare la resa prestazione ai fini del controllo di congruità delle parcelle;
- la valutazione di congruità della parcella con riferimento alle prestazioni ricevute dalla società e la necessaria approvazione del pagamento anche da parte della funzione coinvolta.

14.F) FLUSSI INFORMATIVI VERSO L’ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni coinvolte nei processi transattivi devono comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco delle trattative/transazioni in corso, con specifica evidenza di quelle gestite in deroga;

Flusso 2: elenco delle trattative/transazioni concluse, con specifica evidenza di quelle gestite in deroga.

14.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione

15) "SPESE DI RAPPRESENTANZA E GESTIONE OMAGGISTICA"

15.A) DESCRIZIONE DEL PROCESSO

Il processo relativo alle spese di rappresentanza concerne il sostenimento di attività promozionali (ad es. cessione gratuita di beni e servizi a favore di terzi non dipendenti) con lo scopo di valorizzare all'esterno l'immagine della Società e della sua struttura.

Il processo si articola essenzialmente nelle fasi di:

- sostenimento della spesa;
- gestione dell'erogazione dei beni e servizi.

Il processo relativo alla gestione di omaggistica concerne, invece, tutte le attività necessarie alla distribuzione gratuita di beni e servizi, che rientrano o meno nell'attività propria dell'impresa, a favore, ad esempio, di committenti, clienti, fornitori, lavoratori dipendenti e soggetti estranei all'impresa, con l'obiettivo di sviluppare l'attività commerciale aziendale sia stimolando direttamente la domanda dei beni o servizi dell'impresa che promuovendola indirettamente.

La gestione di omaggistica è sostanzialmente configurabile come un processo di acquisto e si articola, pertanto, nelle fasi di:

- pianificazione e comunicazione del fabbisogno;
- individuazione del fornitore e conseguente acquisizione;
- gestione dell'erogazione dei beni/servizi.

15.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articoli 318, 319, 319 bis e 320 c.p.).

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

Nel caso di specie, il reato di corruzione si verificherebbe nell'ipotesi di promessa, offerta, concessione da parte dei soggetti e degli Uffici competenti a pubblici funzionari e dipendenti di beni di valore non modico e con modalità non conformi agli usi aziendali, al fine di ottenere indebiti favori nell'interesse o a vantaggio della Società.

In sostanza, le spese di rappresentanza o un'attività di omaggistica "fuori dalla norma" possono costituire, quantomeno, un potenziale supporto alla commissione del reato di corruzione ed, in quanto tali, devono essere effettuate secondo regole predeterminate.

15.c) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l'Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Comunicazione (per quanto attiene alle attività promozionale e alla gestione dei rapporti con enti e soggetti terzi)
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti
- la Funzione Tecnologie, Servizi e Sviluppo

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

15.d) SISTEMA DI CONTROLLO

Con particolare riferimento alle spese di rappresentanza, il sistema di controllo si basa sugli elementi qualificanti della **individuazione dei soggetti abilitati** a sostenere e ad autorizzare le spese e sulla **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Identificazione dei soggetti aziendali abilitati a sostenere spese di rappresentanza e previsione di appositi meccanismi autorizzativi;
- Esistenza di livelli di autorizzazione per l'eventuale rimborso delle spese effettuate;
- Esistenza di meccanismi di verifica della corrispondenza tra le spese di rappresentanza effettivamente sostenute e le tipologie di spesa effettuabili (secondo quanto previsto al successivo paragrafo 15.e. Protocollo Comportamentale) con attenzione in particolare all'importo economico delle stesse;
- Registrazione, presso il soggetto aziendale abilitato, delle spese sostenute a favore dei pubblici dipendenti e amministratori e conservazione dell'evidenza documentale relativa al fine di assicurare la tracciabilità degli atti.

Con particolare riferimento alla gestione omaggistica, il sistema di controllo si basa sugli elementi qualificanti **della separazione di ruolo fra richiedente e acquirente** dell'omaggio e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Identificazione dei soggetti aziendali titolati a:
    - rilasciare omaggi (richiedente),
    - provvedere alla fornitura (acquirente);
- Previsione di meccanismi autorizzativi per procedere all’elargizione di omaggi eccedenti soglie di rilievo per la norma in esame (ossia non di modico valore secondo l’uso comune);;
- Previsione di meccanismi di verifica della corrispondenza tra gli omaggi elargiti e le tipologie di beni/servizi che possono essere concessi in omaggio (secondo quanto previsto al successivo paragrafo 15.e. Protocollo Comportamentale) con attenzione in particolare al valore economico degli stessi;
- Registrazione degli omaggi consegnati a pubblici dipendenti e amministratori;
- Conservazione, presso i soggetti coinvolti, dell’evidenza documentale delle singole fasi del processo (richiesta, acquisto e consegna) al fine di assicurare la tracciabilità degli atti.

Sia nel caso delle **spese di rappresentanza** che nel caso **dell’elargizione di omaggi** devono essere previste, inoltre, modalità di escalation autorizzativa per la gestione delle deroghe (particolarmente per il supero del valore economico massimo).

15.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al Presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo. Inoltre:

- Prevedere espressamente le tipologie di spese di rappresentanza effettuabili e dei beni/servizi che possono essere concessi come omaggio (agende, calendari, oggetti sociali, *gadgets*, abbonamenti, etc.)[10]
- Prevedere, sia con riferimento alle spese di rappresentanza che ai beni/servizi oggetto di gestione omaggistica, specifici *range* economici con relativo importo massimo spendibile.

15.F) FLUSSI INFORMATIVI VERSO L’ORGANISMO DI VIGILANZA

I Responsabili di Funzione devono comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco delle spese di rappresentanza sostenute a favore di pubblici dipendenti e amministratori **(**con specifica evidenza dei casi oggetto di deroga).

[10] Sono esclusi dai requisiti di controllo del presente documento i *gadget* aziendali, purché sempre di valore economico esiguo.

Flusso 2: elenco degli omaggi elargiti a pubblici dipendenti e amministratori (con specifica evidenza dei casi oggetto di deroga).

15.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione.

16) "SPONSORIZZAZIONI"

16.A) DESCRIZIONE DEL PROCESSO

Il processo concerne il sostenimento di spese a favore di soggetti terzi per pubblicizzare il proprio marchio e l'immagine della Società.

Il processo si articola nelle seguenti fasi:

- Individuazione delle iniziative di sponsorizzazione e del partner potenziale;
- Negoziazione e contrattualizzazione dell'impegno;
- Gestione operativa del contratto;
- Rilascio benestare, contabilizzazione e pagamento fatture.

16.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articoli 318, 319 e 320 c.p.).

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

In questo quadro, una gestione anomala e non trasparente delle attività di sponsorizzazione potrebbe costituire una modalità strumentale per creare fondi finanziari occulti ed utilizzarli al fine di ottenere favori e vantaggi di ogni genere da parte di pubblici funzionari.

16.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell’Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l’Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Comunicazione (per quanto attiene alle attività promozionale e alla gestione dei rapporti con enti e soggetti terzi)
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

16.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **separazione di ruolo** nelle fasi chiave del processo e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
    - Approvazione di un piano annuale dei Progetti di Sponsorizzazione,
    - Stipula dei contratti,
    - Pagamento degli impegni assunti;
- Esistenza di livelli autorizzativi (in coerenza con il sistema di procure aziendale) per la stipulazione dei contratti e l’approvazione delle relative varianti/integrazioni;
- Formalizzazione degli eventuali rapporti con soggetti esterni (consulenti, terzi rappresentanti o altro) incaricati di svolgere attività a supporto dell’Azienda, prevedendo nei contratti una specifica clausola che li vincoli al rispetto dei principi etico-comportamentali adottati dalla Società[11];
- Tracciabilità delle singole fasi del processo per consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte;

[11] Il testo standard della clausola è riportato nel Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, nota 1.

- Devono essere, inoltre, previste modalità di *escalation* autorizzativa per la gestione delle deroghe ai principi sopra esposti.

16.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al Presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo. Inoltre prevedere:

- la definizione di una policy societaria per la realizzazione dei progetti di sponsorizzazione (criteri di individuazione degli ambiti sociale, culturale, sportivo, etc., delle caratteristiche dell'iniziativa e dei requisiti dei partner);
- la definizione del piano annuale dei Progetti di Sponsorizzazione e la relativa previsione di impegno economico stabilendo che l'approvazione del suddetto piano annuale e delle relative variazioni avvenga a cura del vertice aziendale;
- l'utilizzo di idonei schemi contrattuali, adeguatamente formalizzati.

16.F) FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni interessate devono comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: Piano Annuale dei Progetti di Sponsorizzazione e relativi aggiornamenti di periodo.

Flusso 2: Report periodico circa i progetti di sponsorizzazione realizzati (con specifica evidenza dei casi oggetto di deroga).

16.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione.

17) "LIBERALITÀ"

17.A) DESCRIZIONE DEL PROCESSO

Il processo riguarda l'effettuazione di donazioni e/o elargizioni a favore di soggetti terzi (organismi ed enti no profit), l'assunzione di iniziative di carattere umanitario e culturale, sociale e sportivo, quali interventi concreti

per creare un valore aggiunto agli azionisti e agli *stakeholder* anche in termini etici, civili e morali. Il processo si articola nelle seguenti fasi:

- Individuazione delle possibili iniziative per promozione interna o su richieste esterne;
- Selezione e scelta delle iniziative;
- Conferimento del contributo o gestione dell'iniziativa di carattere umanitario;
- Reportistica sull'attività svolta.

17.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Corruzione (articoli 318, 319 e 320 c.p.).

A seguito della riforma di cui alla L. 190/2012 **(vedi sub precedente punto 1.B)**, il reato di **corruzione** si configura sia laddove pubblici funzionari o incaricati di pubblico servizio percepiscano indebitamente, per l'esercizio delle proprie funzioni o dei propri poteri, qualsiasi forma di utilità, per se stessi o per un terzo, o accettino la promessa di riceverle (nuovo art. art. 318 c.p.), sia laddove un pubblico ufficiale ometta o ritardi, o abbia omesso o ritardato, ovvero compia, o abbia compiuto, un atto contrario ai doveri di ufficio, per sé o per un terzo (ovvero ne accetti la promessa), in cambio di denaro o altra utilità.

In questo quadro, una gestione anomala e non trasparente delle attività di sponsorizzazione potrebbe costituire una modalità strumentale per creare fondi finanziari occulti ed utilizzarli al fine di ottenere favori e vantaggi di ogni genere da parte di pubblici funzionari.

17.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- l'Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Comunicazione
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

17.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **separazione di ruolo** nelle fasi chiave del processo e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
    - Approvazione di un piano di iniziative di liberalità,
    - Conferimento delle donazioni/erogazioni e/o gestione delle iniziative,
    - Pagamento degli impegni assunti;
- Tracciabilità delle singole fasi del processo per consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte;
- Devono essere, inoltre, previste modalità di escalation autorizzativa per la gestione delle deroghe ai principi sopra esposti.

17.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al Presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo. Occorre inoltre prevedere:

- l'esistenza di criteri per l'individuazione degli ambiti di intervento e per la scelta delle organizzazioni beneficiarie;
- la definizione di un piano annuale dei progetti di liberalità e no profit e la relativa previsione di impegno economico stabilendo che l'approvazione del suddetto piano annuale e delle relative variazioni avvenga a cura del vertice aziendale.

17.F) FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni interessate devono comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: Report periodico circa le iniziative di liberalità realizzate (con specifica evidenza dei casi oggetto di deroga e/o di *escalation* autorizzativa).

17.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione.

PARTE SECONDA – DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

(art. 24 bis D. Lgs. 231/2001)

L'art. 7 della Legge 18 marzo 2008, n. 48 ha introdotto nell'ordinamento l'art. 24 *bis* nel Decreto con sanzioni per gli Enti, in conformità alla Convenzione di Budapest che, prevede anche la responsabilità (penale, civile o amministrativa) delle persone giuridiche, quando i reati informatici sono commessi da una persona fisica esercitante poteri direttivi nel loro ambito (artt. 11 e 12 della Convenzione). Nella Convenzione di Budapest è stabilito, infatti, che le sanzioni da scegliere, da parte degli Stati, devono essere effettive, proporzionate, dissuasive e comprendenti anche pene detentive (art. 13). L'introduzione dell'art. 24-*bis* nel Decreto risponde quindi all'esigenza di introdurre forme di responsabilità penale per le persone giuridiche anche con riferimento ai reati informatici più gravi, con l'intento di dare un effetto più esteso, tenuto conto che - ai sensi dell'art. 5 del Decreto- l'Ente è responsabile per i reati commessi nel suo interesse o vantaggio da persone che rivestono funzioni di rappresentanza, amministrazione, direzione dell'ente o di una sua unità organizzativa ma anche da persone sottoposte alla loro direzione o vigilanza. La responsabilità dell'Ente sussiste infatti anche quando l'autore del reato non è stato identificato o non è imputabile e da ciò discende che la necessità degli enti di dotarsi di particolari moduli di organizzazione e vigilanza per evitare la commissione dei reati informatici o commessi attraverso l'uso dell'informatica e a scegliere sistemi per l'individuazione dell'autore di un eventuale reato.

Con riferimento ai reati informatici e al trattamento illecito di dati, introdotti dall'art. 7 della Legge 18 marzo 2008, n. 48, mediante l'inserimento dell'art. 24 *bis* del Decreto, giova innanzitutto precisare che molte di tali ipotesi delittuose – le cui condotte tipiche sono dettagliatamente considerate nella Parte Generale del presente Modello – attengono, ad opera del richiamo contenuto nell'art. 491 *bis* c.p., alle stesse condotte criminose già disciplinate dal codice penale al Libro VII (Delitti contro la fede pubblica), Capo III (Falsità in atti, artt. 476 e ss. c.p.) del Codice Penale, con l'unica differenza che in tal caso l'attività illecita ha ad oggetto o mezzo del reato un sistema informatico o telematico.

Un'unica precisazione si rende necessaria con riferimento al reato di cui all'art. 640 quinquies c.p. (frode informatica del soggetto che presta servizi di certificazione di firma elettronica) che non risulta nel nostro caso applicabile, dal momento che Venis non è una società che presta servizi di certificazione di firma elettronica.

Aree a rischio

Passando alla specifica individuazione delle **aree a rischio,** con riferimento ai reati di cui all'art. 24 bis del Decreto, si segnalano i seguenti relativi **processi operativi**:

1) Gestione di accessi, account e profili. Si tratta di una serie articolata di attività poste in essere al fine di regolamentare la tipologia di accessi ai dati, sistemi ed applicazioni ritenute critiche o sensibili al fine di evitare accessi da parte di personale non autorizzato;

2) Gestione delle reti di telecomunicazione. Si tratta delle attività connesse alla gestione e manutenzione delle reti telematiche e all'implementazione di misure di sicurezza al fine di garantire la riservatezza delle informazioni, oltre che al monitoraggio degli eventi sulle reti atto ad individuare accessi e/o utilizzi anomali ed a definire in maniera tempestiva le azioni correttive;

3) Gestione dei sistemi hardware. Si tratta di una serie di attività finalizzate all’identificazione, all’implementazione, alla manutenzione ed al monitoraggio delle componenti hardware utilizzate dalla Società;

4) Gestione dei sistemi software. Si tratta delle attività connesse all’identificazione, allo sviluppo, alla manutenzione ed al monitoraggio dei sistemi software utilizzati dalla Società;

5) Gestione degli accessi fisici ai siti ove risiedono le infrastrutture IT. Si tratta di una serie articolata di attività finalizzate alla definizione delle misure di sicurezza fisica implementate al fine di evitare accessi non autorizzati ai sistemi ed ai siti fisici ove risiedono i sistemi e le infrastrutture IT;

6) Gestione e sicurezza della documentazione in formato digitale. Si tratta dell’attività di gestione delle tecniche di crittografia applicate alla documentazione informatica e di definizione delle metodologie, delle tempistiche di archiviazione e conservazione dei documenti in formato digitale;

7) Gestione e trattamento di dati personali, nella qualità di Responsabili del Trattamento, ai sensi dell’art. 29 del DIgs 196/2003, di dipendenti della Società, dei soggetti terzi, quali fornitori, consulenti e dei soggetti partecipanti alle gare di appalto, gestite dalla Società; degli utenti dei portali web, e dei cittadini di Venezia archiviati sui database del Comune di Venezia gestiti ed operati dal personale di Venis; nel rispetto del Codice per la protezione dei dati personali e delle disposizione del Garante per la Protezione dei Dati Personali;

8) Conservazione dei dati di traffico telefonici e telematici. Si tratta dell’attività di implementazione delle misure di sicurezza dei dati di traffico telefonici e telematici nel rispetto dei provvedimento del Garante per la protezione dei dati personali.

Fermi restando i principi di carattere generale individuati nel Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, validi con riferimento a tutte le aree a rischio di commissione dei reati di cui al Decreto, nonché delle regole contenute negli standard internazionali applicati da Venis – quali l’ISO/IEC 27002:2005 *Information technology – Security Techniques – Code of Practice for Information Security Management* e ISO 27001:2005, recante “*Information – Security Management System – (ISMS)*” – la rilevanza, per Venis, delle attività proprie delle aree a rischio sopra considerate, rende quanto mai opportuno procedere all’analisi separata di ogni singola area, al fine di individuare specificamente i caratteri propri di ogni processo considerato, considerare i reati ipotizzabili in ogni settore e le relative modalità attuative, le singole attività di controllo previste e gli specifici protocolli comportamentali diretti ad evitare il perfezionamento dei reati ipotizzabili, nonché i flussi informativi con l’O.d.V.

1) “GESTIONE DI ACCESSI, ACCOUNT E PROFILI”

1.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività svolte per la gestione di accessi, account e profili degli utenti da parte di Venis, allo scopo di controllare l’accesso alle informazioni; per impedire l’accesso non autorizzato ai sistemi d’informazione; per accertare la protezione dei servizi in Rete; per impedire l’accesso non autorizzato ai terminali *client*; per rilevare le attività non autorizzate; per accertarsi sulla sicurezza delle informazioni quando sono utilizzate le postazioni mobili di Rete.

Il processo si articola nelle seguenti fasi:

- definizione sistemi per l’accesso ai dati e per l’accesso alle applicazioni ed alla Rete;
- creazione delle password di accesso alla Rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili;
- l’assegnazione dell’accesso remoto ai sistemi da parte di dipendenti e soggetti terzi quali consulenti e fornitori;
- gestione e *logging* degli accessi effettuati sugli applicativi dagli utenti;
- gestione di account e di profili di accesso e verifiche periodiche dei profili utente.

1.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, possiamo considerare **l’accesso abusivo ad un sistema informatico o telematico** (art. 615 ter), il quale può essere commesso attraverso l’introduzione abusiva, eludendo una qualsiasi forma, anche minima, di barriera ostativa all’accesso, in un sistema informatico o telematico protetto da misure di sicurezza, ovvero il persistere abusivamente nel sistema informatico contro la volontà di chi ha diritto di escluderlo. In particolare, si chiarisce che per la giurisprudenza il reato è ipotizzabile nelle fattispecie che seguono:

- Commette il reato di accesso abusivo ad un sistema informatico o telematico di cui all’art. 615 ter c.p. il lavoratore dipendente che, pur avendo titolo per accedere al sistema informatico della propria azienda, vi si introduce con la password di servizio per raccogliere dati protetti per finalità estranee alle ragioni di impiego e agli scopi sottostanti alla protezione dell’archivio informatico; né, ai fini dell’integrazione del reato, si rende necessaria la distruzione dell’archivio informatico, risultando sufficiente la mera duplicazione, comportante una permanenza non autorizzata dell’utente (Cass. pen. Sez. V, 10 dicembre 2009, n. 2987);
- integra il reato di accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.) la condotta del soggetto che, avendo titolo per accedere al sistema, vi si introduca con la password di servizio per raccogliere dati protetti per finalità estranee alle ragioni di istituto ed agli scopi sottostanti alla protezione dell’archivio informatico (Cass. pen. Sez. V Sent., 13 febbraio 2009, n. 18006);
- La duplicazione dei dati contenuti in un sistema informatico o telematico costituisce condotta tipica del reato previsto dall’art. 615 ter c.p., restando in esso assorbito il reato di appropriazione indebita (App. Brescia, 27 Febbraio 2007);
- Commette il reato previsto dall’art. 615 ter c.p. (accesso abusivo ad un sistema informatico o telematico) il soggetto che, avendo titolo per accedere al sistema, lo utilizzi per finalità diverse da quelle consentite (Cass. pen. Sez. V Sent., 8 luglio 2008, n. 37322);
- Ai fini della configurabilità del reato previsto dall’art. 615 ter c.p. (accesso abusivo ad un sistema informatico o telematico), la protezione del sistema può essere adottata anche con misure di carattere organizzativo, che disciplinino le modalità di accesso ai locali in cui il sistema è ubicato e indichino le persone abilitate al suo utilizzo (Cass. pen. Sez. V Sent., 8 luglio 2008, n. 37322);

È possibile, anche, ipotizzare il reato di **detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici** (art. 615 quater c.p.)..

A tal riguardo, la Corte di Cassazione (Cass. pen. Sez. II, (ud. 21-02-2008) 25-09-2008, n. 36721) ha osservato che attraverso l’art. 615 *quater* c.p., il legislatore ha voluto rafforzare la tutela della riservatezza dei dati e dei programmi contenuti in un elaboratore, già assicurata dalla incriminazione dell’accesso e della permanenza abusivi in un sistema informatico o telematico *ex* art. 630 c.p..

- La norma, in altri termini, reprime una serie di condotte prodromiche alla (possibile) realizzazione del delitto di accesso abusivo in un sistema informatico o telematico, protetto da misure di sicurezza, e, quindi, pericolose per il bene giuridico tutelato attraverso l’art. 615 ter c.p.. In sostanza, la norma, pur collocandosi in un’ottica generale di tutela della riservatezza di domicilio informatico, ha come obiettivo, immediato e diretto, quello di tutelare la riservatela dei codici di accesso considerati dal legislatore come qualità personali riservate che identificano l’utente di un servizio informatico. Dal momento che il delitto di accesso abusivo è strutturato come reato di pericolo, la norma di cui all’art. 615 *quater* c.p. delinea una fattispecie di pericolo necessariamente indiretto: dalla condotta volta a procurare a sé o ad altri il codice di accesso al sistema informatico altrui deriva, infatti, il pericolo sia di una successiva, immediata introduzione abusiva nel sistema stesso (che è situazione di per sé pericolosa per la riservatezza dei dati e/o dei programmi che vi sono contenuti), sia di una ulteriore condotta di diffusione del codice che potranno, a loro volta, servirsene per realizzare un accesso abusivo oppure cederlo a terzi. Da quanto sopra esposto ne discende che i due reati ben possano concorrere.

- Quanto all’oggetto della condotta, la norma in questione vieta di procurare a sé o ad altri, abusivamente, codici, parole-chiave o altri mezzi idonei all’accesso ad un sistema informatico o telematico che sia protetto da misure di sicurezza. Oggetto della condotta può essere, innanzitutto, il codice di accesso (o parola-chiave) alfabetico, numerico o alfanumerico che, se digitato alla tastiera o altrimenti comunicato all’elaboratore, consente l’accesso ai dati e ai programmi contenuti nella memoria interna. Ne consegue, pertanto, che oggetto della condotta ben può essere il procurarsi una password e, cioè, uno degli strumenti logici che consentono direttamente l’accesso ad un sistema informatico protetto.

- Infine, per la configurazione del reato è richiesto, oltre al dolo generico - consistente nella volontà di procurarsi, riprodurre, diffondere, comunicare o consegnare codici, parole chiave o mezzi similari che si sa essere idonei a consentire l’accesso ad un sistema informatico protetto - anche il dolo specifico caratterizzato dal fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno; e deve ritenersi sicuramente quale profitto del reato la finalità di procurarsi informazioni o programmi altrui o di prendere conoscenza di dati contenuti nell’elaboratore; senza considerare che il danno ben può consistere nella finalità di immettere comunicazioni e messaggi - in modo da operarne una diffusione nei confronti di un numero indeterminato di persone - tali da ledere, per il loro contenuto, l’immagine del titolare del sistema informatico (nella specie un’azienda).

- Detto reato può essere commesso da chi abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all’accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni in questo senso, allo scopo di procurare a sé o ad altri un profitto, o di arrecare ad altri un danno. In particolare, la giurisprudenza ha chiarito che l’illecita acquisizione di codici di accesso a conti correnti bancari ed il loro successivo utilizzo per effettuare prelievi non autorizzati è inquadrabile come reato di cui all’articolo in esame (Trib. Milano Sent., 28-07-2006 Dir. Internet, 2007, 1, 62).

E' possibile altresì ipotizzare **il reato di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico** (art. 615 *quinquies* c.p.). Tale reato si realizza quando, 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 al fine di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, ci si procurino, si producano, si riproducano, si importino, si diffondano, si comunichino, si consegnino o, comunque, si mettano a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Sul punto, la giurisprudenza ha chiarito quanto segue:

- L'illecita acquisizione di codici di accesso a conti correnti bancari e postali ed il loro successivo utilizzo per effettuare prelievi e bonifici on line non autorizzati (c.d. *phishing*) è inquadrabile ai sensi degli artt. 640-ter, 615-quater e 615-quinquies c.p.(Trib. Milano Sent., 28-07-2006,Dir. Internet, 2007, 1, 62);

- Sono integrati i reati di cui all'art. 615-ter c.p. e all'art. 615-quinquies c.p. nel caso in cui l'imputato diffonda un programma informatico di sua creazione avente per effetto l'alterazione del funzionamento di sistemi informatici (c.d. virus), previa abusiva introduzione in un sistema informatico altrui (Trib. Bologna, 22-12-2005 X, Corriere del Merito, 2006, 4, 507);

- Ai fini della sussistenza dell'elemento soggettivo del reato ex art. 615-quinquies c.p., consistente nella diffusione di programmi (nella specie il programma "Vierika") atti ad alterare alcune delle funzionalità telematiche dei sistemi informatici, si ritiene sufficiente che vi sia l'accertata volontà dell'agente di diffondere il programma con la consapevolezza dei suoi effetti non esigendo la norma che il fine dell'azione sia la distruzione o il danneggiamento del sistema informatico (Trib. Bologna, 22-12-2005 C.S.; Riv. Pen., 2007, 4, 428).

È inoltre ipotizzabile **il reato di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche** (art. 617 *quater* c.p.). Il reato è perpetrato laddove si intercettino fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero, suddette comunicazioni vengano impedite o interrotte. Salvo che il fatto costituisca più grave reato, la stessa pena si applica laddove si riveli, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni sopra menzionate.

Sul punto, la giurisprudenza ha precisato che "*commette il reato di cui all'art. 617-quater c.p. il responsabile del centro elaborazione dati di una società che, pur investito della connessa posizione di amministratore di sistema, avvalendosi di mezzi atti a eludere i meccanismi di sicurezza volti a impedire l'accesso di estranei alle comunicazioni (password, firewall, criptazione od altri analoghi strumenti), intercetti le comunicazioni di posta elettronica indirizzate ai singoli amministratori e dipendenti*" (Cass. pen. Sez. V, 06-07-2007, n. 31135 P.C. in c. Casanova, Dir. e Pratica Lav., 2007, 41, 2508).

Si rileva che anche possibile considerare **il reato di installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche** (art. 617 *quinquies* c.p.). Il reato si configura laddove, fuori dai casi consentiti dalla legge, si installino apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi. A tal riguardo, la giurisprudenza ha chiarito che "*l'utilizzazione di apparecchiature capaci di copiare i codici di accesso degli utenti di un sistema informatico integra la condotta del delitto di cui all'art. 617 quinquies cod. pen., dal momento che la copiatura abusiva dei codici di accesso per la prima comunicazione con il sistema rientra nella nozione di "intercettare" di cui alla norma incriminatrice*" (Cass. pen. Sez. II Sent., 09-11-2007, n. 45207 (rv. 238512), CED Cassazione, 2007).

Si ipotizza ancora **il reato di danneggiamento di informazioni, dati e programmi informatici** (art. 635 *bis* c.p.). Tale reato si perfeziona laddove sia posta in essere una condotta idonea a determinare la distruzione, il deterioramento, la cancellazione, l'alterazione ovvero la soppressione di informazioni, dati o programmi informatici.

Sul punto, la giurisprudenza ha precisato che:

- Integra il delitto previsto dall'art. *635-bis c.p.* la cancellazione di dati informatici, ancorché questi possano essere recuperati attraverso una complessa procedura tecnica che richiede l'uso di particolari sistemi applicativi e presuppone specifiche conoscenze (Cass. pen. Sez. V, 18-11-2011, n. 8555);

- Commette il reato di danneggiamento di dati informatici previsto dall'art. 635-*bis* c.p. il dipendente che cancella un numero rilevante di dati dal computer affidatogli dal datore di lavoro per motivi lavorativi, anche se i files sono stati poi recuperati grazie all'intervento di un tecnico informatico specializzato (Cass. pen. Sez. V, 18-11-2011, n. 8555 S.R.Prat. Lavoro, 2012, 15, 640);

- il reato di danneggiamento di dati informatici previsto dall'art. 635 *bis* cod. pen. deve ritenersi integrato anche quando la manomissione ed alterazione dello stato di un computer sono rimediabili soltanto attraverso un intervento recuperatorio postumo comunque non reintegrativo dell'originaria configurazione dell'ambiente di lavoro (Cass. pen. Sez. V, 18-11-2011, n. 8555 (rv. 251731)CED Cassazione, 2012).

Infine, si considera **il reato di danneggiamento di sistemi informatici o telematici** (art. 635 *quater* c.p.). Tale reato si realizza laddove chiunque, attraverso una condotta finalizzata e diretta a determinare la distruzione, il deterioramento, la cancellazione, l'alterazione ovvero la soppressione di informazioni, dati o programmi informatici ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento. Il reato contempla due aggravanti, laddove il fatto sia compiuto con violenza o minaccia o sia commesso con abuso della qualità di operatore del sistema.

1.c) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- la Funzione Reti e Telecomunicazioni
- l'Amministratore di Sistema
- la Funzione Sistemi e Sicurezza Informatica

Sono, inoltre, interessati tutti gli incaricati del trattamento dei dati nonché di tutti gli addetti tecnici, come a titolo esplicativo e non esaustivo, sistemisti di rete e amministratori di database, addetti al protocollo informatico, ivi compreso il custode delle parole chiave, che siano essi dirigente, dipendenti e/o collaboratori, a qualsiasi titolo, della Società.

Possono essere interessate all'attività di cui sopra anche le Funzioni che seguono:

- la Funzione Tecnologie, Servizi e Sviluppo
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

1.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- sviluppo di sistemi di autenticazione informatica e di definizione di processi informatici per l’accesso ai PC ed ai Server, alla posta elettronica ed alla rete Internet, dalla sede aziendale e/o da remoto, affinché a ciascuna risorsa elettronica possa accedere solo chi è autorizzato, e nel rispetto della tipologia di autorizzazione conferitogli dall’Ente;
- classificazione della tipologia di dato trattato e definizione di procedure di accesso, conformemente al livello di autorizzazione dell’Incaricato al trattamento del dato;
- sviluppo di sistemi di autenticazione informatica e di definizione di processi informatici per l’accesso alle banche dati e per l’accesso alle applicazioni informatiche ed alla Rete, per accertare l’identità delle persone, affinché a ciascuna risorsa elettronica possa accedere solo chi è autorizzato;
- sviluppo di un sistema di autorizzazioni, al fine di individuare le tipologie di dati ai quali i singoli Incaricati possano accedere ed i tipi di trattamenti che su di essi sono autorizzati a svolgere;
- creazione delle password di accesso alla Rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili, che viene rilasciata al singolo utente dai Servizi ICT su segnalazione dell’ufficio risorse umane;
- gestione e *logging* degli accessi effettuati sugli applicativi dagli utenti;
- gestione di account e di profili di accesso;
- sviluppo di un sistema di protezione degli strumenti e dei dati da malfunzionamenti, da attacchi informatici, da programmi che contengono codici virus, da accessi remoti non autorizzati, da aggiornare periodicamente;
- implementazione di un sistema di verifica degli accessi non autorizzati sulle banche dati e sulle risorse informatiche e di registrazione e tracciamento di eventi anomali;
- sviluppo di procedure attinenti al corretto utilizzo della posta elettronica ed alla navigazione in internet.

- La segregazione delle responsabilità;

- Il conferimento di specifiche procure ai responsabili delle unità organizzative coinvolte al fine di dotarli del potere di rappresentanza della Società;

- Le mansioni svolte nell’ambito delle aree specificate devono essere assegnate a personale di chiara competenza informatica nel settore della gestione di rete, sistemisti certificati della Funzione Sistemi e Servizi Tecnologici Sicurezza Informatica che abbiano le competenze necessarie per assumere la qualifica di amministratore di sistema in relazione ai dati il cui accesso è controllato;

- La politica sulla sicurezza delle informazioni deve esser redatta, formalmente approvata, aggiornata periodicamente e comunicata a tutto il personale aziendale; le *policies* e le procedure relative alla gestione della sicurezza delle informazioni devono esser allineate all’orientamento indicato nella politica, devono esser aggiornate periodicamente e diffuse a tutti gli utenti;

- Effettuazione di verifica di congruenza delle disposizioni di sicurezza;

- Tracciabilità della documentazione eventualmente richiesta e consegnata all’ente di riferimento, degli atti e delle fonti informative nelle singole fasi del processo con specifico riferimento ad impiego di risorse e tempi;

- La dotazione di requisiti individuali ed univoci di autenticazione ai sistemi per l’accesso ai dati, alle applicazioni ed alla Rete;

- La procedura che definisce le regole per la creazione delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (ad esempio: lunghezza minima della password, regole di complessità, scadenza, etc.) deve esser formalizzata e comunicata a tutti gli utenti per la selezione e l’utilizzo della propria parola chiave individuale, con relativo obbligo di custodia e non disseminazione;

- L’assegnazione dell’accesso remoto ai sistemi da parte di soggetti terzi quali consulenti e fornitori deve essere regolato mediante l’esecuzione delle attività definite in una procedura formalizzata;

- Gli accessi effettuati sugli applicativi dagli utenti devono essere oggetto di verifiche e, per quanto concerne l’ambito dei dati sensibili, le applicazioni devono tener traccia delle modifiche ai dati compiute dagli utenti e devono essere attivati controlli che identificano variazioni di massa nei database aziendali, *ivi* compresi allarmi generati da sistemi di *Alerting* e di *Anomaly Detection*;

- La gestione di account e di profili di accesso deve prevedere l’utilizzo di un sistema formale di autorizzazione e registrazione dell’attribuzione, modifica e cancellazione dei profili di accesso ai sistemi; devono essere formalizzate procedure per l’assegnazione e l’utilizzo di privilegi speciali (amministratore di sistema, super user, root, etc.);

- Verifiche periodiche dei profili utente al fine di convalidare il livello di responsabilità dei singoli con i privilegi concessi; registrazione dei relativi risultati;

- Verifiche con cadenza annuale dell’attività di controllo interno per verificare la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico, anche per ciò che riguarda la verifica della particolare selettività degli Incaricati, assicurando che i controlli comprendano le

verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di *Alerting* e di *Anomaly Detection*, sulla legittimità e liceità degli accessi ai dati effettuati dagli Incaricati.

1.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- autenticazione dei sistemi per l’accesso ai dati, per l’accesso alle applicazioni ed alla rete;
- nomina di Amministratore di Sistema di specchiata competenza informatica, responsabile dei profili di sicurezza e dei sistemi di controllo con accesso *root* ai sistemi;
- comunicazione delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili;
- assegnazione dell’accesso remoto ai sistemi di rete;
- verifica degli accessi effettuati sugli applicativi dagli utenti;
- gestione di account e di profili di accesso.

1.F) INFORMATIVA VERSO L’ORGANISMO DI VIGILANZA

I Responsabili delle Unità Organizzative devono comunicare all’Organo di Vigilanza, per quanto di competenza quanto segue:

a. informativa circa la politica della sicurezza implementata per la gestione di accessi, account e profili;

b. informativa che permetta di verificare la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti di dati, anche per ciò che riguarda la verifica della particolare selettività degli Incaricati, assicurando che i controlli comprendano le verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di *Alerting* e di *Anomaly Detection*, sulla legittimità e liceità degli accessi ai dati effettuati dagli Incaricati.

1.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione
- Documento Programmatico per la Sicurezza

2) "GESTIONE DELLE RETI DI TELECOMUNICAZIONE"

2.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività svolte per la gestione delle reti di telecomunicazioni di Venis, allo scopo di effettuare lo sviluppo e il manutenzione di sistemi, per accertare che adeguati livelli di sicurezza sino stati implementati all'interno delle operazioni di sistema; per impedire la perdita, la modifica o il cattivo utilizzo dei dati dell'utente all'interno dei sistemi di applicazione; per proteggere riservatezza, autenticità e l'integrità delle informazioni; per accertarsi che le attività di progetto e supporto alle attività siano condotte in modo sicuro; per mantenere la sicurezza del software e dei dati di sistema; e per gestire la continuità operativa, per neutralizzare le interruzioni alle attività economiche ed ai processi critici degli affari, dagli effetti dei guasti.

Il processo si articola nelle seguenti fasi:

- Analisi dei rischi dei sistemi di rete di comunicazione elettronica;
- gestione delle reti di telecomunicazione;
- implementazione di meccanismi di segregazione logico/fisica delle rete;
- implementazione di strumenti di monitoraggio del traffico;
- implementazione di meccanismi di tracciatura degli eventi di sicurezza sulla Rete;
- implementazione e manutenzione di reti telematiche;
- esecuzione di attività di *vulnerability assessment* ed *ethical hacking*.

2.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, possiamo considerare il reato di cui all'art. 617 quater c.p. relative alle **intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematico**. Detto reato punisce la condotta di chi, in maniera fraudolenta, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, le impedisce o le interrompe oppure rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni. Per la giurisprudenza, commette il reato di cui all'art. 617 quater c.p. il responsabile del centro elaborazione dati di una società che, pur investito della connessa posizione di amministratore di sistema, avvalendosi di mezzi atti a eludere i meccanismi di sicurezza volti a impedire l'accesso di estranei alle comunicazioni (*password*, *firewall*, criptazione od altri analoghi strumenti), intercetti le comunicazioni di posta elettronica indirizzate ai singoli amministratori e dipendenti (Cass. pen. Sez. V, 6 luglio 2007, n. 31135).

Possiamo considerare, altresì, il reato di cui all'art. 617 quinques del c.p., relativo all'**installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche**. Detto reato sanziona la condotta di chi, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico,

ovvero intercorrenti fra più sistemi. Per la giurisprudenza, l'utilizzazione di apparecchiature capaci di copiare i codice di accesso degli utenti di un sistema informatico integra la condotta del delitto in esame dal momento che la copiatura abusiva dei codici di accesso per la prima comunicazione con il sistema rientra nella nozione di intercettare di cui alla norma incriminatrice (Cass. Pen. 45207/2007).

Si ipotizza, inoltre, il reato di **danneggiamento di informazioni, dati e programmi informatici** (art. 635 bis c.p.), posto in essere da chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, salvo che il fatto costituisca più grave reato.

Sul punto, la giurisprudenza ha precisato che:

- integra il delitto previsto dall'art. 635 *bis* c.p. la cancellazione di dati informatici, ancorché questi possano essere recuperati attraverso una complessa procedura tecnica che richiede l'uso di particolari sistemi applicativi e presuppone specifiche conoscenze (Cass. pen. Sez. V, 18-11-2011, n. 8555);

- commette il reato di danneggiamento di dati informatici previsto dall'art. 635 *bis* c.p. il dipendente che cancella un numero rilevante di dati dal computer affidatogli dal datore di lavoro per motivi lavorativi, anche se i files sono stati poi recuperati grazie all'intervento di un tecnico informatico specializzato (Cass. pen. Sez. V, 18-11-2011, n. 8555 S.R.Prat. Lavoro, 2012, 15, 640);

- il reato di danneggiamento di dati informatici previsto dall'art. 635 *bis* cod. pen. deve ritenersi integrato anche quando la manomissione ed alterazione dello stato di un computer sono rimediabili soltanto attraverso un intervento recuperatorio postumo comunque non reintegrativo dell'originaria configurazione dell'ambiente di lavoro (Cass. pen. Sez. V, 18-11-2011, n. 8555 (rv. 251731)CED Cassazione, 2012).

Si può ipotizzare, inoltre, anche il reato di **danneggiamento di sistemi informatici o telematici** (art. 635 quater c.p.), che punisce la condotta di chi, mediante le condotte di cui all'articolo 635 bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento, salvo che il fatto costituisca più grave reato.

Si può considerare il reato di **danneggiamento di sistemi informatici o telematici di pubblica utilità di cui all'art. 635 quinquies c.p.**, che punisce la condotta diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. Si rileva, in particolare, che possono considerarsi di pubblica utilità le informazioni, i dati, e i programmi informatici del Comune di Venezia, gestiti ed archiviati dalla Società. In tal senso, quindi, commette il suddetto reato altresì il lavoratore, collaboratore e il dirigente della Venis che danneggia le suddette informazioni e i dati del Comune di Venezia, con qualsiasi mezzo, *ivi* compreso, l'accesso remoto ai server del Comune stesso.

Può essere altresì posto in essere il reato di **diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico** (art. 615 quinquies c.p.), che sanziona la condotta di chi, per danneggiare illecitamente un sistema informatico o telematico, ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero per favorire l'interruzione o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna, o comunque mette a disposizione di altri apparecchiature, dispositivi o programmi informatici. Sul punto, la giurisprudenza ha chiarito che il reato in esame è integrato nel caso di diffusione di un virus in un sistema informatico altrui (Tribunale di Bologna del 22 dicembre 2005).

2.c) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- la Funzione Tecnologie, Servizi e Sviluppo
- la Funzione Reti e Telecomunicazioni
- l'Amministratore di Sistema
- la Funzione Sistemi e Sicurezza Informatica.

Sono, inoltre, interessati tutti gli incaricati del trattamento dei dati nonché di tutti gli addetti tecnici, come a titolo esplicativo e non esaustivo, sistemisti di rete e amministratori di database, addetti al protocollo informatico, che siano essi dirigente, dipendenti e/o collaboratori, a qualsiasi titolo, della Società.

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

2.d) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- la segregazione delle responsabilità;
- conferimento di specifiche procure ai responsabili delle unità organizzative coinvolte al fine di dotarli del potere di rappresentanza della Società;
- le mansioni svolte nell'ambito delle aree specificate devono essere assegnate a personale di chiara competenza informatica nel settore della gestione di rete, sistemisti certificati della Funzione Sistemi e Servizi Tecnologici Sicurezza Informatica che abbiano le competenze necessarie per assumere la qualifica di amministratore di sistema in relazione ai dati ed ai sistemi il cui accesso è controllato;
- effettuazione di verifica di congruenza delle disposizioni di sicurezza;
- tracciabilità della documentazione eventualmente richiesta e consegnata all'ente di riferimento, degli atti e delle fonti informative nelle singole fasi del processo con specifico riferimento ad impiego di risorse e tempi;
- definizione ed implementazione di controlli di sicurezza al fine di garantire la riservatezza dei dati

all’interno della rete e dei dati in transito su reti pubbliche;

- adozione di meccanismi di segregazione logico/fisica delle reti e di strumenti di monitoraggio del traffico di rete;
- implementazione di meccanismi di tracciatura degli eventi di sicurezza sulle reti;
- implementazione e la manutenzione di reti telematiche;
- definizione di verifiche periodiche sul funzionamento delle reti e sulle anomalie riscontrate, l’esecuzione di attività periodiche di *vulnerability assessment* ed *ethical hacking*.

2.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- gestione delle reti di telecomunicazione;
- implementazione di meccanismi di segregazione delle rete;
- implementazione di strumenti di monitoraggio del traffico;
- implementazione di meccanismi di tracciatura degli eventi di sicurezza sulla rete;
- implementazione e manutenzione di reti telematiche;
- istallazione di apparecchiature e misure di controllo sulla rete rivolte alla protezione da intrusioni nei data base e negli archivi dell’Ente. Implementazione e sviluppo di sistemi di sicurezza e tutela delle reti da tentativi di accesso remoto non autorizzato e accessi non autorizzati attraverso Internet;
- esecuzione di attività di *vulnerability assessment* ed *ethical hacking*
- Sviluppo di un piano di Disaster Recovery.

2.F) INFORMATIVA VERSO L’ORGANISMO DI VIGILANZA

I Responsabili delle Unità Organizzative devono comunicare, per quanto di competenza quanto segue:

a. informativa circa la politica di gestione e mantenimento delle reti di comunicazione elettronica;

b. informativa sugli eventi che hanno inficiato il funzionamento delle reti di telecomunicazioni, e sulla risoluzione delle problematiche riscontrate;

c. informativa sull’efficacia del piano di *Disaster Recovery* e sulle eventuali contromisure adottate;

2.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione
- Documento Programmatico per la Sicurezza

3) “GESTIONE DEI SISTEMI HARDWARE”

3.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività svolte per la gestione dei sistemi hardware di Venis, allo scopo di accertarsi del corretto funzionamento e facilità di elaborazione dell’informazione; per minimizzare il rischio di guasti dei sistemi; proteggere l’integrità dei sistemi hardware e software e delle informazioni; mantenere l’integrità e la validità dei processi di elaborazione dell’informazione e della comunicazione; garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture a supporto; prevenire danni ai beni e le interruzioni alle attività economiche; impedire perdita, modifica o abuso delle informazioni scambiate fra le organizzazioni.

Si rileva che nella struttura informatica di Venis sono presenti, complessivamente nelle due sedi di Palazzo Ziani e di Pleiadi, un centinaio di client; i server sono ospitati nel data center presso l’edificio Pleiadi. La rete dati è compartimentata e protetta tramite firewall e sistema IPS (Intrusion Prevention System). La sicurezza delle reti, in particolare di quella del Comune di Venezia, è attualmente garantita da tre distinti sistemi di firewalling:

- Coppia di dispositivi Cisco ASA-5550;
- Coppia di dispositivi Cisco PIX-535;
- Singolo dispositivo Cisco PIX-525.

In tal senso, quindi, il processo si articola nelle seguenti fasi:

- analisi dei rischi dei sistemi hardware;
- gestione dei sistemi hardware;
- manutenzione dei sistemi hardware;
- compilazione di un inventario dei sistemi hardware in uso presso la Società:
- definizione di opportune cautele per la custodia e l’utilizzo di supporti hardware rimovibili, nei quali possano essere contenuti dati personali;
- verifiche e controlli di supporti consegnati in manutenzione ad esecuzione delle operazioni di cancellazione sicura;

- adozione di procedure per la rottamazione e lo smaltimento di strumenti di elaborazione e di supporti di memorizzazione

3.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

E' possibile considerare il reato di cui all'art. 617 quinques c.p., relativo all' **installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche**. Detto reato sanziona la condotta di chi, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico, ovvero intercorrenti fra più sistemi.

Si ipotizza, altresì, il reato di **danneggiamento di informazioni, dati e programmi informatici** (art. 635 *bis* c.p.), posto in essere da chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, salvo che il fatto costituisca più grave reato.

Si può ipotizzare, inoltre, anche il reato di **danneggiamento di sistemi informatici o telematici** (art. 635 quater c.p.), che punisce la condotta di chi, 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, salvo che il fatto costituisca più grave reato.

Si può considerare il reato di **danneggiamento di sistemi informatici o telematici di pubblica utilità di cui all'art. 635 quinquies c.p.**, che punisce la condotta diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. Si rileva, in particolare, che possono considerarsi di pubblica utilità i sistemi del Comune di Venezia, gestiti dalla Società. In tal senso, quindi, commette il suddetto reato altresì il lavoratore, collaboratore e il dirigente della Venis che danneggia i sistemi informatici del Comune di Venezia o ne ostacola il funzionamento, con qualsiasi mezzo, *ivi* compreso, l'accesso remoto ai server del Comune stesso.

Può essere altresì posto in essere il reato di **diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico** (art. 615 quinquies c.p.), che sanziona la condotta di chi, per danneggiare illecitamente un sistema informatico o telematico, ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero per favorire l'interruzione o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna, o comunque mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Si ipotizza, inoltre, il reato di **danneggiamento di informazioni, dati e programmi informatici** (art. 635 bis c.p.), posto in essere da chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, salvo che il fatto costituisca più grave reato.

3.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- la Funzione Tecnologie, Servizi e Sviluppo
- la Funzione Reti e Telecomunicazioni
- la Funzione Sistemi e Sicurezza Informatica.

Sono, inoltre, interessati tutti gli incaricati del trattamento dei dati, nonché di tutti gli addetti tecnici, come a titolo esplicativo e non esaustivo, Amministratori di Sistema della Società, sistemisti di rete e amministratori di database, addetti al protocollo informatico, che siano essi dirigente, dipendenti e/o collaboratori, a qualsiasi titolo, della Società.

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

3.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- segregazione delle responsabilità;
- conferimento di specifiche procure ai responsabili delle unità organizzative coinvolte al fine di dotarli del potere di rappresentanza della Società;
- effettuazione di verifica di congruenza delle disposizioni di sicurezza;
- tracciabilità della documentazione eventualmente richiesta e consegnata all’ente di riferimento, degli atti e delle fonti informative nelle singole fasi del processo con specifico riferimento ad impiego di risorse e tempi;
- definizione ed implementazione di controlli di sicurezza sui sistemi hardware;
- compilazione di un inventario sui sistemi hardware presenti nella Società;
- gestione dei sistemi hardware;
- controllo dei sistemi di messa in sicurezza dei Server;
- controllo dei sistemi di protezione dell’alimentazione dei Server (UPS on line con by-pass automatico);
- verifica attività di manutenzione dei sistemi hardware;
- vetrifica di attività di custodia e di utilizzo di supporti hardware rimovibili, nei quali possano essere contenuti dati personali;

- verifiche e controlli di supporti consegnati in manutenzione ad esecuzione delle operazioni di cancellazione sicura;

- verifica delle misure di attuazione della rottamazione e dello smaltimento di strumenti di elaborazione e di supporti di memorizzazione.

3.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- gestione dei sistemi hardware;
- implementazione di meccanismi di tracciatura degli eventi di sicurezza sui sistemi hardware;
- implementazione e manutenzione dei sistemi hardware;
- esecuzione di attività di *vulnerability assessment*.

3.F) INFORMATIVA VERSO L’ORGANISMO DI VIGILANZA

I Responsabili delle Unità Organizzative devono comunicare, per quanto di competenza quanto segue:

a. informativa circa la politica di gestione e mantenimento dei sistemi hardware;

b. informativa sulla attività di gestione e manutenzione sei sistemi hardware implementata;

c. informativa sugli eventi che hanno inficiato la sicurezza dei sistemi hardware, e contromisure adottate.

3.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione.
- Documento Programmatico per la Sicurezza

4) "GESTIONE DEI SISTEMI SOFTWARE"

4.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività svolte per la gestione dei sistemi software licenziati o di Venis, allo scopo di accertarsi del corretto funzionamento e facilità di elaborazione dell'informazione; per minimizzare il rischio di guasti dei sistemi; proteggere l'integrità delle informazioni; mantenere l'integrità e la validità dei processi di elaborazione dell'informazione e della comunicazione; garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture a supporto; prevenire danni ai beni e le interruzioni alle attività economiche; impedire perdita, modifica o abuso delle informazioni scambiate fra le organizzazioni.

A tal riguardo, si precisa che le risorse software utilizzate per il protezione dei dati sono:

- Antivirus;
- Firewall;
- Antispam;
- Content Filtering.

Il processo si articola nelle seguenti fasi:

- Analisi dei rischi dei sistemi software;
- gestione dei sistemi software;
- manutenzione dei sistemi software;
- compilazione di un inventario dei sistemi software in uso presso la Società;
- verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso;
- implementazione di procedure di sicurezza in caso di *virus, spyware e malaware* ecc;
- attività di back up dei dati e delle informazioni;
- sviluppo ed implementazione di misure di *Disaster Recovery e Data Loss Protection;*
- sviluppo ed implementazione di misure di *Business Continuity* che assicurino in caso di eventi di eccezionale gravità che possano inficiare i software utilizzati.

4.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, si considerino i seguenti:

- **falsità in documenti informatici** (art. 491 bis c.p.)

Questo delitto estende la penale perseguibilità dei reati inerenti alle ipotesi di falsità, materiale o ideologica, commesse su atti pubblici, certificati, autorizzazioni, scritture private o atti privati, da parte di un rappresentante della pubblica amministrazione ovvero da un privato, qualora le stesse abbiano ad oggetto un "*documento informatico avente efficacia probatoria*", ossia un documento informatico munito quanto meno di firma elettronica semplice. Per "documento informatico" si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, c. 1, lett. p, Decreto Legislativo 7 marzo 2005, n. 82).

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

Tale fattispecie punisce la condotta di chi si introduce abusivamente, ossia eludendo una qualsiasi forma, anche minima, di barriera ostativa all'accesso, in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo. Detto reato si configura nel caso in cui il lavoratore dipendente, collaboratore, amministratore di sistema ecc., pur avendo titolo per accedere al sistema informatico dell'azienda, vi si introduce con la password di servizio per raccogliere dati protetti per finalità estranee alle ragioni di impiego e agli scopi sottostanti alla protezione dell'archivio informatico. Anche la duplicazione dei dati contenuti in un sistema informatico o telematico costituisce una condotta tipica del reato in esame.

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

La norma sanziona la condotta di chi, per danneggiare illecitamente un sistema informatico o telematico, ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero per favorire l'interruzione o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna, o comunque mette a disposizione di altri apparecchiature, dispositivi o programmi informatici. La diffusione ad esempio di virus nel sistema informatico o telematico integra la fattispecie del reato in esame. Per la giurisprudenza, sono integrati i reati di cui all'art. 615-*ter* c.p. e all'art. 615-*quinquies* c.p. nel caso in cui l'imputato diffonda un programma informatico di sua creazione avente per effetto l'alterazione del funzionamento di sistemi informatici (c.d. virus), previa abusiva introduzione in un sistema informatico altrui (Trib. Bologna, 22-12-2005 X,Corriere del Merito, 2006, 4, 507)

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

Tale reato si perfeziona laddove sia posta in essere una condotta idonea a determinare la distruzione, il deterioramento, la cancellazione, l'alterazione ovvero la soppressione di informazioni, dati o programmi informatici. Sul punto, la giurisprudenza ha precisato che:

- integra il delitto previsto dall'art. 635 *bis* c.p. la cancellazione di dati informatici, ancorché questi possano essere recuperati attraverso una complessa procedura tecnica che richiede l'uso di particolari sistemi applicativi e presuppone specifiche conoscenze (Cass. pen. Sez. V, 18-11-2011, n. 8555);

- commette il reato di danneggiamento di dati informatici previsto dall'art. 635 *bis* c.p. il dipendente che cancella un numero rilevante di dati dal computer affidatogli dal datore di lavoro per motivi lavorativi, anche se i files sono stati poi recuperati grazie all'intervento di un tecnico informatico specializzato (Cass. pen. Sez. V, 18-11-2011, n. 8555 S.R.Prat. Lavoro, 2012, 15, 640);

- il reato di danneggiamento di dati informatici previsto dall'art. 635 *bis* cod. pen. deve ritenersi integrato anche quando la manomissione ed alterazione dello stato di un computer sono rimediabili soltanto attraverso un intervento recuperatorio postumo comunque non reintegrativo dell'originaria

configurazione dell'ambiente di lavoro (Cass. pen. Sez. V, 18-11-2011, n. 8555 (rv. 251731)CED Cassazione, 2012).

- **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.)

La norma sanziona la condotta di chi commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, salvo che il fatto costituisca più grave reato. Il reato potrebbe essere commesso dal lavoratore, collaboratore o dirigente della Venis che danneggi informazioni e dati del Comune di Venezia, con qualsiasi mezzo, ivi compreso, l'accesso remoto ai server del Comune stesso.

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

La fattispecie in esame punisce la condotta di chi, mediante le condotte di cui all'articolo 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, salvo che il fatto costituisca più grave reato.

- **danneggiamento di sistemi informatici o telematici di pubblica utilità** (art. 635 quinquies)

La norma in oggetto incrimina la condotta descritta al precedente art. 635 quater c.p., qualora essa sia diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. Si rileva, in particolare, che possono considerarsi di pubblica utilità le informazioni, i dati, e i programmi informatici del Comune di Venezia, gestiti ed archiviati dalla Società. In tal senso, quindi, commette il suddetto reato altresì il lavoratore, collaboratore e il dirigente della Venis che danneggia le suddette informazioni e i dati del Comune di Venezia, con qualsiasi mezzo, ivi compreso, l'accesso remoto ai server del Comune stesso.

4.c) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- la Funzione Tecnologie, Servizi e Sviluppo;
- la Funzione Reti e Telecomunicazioni;
- l'Amministratore di Sistema;
- la Funzione Sistemi e Sicurezza Informatica.

Sono, inoltre, interessati tutti gli incaricati del trattamento dei dati nonché di tutti gli addetti tecnici, come a titolo esplicativo e non esaustivo, sistemisti di rete e amministratori di database, addetti al protocollo informatico, che siano essi dirigente, dipendenti e/o collaboratori, a qualsiasi titolo, della Società.

Si ritiene, comunque, che possono essere interessate all’attività di cui sopra anche le Funzioni che seguono;

- la Funzione Tecnologie, Servizi e Sviluppo

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

4.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- segregazione delle responsabilità;
- conferimento di specifiche procure ai responsabili delle unità organizzative coinvolte al fine di dotarli del potere di rappresentanza della Società;
- effettuazione di verifica di congruenza delle disposizioni di sicurezza;
- tracciabilità della documentazione eventualmente richiesta e consegnata all’ente di riferimento, degli atti e delle fonti informative nelle singole fasi del processo con specifico riferimento ad impiego di risorse e tempi;
- definizione ed implementazione di controlli di sicurezza sui sistemi software;
- compilazione di un inventario sui sistemi software in uso nella Società:

4.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- gestione dei sistemi software;
- implementazione di meccanismi di tracciatura degli eventi di sicurezza sui sistemi software;
- implementazione e manutenzione dei sistemi software;

- esecuzione di attività di verifica sulla vulnerabilità del sistema;
- sviluppo ed implementazione di piani di *Disaster Recovery* e *Data Loss Protection.*

4.F) INFORMATIVA VERSO L'ORGANISMO DI VIGILANZA

I Responsabili delle Unità Organizzative devono comunicare, per quanto di competenza quanto segue:

a. informativa circa la politica di gestione e mantenimento dei sistemi software;

b. informativa sull'attività di gestione e manutenzione dei sistemi software;

c. informativa sugli eventi che hanno inficiato la sicurezza sui sistemi software e contromisure adottate.

4.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione.
- Documento Programmatico per la Sicurezza

5) "GESTIONE DEI DEGLI ACCESSI FISICI AI SITI OVE RISIEDONO LE INFRASTRUTTURE IT"

5.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività svolte per la gestione degli accessi fisici ai siti ove risiedono le infrastrutture, allo scopo di controllare l'accesso alle infrastrutture o apparati di telecomunicazioni; per impedire l'accesso non autorizzato; per accertare la protezione dei servizi in Rete e/o per rilevare le attività non autorizzate.

Il processo si articola nelle seguenti fasi:

- gestione della sicurezza fisica dei siti ove risiedono le infrastrutture di rete;
- attività di vigilanza;
- attività di *reporting* delle violazioni dei locali o delle misure di sicurezza;
- definizione di codici di accesso ai locali in cui risiedono le infrastrutture di rete;
- definizione di attività di controllo sulle abilitazioni concesse per l'accesso alle infrastrutture di rete.

5.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, si considerano i seguenti:

- **accesso abusivo ad un sistema informatico o telematico** (art. 615 ter)

Tale fattispecie punisce la condotta di chi si introduce abusivamente, ossia eludendo una qualsiasi forma, anche minima, di barriera ostativa all'accesso, in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo. Detto reato si configura nel caso in cui il lavoratore dipendente, collaboratore, amministratore di sistema ecc., pur avendo titolo per accedere al sistema informatico dell'azienda, vi si introduce con la password di servizio per raccogliere dati protetti per finalità estranee alle ragioni di impiego e agli scopi sottostanti alla protezione dell'archivio informatico. Anche la duplicazione dei dati contenuti in un sistema informatico o telematico costituisce una condotta tipica del reato in esame.

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

Il delitto in esame sanziona la condotta di chi abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni in questo senso, allo scopo di procurare a sé o ad altri un profitto, o di arrecare ad altri un danno.

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

La norma sanziona la condotta di chi, per danneggiare illecitamente un sistema informatico o telematico, ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero per favorire l'interruzione o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna, o comunque mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

- **intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematico** (art. 617 quater)

La norma punisce la condotta di chi, in maniera fraudolenta, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, le impedisce o le interrompe oppure rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni.

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

La fattispecie in esame sanziona la condotta di chi, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico, ovvero intercorrenti fra più sistemi.

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

La fattispecie punisce la condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o

programmi informatici altrui, salvo che il fatto costituisca più grave reato.

- **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.)

La norma sanziona la condotta di chi commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, salvo che il fatto costituisca più grave reato. Si rileva, in particolare, che possono considerarsi di pubblica utilità le informazioni, i dati e i programmi informatici del Comune di Venezia, gestiti ed archiviati dalla Società. In tal senso, quindi, commette il suddetto reato altresì il lavoratore, collaboratore e il dirigente della Venis che danneggia le suddette informazioni e i dati del Comune di Venezia, con qualsiasi mezzo, *ivi* compreso, l'accesso remoto ai server del Comune stesso.

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

La fattispecie in esame punisce la condotta di chi, mediante le condotte di cui all'articolo 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, salvo che il fatto costituisca più grave reato.

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

La norma in oggetto incrimina la condotta descritta al precedente articolo 635 quater c.p., qualora essa sia diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. Si rileva, in particolare, che possono considerarsi di pubblica utilità i sistemi del Comune di Venezia, gestiti dalla Società, ovvero quelli sviluppati da Venis nell'interesse della cittadinanza. In tal senso, quindi, commette il suddetto reato altresì il lavoratore, collaboratore e il dirigente della Venis che danneggia i sistemi informatici del Comune di Venezia o ne ostacola il funzionamento, con qualsiasi mezzo, ivi compreso, l'accesso remoto ai server del Comune stesso.

5.c) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- la Funzione Tecnologie, Servizi e Sviluppo
- la Funzione Reti e Telecomunicazioni
- la Funzione Sistemi e Sicurezza Informatica

Sono, inoltre, interessati tutti gli incaricati del trattamento dei dati, nonché di tutti gli addetti tecnici, come a titolo esplicativo e non esaustivo, amministratori di sistema interni e/o esterni della Società, sistemisti di rete e amministratori di database, addetti al protocollo informatico, che siano essi dirigente, dipendenti e/o collaboratori, a qualsiasi titolo, della Società.

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

5.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- segregazione delle responsabilità;
- conferimento di specifiche procure ai responsabili delle unità organizzative coinvolte al fine di dotarli del potere di rappresentanza della Società;
- effettuazione di verifica di congruenza delle disposizioni di sicurezza;
- tracciabilità della documentazione eventualmente richiesta e consegnata all’ente di riferimento, degli atti e delle fonti informative nelle singole fasi del processo con specifico riferimento ad impiego di risorse e tempi;
- definizione ed implementazione di controlli di sicurezza sui sistemi di accesso ai locali in cui si trovano le infrastrutture di comunicazioni;
- verifica della congruità dei sistemi di controllo per l’accesso;
- attività di vigilanza sui siti;
- verifica del report sulle violazioni/effrazioni dei locali tecnici o delle misure di sicurezza,
- verifica della funzionalità dei codici di accesso a sale protette e modifica dei codici con cadenza semestrale;
- controlli periodici sulla corrispondenza delle abilitazioni concesse ed il ruolo ricoperto dall’utente autorizzato.

5.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- gestione della sicurezza fisica dei siti ove risiedono le infrastrutture di rete;
- attività di vigilanza;

- attività di *reporting* delle violazioni dei locali o delle misure di sicurezza;
- definizione di contromisure possibili in caso di violazione dei locali o delle misure di sicurezza;
- definizione di codici di accesso ai locali in cui risiedono le infrastrutture di rete;
- definizione di attività di controllo sulle abilitazioni concesse per l'accesso alle infrastrutture di rete.

5.F) INFORMATIVA VERSO L'ORGANISMO DI VIGILANZA

I Responsabili delle Unità Organizzative devono comunicare, per quanto di competenza quanto segue:

a. informativa circa la politica di gestione e mantenimento dei siti in cui si trovano le infrastrutture TLC;

b. informativa sulla violazione dei siti;

c. informativa sulle misure adottate in caso di violazione dei siti.

5.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione
- Documento Programmatico per la Sicurezza

6) "GESTIONE E SICUREZZA DELLA DOCUMENTAZIONE IN FORMATO DIGITALE"

6.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività svolte per la gestione delle tecniche di crittografia applicate alla documentazione informatica e di definizione delle metodologie, delle tempistiche di archiviazione e conservazione dei documenti in formato digitale.

Il processo si articola nelle seguenti fasi:

- utilizzo di tecniche di crittografia per la protezione e la trasmissione di informazioni e documenti;
- sviluppo di un sistema di gestione di chiavi a sostegno dell'uso delle tecniche crittografiche;
- gestione dell'attività di generazione, distribuzione, revoca ed archiviazione delle chiavi crittografiche;

- gestione dell’attività di controllo dei sistemi di protezione delle chiavi, da eventuali modifiche, distribuzioni, e utilizzi non autorizzati;

- utilizzo della firma digitale nei documenti;

- definizione delle procedure per l’adozione di sistemi di certificazione, invio di documenti, modalità di archiviazione e distribuzione.

6.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, si considerino i seguenti:

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

Tale fattispecie punisce la condotta di chi si introduce abusivamente, ossia eludendo una qualsiasi forma, anche minima, di barriera ostativa all’accesso, in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo.

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

Il delitto in esame sanziona la condotta di chi abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all’accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni in questo senso, allo scopo di procurare a sé o ad altri un profitto, o di arrecare ad altri un danno.

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

La norma sanziona la condotta di chi, per danneggiare illecitamente un sistema informatico o telematico, ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero per favorire l’interruzione o l’alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna, o comunque mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

- **intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematico** (art. 617 quater c.p.)

La norma punisce la condotta di chi, in maniera fraudolenta, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, le impedisce o le interrompe oppure rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni.

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

La fattispecie in esame sanziona la condotta di chi, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico, ovvero intercorrenti fra più sistemi.

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

La fattispecie punisce la condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, salvo che il fatto costituisca più grave reato.

- **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.)

La norma sanziona la condotta di chi commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, salvo che il fatto costituisca più grave reato.

Si rileva, in particolare, che possono considerarsi di pubblica utilità le informazioni, i dati, e i programmi informatici del Comune di Venezia, gestiti ed archiviati dalla Società nonché gli applicativi o sistemi di gestione informatica sviluppati da personale Venis (quali le attività tipiche della Funzione Anagrafe e Servizi Elettorali, o la Funzione Tributi e Laboratorio Sviluppo) nell'interesse del Comune di Venezia. In tal senso, quindi, commette il suddetto reato altresì il lavoratore, collaboratore e il dirigente della Venis che danneggia le suddette informazioni e i dati del Comune di Venezia, con qualsiasi mezzo, ivi compreso, l'accesso remoto ai server del Comune stesso.

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

La fattispecie in esame punisce la condotta di chi, mediante le condotte di cui all'articolo 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, salvo che il fatto costituisca più grave reato.

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

La norma in oggetto incrimina la condotta descritta al precedente articolo 635 quater c.p., qualora essa sia diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. Si rileva, in particolare, che possono considerarsi di pubblica utilità i sistemi del Comune di Venezia, gestiti dalla Società nonché gli applicativi o sistemi di gestione informatica sviluppati da personale Venis (quali le attività tipiche della Funzione Anagrafe e Servizi Elettorali, o la Funzione Tributi e Laboratorio Sviluppo) nell'interesse del Comune di Venezia. In tal senso, quindi, commette il suddetto reato altresì il lavoratore, collaboratore e il dirigente della Venis che danneggia i sistemi informatici del Comune di Venezia o ne ostacola il funzionamento, con qualsiasi mezzo, ivi compreso, l'accesso remoto ai server del Comune stesso.

6.c) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- la Funzione Reti e Telecomunicazioni

- la Funzione Sistemi e Sicurezza Informatica

- la Funzione Tecnologie, Servizi e Sviluppo (in particolare la Funzione Conduzione Servizi, per i servizi di Anagrafe e Servizi Elettorali)

Sono, inoltre, interessati tutti gli incaricati del trattamento dei dati nonché di tutti gli addetti tecnici, come a titolo esplicativo e non esaustivo, amministratori di sistema interni e/o esterni della Società, sistemisti di rete e amministratori di database, addetti al protocollo informatico, che siano essi dirigente, dipendenti e/o collaboratori, a qualsiasi titolo, della Società.

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

6.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- segregazione delle responsabilità;

- conferimento di specifiche procure ai responsabili delle unità organizzative coinvolte al fine di dotarli del potere di rappresentanza della Società;

- definizione delle procedure per l’adozione di sistemi di certificazione, invio di documenti, modalità di archiviazione e distribuzione:

- effettuazione di verifica di congruenza delle disposizioni di sicurezza;

- tracciabilità della documentazione eventualmente richiesta e consegnata all’ente di riferimento, degli atti e delle fonti informative nelle singole fasi del processo con specifico riferimento ad impiego di risorse e tempi;

- verifica del funzionamento dei sistemi di protezione e trasmissione delle informazioni e dei documenti;

- verifica dell’attività di gestione dell’utilizzo della firma digitale nei documenti;

- verifica del funzionamento dei sistemi di certificazione, utilizzo ed invio dei documenti, e delle modalità di archiviazione e distruzione degli stessi;

- verifica della diffusione della procedura di archiviazione, produzione e manutenzione di un documento informatico a tutti i soggetti che sono coinvolti nel processo di gestione di un documento informatico.

6.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- definizione di sistemi di certificazione, invio di documenti, modalità di archiviazione e distribuzione:
- gestione dei sistemi di sicurezza e verifica del funzionamento dei sistemi di protezione e trasmissione delle informazioni e dei documenti
- attività di vigilanza;
- attività di *reporting* delle violazioni sulla sicurezza delle chiavi crittografiche;
- definizione di misure informatiche di controllo (ad es. con duplice autorizzazione di accesso) per operazioni informatiche di modifica, cancellazione, remotizzazione, alterazione, copiatura e/o distruzione e eliminazione di *files* o applicativi sui sistemi del Comune di Venezia gestiti da Venis;
- verifica dell’attività di gestione dell’utilizzo della firma digitale nei documenti;
- verifica della diffusione della procedura di archiviazione, produzione e manutenzione di un documento informatico a tutti i soggetti che sono coinvolti nel processo di gestione di un documento in formato elettronico.

6.F) INFORMATIVA VERSO L’ORGANISMO DI VIGILANZA

I Responsabili delle Unità Organizzative devono comunicare, per quanto di competenza quanto segue:

a. informativa circa la politica di certificazione, invio di documenti, modalità di archiviazione e distribuzione di documenti in formato elettronico;

b. informativa sulla violazione della sicurezza dei documenti in formato elettronico e sulle misure all’uopo adottate a titolo di contromisure.

6.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione
- Documento Programmatico per la Sicurezza

7) “GESTIONE E TRATTAMENTO DEI DATI PERSONALI”

7.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività di gestione e conservazione dei dati personali sensibili e non dei dipendenti della Società, attinenti anche alle rilevazione delle presenze del personale di Venis, gestito con il sistema WinRAP ed ai permessi e piani ferie, rilevati con il sistema SSD (Self Service Dipendente); i dati personali dei soggetti terzi, quali fornitori, consulenti e dei soggetti partecipanti alle gare di appalto gestite dalla Società; i dati personali degli utenti dei portali web gestiti dalla Società, e i dati personali dei cittadini di Venezia, presenti nel database del Comune di Venezia, ingegnerizzato, operato e manutenuto da personale della Società, nel pieno rispetto del Codice per la protezione dei dati personali e delle disposizione del Garante per la Protezione dei Dati Personali per la gestione e il trattamento dei dati personali.

Il processo si articola nelle seguenti fasi:

- Trattamento dei dati con strumenti informatici:
    - Sistema di autenticazione informatica,
    - Sistema di autorizzazione,
    - Altre misure di sicurezza,
    - Definizione del documento programmatico sulla sicurezza,
    - Ulteriori misure in caso di trattamento di dati sensibili o giudiziari;
- Trattamento dei dati senza l’ausilio di strumenti informatici.

7.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, si considerano i seguenti:

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

Tale fattispecie punisce la condotta di chi si introduce abusivamente, ossia eludendo una qualsiasi forma, anche minima, di barriera ostativa all’accesso, in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo. Detto reato si configura nel caso in cui il lavoratore dipendente, collaboratore, amministratore di sistema, etc., pur avendo titolo per accedere al sistema informatico dell’azienda, vi si introduce con la password di servizio per raccogliere dati protetti per finalità estranee alle ragioni di impiego e agli scopi sottostanti alla protezione dell’archivio informatico. Anche la duplicazione dei dati contenuti in un sistema informatico o telematico costituisce una condotta tipica del reato in esame.

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

Il delitto in esame sanziona la condotta di chi abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all’accesso ad un sistema informatico o telematico protetto da

misure di sicurezza, o comunque fornisce indicazioni o istruzioni in questo senso, allo scopo di procurare a sé o ad altri un profitto, o di arrecare ad altri un danno.

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

La norma sanziona la condotta di chi, per danneggiare illecitamente un sistema informatico o telematico, ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero per favorire l’interruzione o l’alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna, o comunque mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

- **intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematico** (art. 617 quater c.p.)

La norma punisce la condotta di chi, in maniera fraudolenta, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, le impedisce o le interrompe oppure rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni.

- **installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche** (art. 617 quinquies)

La fattispecie in esame sanziona la condotta di chi, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico, ovvero intercorrenti fra più sistemi.

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

La fattispecie punisce la condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, salvo che il fatto costituisca più grave reato.

- **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.)

La norma sanziona la condotta di chi commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, salvo che il fatto costituisca più grave reato. Si rileva, in particolare, che possono considerarsi di pubblica utilità le informazioni, i dati, e i programmi informatici del Comune di Venezia, gestiti ed archiviati dalla Società. In tal senso, quindi, commette il suddetto reato altresì il lavoratore, collaboratore e il dirigente della Venis che danneggia le suddette informazioni e i dati del Comune di Venezia, con qualsiasi mezzo, ivi compreso, l’accesso remoto ai server del Comune stesso.

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

La fattispecie in esame punisce la condotta di chi, mediante le condotte di cui all’articolo 635 bis, ovvero attraverso l’introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento, salvo che il fatto costituisca più grave reato.

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

La norma in oggetto incrimina la condotta descritta al precedente articolo 635 quater, qualora essa sia diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. Si rileva, in particolare, che possono considerarsi di pubblica utilità i sistemi del Comune di Venezia, gestiti dalla Società o alcuni applicativi gestiti da Funzioni di Venis nell'interesse del Comune di Venezia (quali quelli sviluppati dalle Funzioni Anagrafe e Servizi Elettorali o Contabilità e Personale).

In tal senso, quindi, commette altresì il suddetto reato il lavoratore, collaboratore e il dirigente della Venis che danneggi i sistemi informatici del Comune di Venezia o ne ostacoli il funzionamento, con qualsiasi mezzo, *ivi* compreso, l'accesso remoto ai server del Comune stesso.

7.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti
- la Funzione Tecnologie, Servizi e Sviluppo
- la Funzione Reti e Telecomunicazioni
- la Funzione Sistemi e Sicurezza Informatica

Sono, inoltre, interessati tutti gli incaricati del trattamento dei dati nonché di tutti gli addetti tecnici, come a titolo esplicativo e non esaustivo, amministratori di sistema esterni alla Società in rapporto diretto o funzionale con le Funzioni citate, sistemisti di rete e amministratori di database, addetti al protocollo informatico, che siano essi dirigente, dipendenti e/o collaboratori, a qualsiasi titolo, della Società.

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

7.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

Quanto ai trattamenti con strumenti elettronici:

- Sistema di autenticazione informatica:

- Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti;

- Le credenziali di autenticazione consistono in un codice per l’identificazione dell’incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell’incaricato, eventualmente associato a un codice identificativo o a una parola chiave;

- Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l’autenticazione;

- Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell’incaricato;

- La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all’incaricato ed è modificata da quest’ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi;

- Il codice per l’identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi;

- Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;

- Le credenziali sono disattivate anche in caso di perdita della qualità che consente all’incaricato l’accesso ai dati personali;

- Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;

- Quando l’accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l’autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell’incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l’incaricato dell’intervento effettuato;

- Sistema di autorizzazione:

  - per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione;

- I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all’inizio del trattamento, in modo da limitare l’accesso ai soli dati necessari per effettuare le operazioni di trattamento;

- Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione;

- Altre misure di sicurezza

  - Nell’ambito dell’aggiornamento periodico con cadenza almeno annuale dell’individuazione dell’ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione;

  - I dati personali sono protetti contro il rischio di intrusione e dell’azione di programmi di cui all’art. 615 quinquies c.p., mediante l’attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale;

  - Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l’aggiornamento è almeno semestrale;

  - Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale;

- Documento programmatico sulla sicurezza:

  - Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo;

- Ulteriori misure in caso di trattamento di dati sensibili o giudiziari:

  - I dati sensibili o giudiziari sono protetti contro l’accesso abusivo, di cui all’art. 615 ter c.p., mediante l’utilizzo di idonei strumenti elettronici;

  - Sono impartite istruzioni organizzative e tecniche per la custodia e l’uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti, anche attraverso sistemi di riconoscimento biometrico e relativa *strong authentication* abbinata a *password* o *passphrase*;

  - I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili;

- Sono adottate idonee misure per garantire il ripristino dell’accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Quanto ai trattamenti senza l’ausilio di strumenti elettronici:

- Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l’intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell’ambito dell’aggiornamento periodico con cadenza almeno annuale dell’individuazione dell’ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione;

- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;

- L’accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l’orario di chiusura, sono identificate e registrate.

7.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- Trattamento dei dati mediante l’ausilio di strumenti informatici;

- Trattamento dei dati senza l’ausilio di strumenti informatici.

7.F) INFORMATIVA VERSO L’ORGANISMO DI VIGILANZA

I Responsabili delle Unità Organizzative devono comunicare, per quanto di competenza quanto segue:

a. informativa circa la politica di gestione dei dati;

b. informativa sulla violazione della misure di sicurezza della gestione dei dati;

c. informativa sulle misure adottate in caso di violazione delle misure di sicurezza della gestione dei dati;

7.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione;
- Documento Programmatico per la Sicurezza.

8) "GESTIONE E CONSERVAZIONE DEI DATI DI TRAFFICO TELEFONICO E TELEMATICO"

8.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività svolte per la gestione e conservazione dei dati di traffico telefonico e telematico nel rispetto del provvedimento del Garante per la Protezione dei Dati Personali (anche "Garante") del 17 gennaio 2008, e successive modifiche ed integrazioni.

Il processo si articola nelle seguenti fasi:

- Sviluppo di sistemi di autenticazione informata basata su tecniche di *strong authentication*;
- Sviluppo di procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati;
- Sviluppo di sistemi informatici distinti per la conservazione dei dati di traffico per esclusive finalità di accertamento e repressione di reati;
- Designazione degli gli incaricati che possono accedere ai dati di traffico conservati per le finalità di cui all'art. 132 del Codice per la protezione dei dati personali, anche per consentire l'esercizio dei diritti di cui all'art. 7 del Codice medesimo;
- Sviluppo di sistemi che rendono i dati di traffico immediatamente non disponibili per le elaborazioni dei sistemi informativi allo scadere dei termini previsti dalle disposizioni vigenti;
- Sviluppo di soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento;
- Verifiche di controllo annuali sulla rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati;
- Attività di documentazione dei sistemi informativi utilizzati per il trattamento dei dati di traffico in modo idoneo secondo i princìpi dell'ingegneria del *software*, evitando soluzioni documentali non corrispondenti a metodi descrittivi *standard* o di ampia accettazione;

- Attività di protezione dei dati di traffico trattati per esclusive finalità di giustizia con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema.

8.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, si considerano i seguenti:

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

Tale fattispecie punisce la condotta di chi si introduce abusivamente, ossia eludendo una qualsiasi forma, anche minima, di barriera ostativa all'accesso, in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo. Detto reato si configura nel caso in cui il lavoratore dipendente, collaboratore, amministratore di sistema ecc., pur avendo titolo per accedere al sistema informatico dell'azienda, vi si introduce con la password di servizio per raccogliere dati protetti per finalità estranee alle ragioni di impiego e agli scopi sottostanti alla protezione dell'archivio informatico. Anche la duplicazione dei dati contenuti in un sistema informatico o telematico costituisce una condotta tipica del reato in esame.

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

La norma sanziona la condotta di chi, per danneggiare illecitamente un sistema informatico o telematico, ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero per favorire l'interruzione o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna, o comunque mette a disposizione di altri apparecchiature, dispositivi o programmi informatici. Rientra in questa fattispecie di reato la diffusione di virus informatici.

- **intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematico** (art. 617 quater c.p.)

La norma punisce la condotta di chi, in maniera fraudolenta, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, le impedisce o le interrompe oppure rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni.

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

La fattispecie punisce la condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, salvo che il fatto costituisca più grave reato.

- **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.)

La norma sanziona la condotta di chi commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, salvo che il fatto costituisca più grave reato. Si rileva, in particolare, che possono considerarsi di pubblica utilità le informazioni, i dati e i programmi informatici del Comune di

Venezia, gestiti, processati o archiviati dalla Società. In tal senso, quindi, commette il suddetto reato altresì il lavoratore, collaboratore e il dirigente della Venis che danneggia le suddette informazioni e i dati del Comune di Venezia, con qualsiasi mezzo, ivi compreso, l’accesso remoto ai server del Comune stesso.

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

La fattispecie in esame punisce la condotta di chi, mediante le condotte di cui all’articolo 635 bis, ovvero attraverso l’introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento, salvo che il fatto costituisca più grave reato.

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

La norma in oggetto incrimina la condotta descritta al precedente articolo 635-quater, qualora essa sia diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Si rileva, in particolare, che possono considerarsi di pubblica utilità i sistemi del Comune di Venezia, gestiti dalla Società. In tal senso, quindi, commette il suddetto reato altresì il lavoratore, collaboratore e il dirigente della Venis che danneggia i sistemi informatici del Comune di Venezia o ne ostacola il funzionamento, con qualsiasi mezzo, ivi compreso, l’accesso remoto ai server del Comune stesso.

8.c) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell’Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- la Funzione Tecnologie, Servizi e Sviluppo
- la Funzione Reti e Telecomunicazioni
- la Funzione Sistemi e Sicurezza Informatica

Sono, inoltre, interessati tutti gli incaricati del trattamento dei dati nonché di tutti gli addetti tecnici, come a titolo esplicativo e non esaustivo, amministratori di sistema esterni della Società in rapporto funzionale con gli indicati Uffici, sistemisti di rete e amministratori di database, addetti al protocollo informatico, che siano essi dirigente, dipendenti e/o collaboratori, a qualsiasi titolo, della Società.

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

8.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Verifica dei sistemi di autenticazione informatica basati su tecniche di *strong authentication,* consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, che si applichino agli accessi ai sistemi di elaborazione da parte di tutti gli incaricati di trattamento, nonché di tutti gli addetti tecnici (amministratori di sistema, di rete, di data base) che possano accedere ai dati di traffico custoditi nelle banche dati della Società, qualunque sia la modalità, locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti; inoltre:

    - Verifica che siano applicate sistemi di elaborazione dei dati di traffico trattati per esclusive finalità di accertamento e repressione dei reati basate su caratteristiche biometriche dell'incaricato, in modo tale da assicurare la presenza fisica di quest'ultimo presso la postazione di lavoro utilizzata per il trattamento;

    - Verifica che tali modalità di autenticazione siano applicate anche a tutti gli addetti tecnici (amministratori di sistema, di rete, di data base) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore;

    - verifica che relativamente ai soli addetti tecnici sopra indicati, qualora circostanze legate a indifferibili interventi per malfunzionamenti, guasti, installazioni hardware e software, aggiornamento e riconfigurazione dei sistemi, determinino la necessità di accesso informatico a sistemi di elaborazione che trattano dati di traffico in assenza di *strong authentication*, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B) al Codice per la protezione dei dati personali, sia tenuta traccia dell'evento in un apposito "registro degli accessi", nonché delle motivazioni che li hanno determinati, con una successiva descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve è custodito dalla Società presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dalla Società;

- verifica delle procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati. La Società definisce e attribuisce agli incaricati specifici profili di autorizzazione differenziando le funzioni di trattamento dei dati di traffico per finalità di ordinaria gestione da quelle per finalità di accertamento e repressione dei reati e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato;

- per la conservazione dei dati di traffico per esclusive finalità di accertamento e repressione di reati, verifica dello sviluppo di sistemi informatici distinti fisicamente da quelli utilizzati per gestire dati di traffico anche per altre finalità, sia nelle componenti di elaborazione, sia di immagazzinamento dei dati (*storage*). I dati di traffico conservati per un periodo non superiore ai sei mesi dalla loro generazione

possono, invece, essere trattati per le finalità di giustizia sia prevedendone il trattamento con i medesimi sistemi di elaborazione e di immagazzinamento utilizzati per la generalità dei trattamenti, sia provvedendo alla loro duplicazione, con conservazione separata rispetto ai dati di traffico trattati per le ordinarie finalità; inoltre;

- Verifica che le attrezzature informatiche utilizzate per i trattamenti di dati di traffico per le esclusive finalità di giustizia di cui sopra siano collocate all’interno di aree ad accesso selezionato (ovvero riservato ai soli soggetti legittimati ad accedervi per l’espletamento di specifiche mansioni) e munite di dispositivi elettronici di controllo o di procedure di vigilanza che comportino la registrazione dei dati identificativi delle persone ammesse, con indicazione dei relativi riferimenti temporali;

- Nel caso di trattamenti di dati di traffico telefonico per esclusive finalità di giustizia, il controllo degli accessi comprende una procedura di riconoscimento biometrico;

- Verifica che la società adotti misure idonee a garantire il ripristino dell’accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici in tempi compatibili con i diritti degli interessati e comunque non superiori a sette giorni;

- verifica sulla designazione degli incaricati che possono accedere ai dati di traffico conservati per le finalità di cui all’art. 132 del Codice per la protezione dei dati personali, anche per consentire l’esercizio dei diritti di cui all’art. 7 del Codice medesimo. Il processo di designazione prevede la documentata frequenza di una periodica attività formativa concernente l’illustrazione delle istruzioni, il rispetto delle misure di sicurezza e le relative responsabilità; inoltre:

  - Verifica, per quanto riguarda le richieste per l’esercizio dei diritti di cui all’art. 7 del Codice per la protezione dei dati personali che comportano l’estrazione dei dati di traffico, che Venis conservi in forma specifica la documentazione comprovante l’idonea verifica dell’identità del richiedente, e adottare opportune cautele per comunicare i dati al solo soggetto legittimato in base al medesimo articolo;

- verifica del sistema che determina i dati di traffico immediatamente non disponibili per le elaborazioni dei sistemi informativi allo scadere dei termini previsti dalle disposizioni vigenti; inoltre:

  - verifica che i sistemi elettronici di memorizzazione anche temporanea di Venis cancellino o rendano anonimi senza ritardo tali dati, in tempi tecnicamente compatibili con l’esercizio delle relative procedure informatiche, nei data base e nei sistemi di elaborazione utilizzati per i trattamenti nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (*backup*, sincrono ed asincrono, e *disaster recovery*) effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente e, al più tardi, documentando tale operazione entro i trenta giorni successivi alla scadenza dei termini di cui all’art. 132 del Codice per la protezione dei dati personali;

- verifica delle soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento; inoltre:

  - Tra le soluzioni sono comprese la registrazione, in un apposito *audit log*, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi

connessi, sia quando consistono o derivano dall’uso interattivo dei sistemi, sia quando sono svolte tramite l’azione automatica di programmi informatici;

- I sistemi di *audit log* devono garantire la completezza, l’immodificabilità, l’autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad auditing;

- Verifica che siano adottate, per la registrazione dei dati di auditing, anche in forma centralizzata per ogni impianto di elaborazione o per *data center*, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull’utilizzo di tecnologie crittografiche;

- verifica, con cadenza almeno annuale, un’attività di controllo interno per verificare costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati. Tale attività di controllo è demandata a un’unità organizzativa o, comunque, a personale diverso rispetto a quelli cui è affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati. I controlli comprendono anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di *Alerting* e di *Anomaly Detection*, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull’integrità dei dati e delle procedure informatiche adoperate per il loro trattamento; inoltre:

  - Verifiche periodiche sull’effettiva cancellazione dei dati decorsi i periodi di conservazione. L’attività di controllo è adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate. L’esito dell’attività di controllo deve essere: comunicato alle persone e agli organi legittimati ad adottare decisioni e ad esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della società; richiamato nell’ambito del documento programmatico sulla sicurezza nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza; messo, a richiesta, a disposizione del Garante o dell’autorità giudiziaria;

- verifica sull’attività di documentazione dei sistemi informativi utilizzati per il trattamento dei dati di traffico in modo idoneo secondo i principi dell’ingegneria del software, evitando soluzioni documentali non corrispondenti a metodi descrittivi standard o di ampia accettazione; inoltre:

  - La descrizione comprende, per ciascun sistema applicativo, l’architettura logico-funzionale, l’architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di input/output dei dati di traffico da e verso altri sistemi, l’architettura della rete di comunicazione, l’indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema;

  - La documentazione è corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l’esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati;

  - La documentazione tecnica è aggiornata e messa a disposizione dell’Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico;

- verifica dell’attività di protezione dei dati di traffico trattati per esclusive finalità di giustizia con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema; inoltre:

    - La Società adotta soluzioni che rendano le informazioni residenti nelle basi di dati a servizio delle applicazioni informatiche utilizzate per i trattamenti, non intelligibili a chi non disponga di diritti di accesso e profili di autorizzazione idonei, ricorrendo a forme di cifratura od offuscamento di porzioni dei data base o degli indici o ad altri accorgimenti tecnici basati su tecnologie crittografiche;

    - I flussi di trasmissione dei dati di traffico tra sistemi informatici di Venis hanno luogo tramite protocolli di comunicazione sicuri, basati su tecniche crittografiche, o comunque evitando il ricorso alla trasmissione in chiaro dei dati. Protocolli di comunicazione sicuri sono adottati anche per garantire più in generale la sicurezza dei sistemi evitando di esporli a vulnerabilità e a rischio di intrusione.

8.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- Sviluppo di sistemi di autenticazione informata basata su tecniche di *strong authentication*;

- Sviluppo di procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati;

- Sviluppo di sistemi informatici distinti per la conservazione dei dati di traffico per esclusive finalità di accertamento e repressione di reati;

- Designazione degli gli incaricati che possono accedere ai dati di traffico conservati per le finalità di cui all’art. 132 del Codice per la protezione dei dati personali, anche per consentire l’esercizio dei diritti di cui all’art. 7 del Codice medesimo;

- Sviluppo di sistemi che rendono i dati di traffico immediatamente non disponibili per le elaborazioni dei sistemi informativi allo scadere dei termini previsti dalle disposizioni vigenti;

- Sviluppo di soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento;

- Verifiche di controllo annuali sulla rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati,

- Attività di documentazione dei sistemi informativi utilizzati per il trattamento dei dati di traffico in modo idoneo secondo i principi dell’ingegneria del *software*, evitando soluzioni documentali non corrispondenti a metodi descrittivi *standard* o di ampia accettazione;

- Attività di protezione dei dati di traffico trattati per esclusive finalità di giustizia con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema.

8.F) INFORMATIVA VERSO L’ORGANISMO DI VIGILANZA

I Responsabili delle Unità Organizzative devono comunicare, per quanto di competenza quanto segue:

a. informativa circa la politica di gestione dei dati di traffico telefonici e telematici;

b. informativa sulla violazione della misure di sicurezza della gestione dei dati;

c. informativa sulle misure adottate in caso di violazione delle misure di sicurezza della gestione dei dati.

8.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;

- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione

- Documento Programmatico per la Sicurezza

PARTE TERZA – DELITTI DI CRIMINALITÀ ORGANIZZATA

(art. 24 ter del Decreto)

L'art. 24 ter del Decreto, aggiunto dal comma 29 dell'articolo 2 della legge 15 luglio 2009, n. 94, ha esteso l'ambito di applicazione della responsabilità amministrativa dell'Ente ai c.d. reati associativi. A seguito dell'introduzione dell'art. 24 ter, tali reati, che precedentemente rientravano nell'ambito del medesimo Decreto soltanto quando presentavano il carattere della transnazionalità (ad opera della Legge 16 marzo 2006, n. 146, di Ratifica ed Esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, che li aveva introdotti), assumono oggi rilievo anche quando non costituiscono oggetto di criminalità internazionale.

Si tratta, precisamente, dei reati di **associazione per delinquere** (art. 416 c.p.) e **associazione mafiosa** (art 416 bis c.p.), del reato di **scambio elettorale politico-mafioso** (art. 416 ter del c.p.), del reato di **sequestro di persona a scopo di estorsione** (art. 630 c.p.) e dei **reati di associazione finalizzata al traffico degli stupefacenti**, previsti dall'art. 74 del T.U. di cui al d.P.R. n. 309 del 1990 (Testo Unico sugli stupefacenti).

Rientrando nella categoria dei reati di associazione, per il perfezionamento dei reati sopra elencati è richiesto che tre o più persone fisiche si associno al precipuo scopo di commettere uno o più delitti. Perché le descritte fattispecie criminose siano rilevanti ai fini del Decreto debbono inoltre essere poste in essere nell'interesse o a vantaggio della Società. Tra le possibili modalità attuative di tali reati sono da ricomprendervi anche quelle condotte che si sostanziano in una agevolazione della organizzazione criminale, mediante l'individuazione, la creazione e la corresponsione di fonti finanziamento e di sostentamento, in modo da contribuire alla costituzione, alla conservazione ed al rafforzamento dell'organizzazione medesima. In concreto, possono assumere rilevanza la realizzazione di acquisti o l'effettuazione di finanziamenti ed investimenti finalizzati al supporto dell'organizzazione criminale.

In considerazione dell'attività svolta da Venis e delle sue finalità statutarie, il rischio concreto di perfezionamento di tali reati è sostanzialmente inesistente, con la sola possibile eccezione della fattispecie prevista all'art. 416 ter c.p. (scambio elettorale politico-mafioso), comunque remoto in considerazione del profilo della Società, dei sistemi di controllo e comportamento adottati, la sua vocazione operativa e l'etica condivisa dai suoi componenti.

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

(art. 25 bis del Decreto)

Di seguito, sono elencate le aree di attività "a rischio" e le eventuali modalità attuative dei reati contro la fede pubblica di cui all'articolo 25 bis del Decreto.

Aree a rischio

Nonostante in considerazione dell'attività svolta da Venis e del suo oggetto sociale, sia estremamente difficile che tali reati possano essere perpetrati, è il caso comunque di soffermare l'attenzione sulle seguenti attività a rischio:

1) Acquisti di beni e servizi, incassi, pagamenti.

1) "ACQUISTI DI BENI E SERVIZI, INCASSI, PAGAMENTI"

1.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce a tutte le attività svolte dagli Uffici aziendali preposti agli acquisti di beni e servizi, agli incassi ed ai pagamenti.

1.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Spendita e introduzione nello Stato, senza concerto, di monete falsificate; spendita di monete falsificate ricevute in buona fede (artt. 455 e 457 c.p.).

Il **reato di cui all'art. 455 c.p.** si configura nel caso di acquisizione ovvero nel caso di detenzione, al fine della spendita, di monete falsificate, da parte dei soggetti preposti alle operazioni di incasso e pagamento, effettuate in contanti, anche laddove le monete falsificate siano state ricevute in buona fede.

Il **reato di cui all'art. 457 c.p.**, si configura nel caso di spendita o messa in circolazione di monete contraffatte o alterate, da parte dei soggetti preposti alle operazioni di incasso e pagamento, effettuate in contanti, anche laddove le monete falsificate siano state ricevute in buona fede.

Affinché si perfezioni il reato in esame, non è necessario che sussista il dolo. In ogni caso, affinché si perfezionino entrambe le fattispecie criminose, è necessaria l'accettazione della moneta falsificata da parte del terzo.

1.C) FUNZIONI INTERESSATE

Gli ambiti aziendali potenzialmente interessati dalle attività a rischio di commissione di reati contro la fede pubblica sono stati individuati sulla base dell'Organigramma Venis allegato alla Parte Generale del Presente Modello.

Essi ricomprendono:

- l'Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza e Bilancio
- la Funzione Acquisti, Gare e Contratti

Sono altresì interessati tutti i dirigenti, dipendenti e collaboratori, pur non ricompresi nelle Funzioni sopra elencate, operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

1.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi della **separazione di ruolo** nelle fasi chiave del processo e della **tracciabilità delle fasi del processo**. In particolare, gli elementi specifici di controllo sono di seguito rappresentati:

- la segregazione delle responsabilità tra le aree/soggetti che svolgono le attività di:
    - Acquisti
    - Incassi
    - Pagamenti
- l'esistenza di specifici criteri autorizzativi;
- l'esistenza di sistemi di verifica per perseguire il rispetto dei canoni di integrità, trasparenza e correttezza del processo con particolare riguardo alla tracciabilità delle varie fasi, nonché ai tempi e alle risorse impiegate;
- l'esistenza di adeguati meccanismi di gestione delle deroghe a quanto sopra esposto.

1.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo.

In particolare:

- procedere agli acquisti ed ai pagamenti soltanto nel pieno rispetto di quanto previsto dalle procedure organizzative aziendali;
- definire criteri di rotazione delle persone coinvolte nei processi di acquisti di beni e servizi, incassi e pagamenti.

1.F) FLUSSI INFORMATIVI VERSO L’ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni interessate devono comunicare, per quanto di competenza e con periodicità definita, quanto segue:

Flusso 1: elenco degli acquisti gestiti in deroga

Flusso 2: elenco degli incassi e pagamenti gestiti in deroga

1.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Principi di Comportamento Generali e nei Rapporti con la Pubblica Amministrazione.

PARTE QUINTA – DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

(art. 25 bis 1 del Decreto)

Nell'estendere la responsabilità amministrativa degli Enti ai delitti contro l'industria ed il commercio l'art. 25 bis 1 del Decreto richiama espressamente gli articoli dal 513 al 517 quater del c.p.. L'ambito della responsabilità amministrativa è quindi esteso ai seguenti delitti contro l'economia pubblica: **turbata libertà dell'industria o del commercio** (art. 513 c.p.), **illecita concorrenza con minaccia o violenza** (art. 513 bis c.p.), **frodi contro le industrie nazionali** (art. 514 c.p.), **frode nell'esercizio del commercio** (art. 515 c.p.), **vendita di sostanze alimentari non genuine come genuine** (art. 516 c.p.), **vendita di prodotti industriali con segni mendaci** (art. 517 c.p.), **fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale** (art. 517 ter c.p.), **contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari** (art. 517 quater c.p.).

In considerazione dell'attività svolta da Venis e del suo oggetto sociale, tenuto conto della peculiarità dei reati in questione caratterizzati da particolari modalità di condotta e da finalità fortemente tipizzate, il rischio di commissione degli stessi da parte di personale Venis o incaricato è da ritenersi pressoché inesistente.

PARTE SESTA – REATI SOCIETARI

(art. 25 ter D.Lgs 231/2001)

Con l'introduzione dell'art. 25 ter del Decreto, la responsabilità amministrativa dell'Ente è stata estesa ad alcuni reati societari, se commessi nell'interesse della Società da amministratori, direttori generali o liquidatori nonché da persone sottoposte alla loro vigilanza qualora il fatto non si fosse realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica. L'art. 25 ter richiama espressamente alcuni articoli del Codice Civile, che in questa sede non si riportano in quanto oggetto di specifica analisi nella Parte Generale del presente Modello.

La L. 6 novembre 2012 n. 190 "(*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalita' nella pubblica amministrazione*) ha disposto l'integrale sostituzione dell'art. 2635 del c.c. (ex infedeltà patrimoniale), oggi rubricato "corruzione tra privati".

"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.

2. 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.

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

4. 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.

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

La medesima legge ha introdotto nell'art. 25 ter, **la nuova lettera s-bis** che annovera, tra i reati-presupposto del decreto, il nuovo reato di "**corruzione tra privati**", limitatamente ai casi previsti dal terzo comma del medesimo articolo, cioè **limitatamente al lato attivo della fattispecie criminosa plurisoggettiva (la dazione/promessa di utilità da parte di chiunque a favore dei soggetti societari qualificati di cui ai commi 1 e 2 dell'art. 2365 c.c.)**.

Stando al richiamo di cui all'art. 25 ter, D. Lgs. 231/2001, lett. s-bis, può essere sanzionata la Società nel cui interesse/vantaggio, chiunque corrisponda e/o prometta denaro e/o utilità a favore dei soggetti individuati nei commi 1 e 2 dell'art. 2635 c.c..

La fattispecie delittuosa in esame viene quindi in essere con riferimento a due distinte società, quella alla quale appartiene al corruttore e quella alla quale appartengono i soggetti corrotti. Ai sensi del Decreto, la sanzionabilità dell'Ente per responsabilità amministrativa dipendente da reato riguarda soltanto la società a cui appartiene il soggetto corruttore.

Il principio è che solo questa società possa essere avvantaggiata dalla condotta corruttrice, mentre, la società cui appartiene il soggetto corrotto sarebbe vittima di un danno, legato alla condotta corruttiva e determinato dalla violazione dei doveri d'ufficio o di fedeltà da parte dei soggetti qualificati aziendali.

Nella realtà, non è difficile ipotizzare dei casi in cui soggetto corruttore e corrotto appartengano alla medesima società (cosiddetta corruzione "endosocietaria"). L'esempio di scuola è quello in cui l'amministratore di una società, per coprire un propria responsabilità nella gestione, corrisponda una somma di danaro ad un membro del collegio sindacale. Il sindaco, in violazione dei propri doveri, omette di rilevare il problema con un evidente **danno per la Società**. E' chiaro che in un caso come questo, tuttavia, l'amministratore potrebbe avere in mente anche una **finalità di vantaggio per l'Ente**, nella prospettiva, ad esempio, di una futura operazione di fusione o di vendita. Ne discende che sarebbe anche ipotizzabile una responsabilità della Società ex D. lgs. 231/2001.

E' allora possibile che una stessa Società sia responsabile del fatto criminoso ex D. Lgs. 231/2001 e nello stesso tempo persona offesa da un fatto di corruzione tra privati?

La dottrina recentissima formatasi in materia ravvisa la soluzione del quesito nella descrizione della fattispecie tipica della corruzione tra privati. **Trattasi invero di un reato di evento, in cui l'evento è il danno per la Società**. Laddove non si verifichi il nocumento per la Società, il fatto che il soggetto (amministratore, direttore generale, dirigente o sindaco, come nel caso di specie) compia od ometta, in cambio di una dazione o promessa di utilità, un atto contrario al proprio ufficio o obbligo di fedeltà, non è penalmente rilevante.

Ne consegue che **non sembra possibile la contestuale qualificazione della medesima Società come persona offesa da un fatto di corruzione tra privati e, nel medesimo tempo, responsabile di quel fatto ai sensi del D. Lgs. 231/2001, con esclusione della cosiddetta corruzione endosociataria**.

Per completezza occorre segnalare che parte della dottrina ha rilevato come si sarebbe potuta raggiungere una diversa conclusione, se la corruzione tra privati fosse stata inquadrata come un reato di pericolo in cui il bene giuridico tutelato fosse la libera concorrenza, come si era prospettato durante i lavori parlamentari della Legge 190/2012. In tal caso sarebbe stato possibile ipotizzare un accordo illecito nell'ambito della stessa Società, distorsivo della concorrenza da un lato e finalizzato nel contempo ad avvantaggiare la Società, con conseguente responsabilità della stessa ex D. lgs. 231/2001.

In considerazione dell'attività svolta da Venis, se pur il linea teorica, considerata la vocazione ed i principi a cui si ispira la Società nello svolgimento della propria attività e nel perseguimento della propria missione, espressi e cristallizzati nel Codice Etico, il rischio di commissione dei reati di cui all'art. 25 ter del Decreto, ivi compresa la fattispecie di cui alla nuova lettera s-bis, non può essere escluso.

Una ulteriore precisazione si rende necessaria con riferimento al reato di aggiotaggio (art. 2637 c.c.). Si tratta di reato di pericolo concreto, che si realizza attraverso la diffusione di notizie false ovvero attraverso operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati oppure per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

Circa i soggetti attivi, la fattispecie si presenta come reato comune, e quindi potrebbe teoricamente interessare trasversalmente tutte le funzioni apicali di Venis detentrici di informazioni che possano rivestire una qualche incidenza sulla percezione aziendale sul mercato, nel caso teorico in cui (tutt'altro che ipotizzabile, salvo eventi societari straordinari quali un mutamento di azionariato o di vocazione della Società) Venis intenda dar vita all'emissione di strumenti finanziari propri.

Aree a rischio

Passando alla specifica individuazione delle **aree a rischio,** con riferimento al reato di cui all'art. 25 *ter* del Decreto, si segnalano i seguenti relativi **processi operativi**:

1) redazione del bilancio, delle situazioni patrimoniali, e delle relazioni e delle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico;

2) restituzione dei conferimenti;

3) ripetizione degli utili e delle riserve;

4) operazioni sul capitale e destinazione dell'utile;

5) riduzione del capitale sociale, fusioni e scissioni ed aumento del capitale sociale;

6) ripartizione dei beni sociali da parte dei liquidatori;

7) lavori dell’assemblea;

8) relazioni tra amministratori e collegio sindacale incaricato della revisione dei conti in merito all’attività di controllo e di revisione di quest’ultimi;

9) rapporti con organismi di vigilanza relativi allo svolgimento di attività regolate dalla legge;

10) emissione di strumenti finanziari propri

Fermi restando i principi di carattere generale individuati nel Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione e validi con riferimento a tutte le aree a rischio di commissione dei reati societari, la rilevanza, per Venis, delle attività proprie delle aree a rischio sopra considerate, rende quanto mai opportuno procedere all’analisi separata di ogni singola attività aziendale interessata, al fine di individuare specificamente i caratteri propri di ogni processo considerato, verificando i reati ipotizzabili in ogni settore e le relative possibili modalità attuative, le singole attività di controllo previste e gli specifici protocolli comportamentali diretti ad evitare il perfezionamento dei reati ipotizzabili ed infine inquadrare i relativi flussi informativi con l’O.d.V..

1) “REDAZIONE DEL BILANCIO E DELLE COMUNICAZIONI SOCIALI”

1.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività svolte per la redazione del bilancio, delle situazioni patrimoniali e delle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, da parte di Venis, allo scopo di assicurare che la Società ponga in essere ogni attività in tal senso necessaria nel rispetto delle prescrizioni di legge.

Il processo si articola nelle seguenti fasi:

- elaborazione delle stime necessarie e delle valutazioni per la redazione di bilancio e degli altri documenti contabili;
- predisposizione ed elaborazione di ogni dato economico, patrimoniale e finanziario sottostante alla redazione dei documenti contabili;
- redazione del progetto di bilancio;
- approvazione del progetto di bilancio da parte dell’Organo Amministrativo;
- preparazione e redazione delle relazioni di accompagnamento al bilancio e delle altre comunicazioni sociali previste dalla legge;
- deposito delle comunicazioni sociali.

1.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, possiamo considerare le false comunicazioni sociali (art. 2621 c.c.), le false comunicazioni sociali in danno dei soci e dei creditori (art. 2622 c.c.) e la corruzione tra privati (art. 2635 c.c. terzo comma).

La **fattispecie di cui all'art. 2621 c.c.**, in quanto reato proprio, si perfeziona laddove gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci ed i liquidatori, nonché coloro che secondo l'articolo 110 del codice penale, concorrono nel reato da questi ultimi commesso (soggetti attivi del reato), espongano fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni nei bilanci, nelle relazioni e nelle altre comunicazioni sociali previste dalla legge e dirette ai soci o al pubblico, ovvero omettano informazioni la cui comunicazione sia imposta dalla legge, al fine di ingannare i soci o il pubblico e di conseguire per sé o per altri un ingiusto profitto. Sia la falsità che l'omissione devono riguardare la situazione economica, finanziaria e patrimoniale della Società in modo da indurre in errore i destinatari della stessa. Il reato si consuma, infatti, nel momento in cui la comunicazione, falsa o incompleta, giunge a conoscenza dei soci e del pubblico.

Soggetto attivo di tali reati è anche colui che svolga, in modo significativo e continuativo, le medesime funzioni sopra considerate, anche se diversamente qualificate.

La punibilità è estesa anche all'ipotesi in cui le informazioni false ovvero omesse riguardino beni posseduti od amministrati dalla Società per conto di terzi, mentre, perché si abbia punibilità, le falsità e le omissioni debbono alterare in modo sensibile la rappresentazione della situazione economica, patrimoniale e finanziaria.

È necessario, infatti, che le informazioni false o omesse, idonee ad indurre in errore i destinatari, abbiano un particolare rilievo per la punibilità. Quest'ultima è, infatti, esclusa dal legislatore: (a) nel caso in cui le informazioni false o omesse siano tali da non alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene; (b) qualora le falsità o le omissioni non determinino 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 differiscono in misura non superiore al 10% da quella corretta. La punibilità si estende anche all'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla Società per conto di terzi.

Il reato preso in esame si configura, quindi, con riferimento a Funzioni apicali dell'azienda ovvero coinvolte direttamente o indirettamente nella predisposizione ed elaborazione dei dati finanziari o economici e patrimoniali aziendali, ovvero funzioni aventi potenzialmente il ruolo di comunicare informazioni della Società a terzi (quale, nel caso specifico, la Funzione Sistema Qualità, Relazioni Esterne e Formazione).

Affinché si produca la **fattispecie delittuosa di cui all'art. 2622 c.c.** è necessario anche che sia cagionato un danno patrimoniale ai soci o ai creditori.

Il reato prende in esame gli obblighi di informativa a carico delle funzioni apicali preposte, innanzitutto, alla tutela e gestione del patrimonio sociale nell'interesse degli *stakeholders* e quindi risultano coinvolte nella fattispecie le funzioni di Venis coinvolte direttamente o indirettamente nella predisposizione ed elaborazione di ogni dato economico, patrimoniale e finanziario sottostante alla redazione dei documenti contabili aziendali ovvero funzioni aventi potenzialmente il ruolo di comunicare informazioni della Società a terzi.

Quanto alle modalità attuative di entrambi i reati in esame, essi potrebbero realizzarsi laddove venissero esposti dati non veritieri, ovvero venissero omesse informazioni la cui comunicazione è imposta per legge, oltre che nel bilancio di esercizio e nel bilancio consolidato, anche nella relazione degli amministratori alla società, *ex* art. 2428

c.c., nella relazione degli amministratori ai sindaci, *ex* art. 2429 c.c., nel prospetto contabile di cui all'art 2433 bis c.c., relativamente alla delibera degli amministratori di distribuzione di acconti sui dividendi, ovvero nella relazione con la quale gli amministratori illustrano le proposte di aumento del capitale sociale ai soci ed al collegio sindacale, *ex* art. 2441 c.c. ed, in ogni caso, in tutte le comunicazioni previste dalla legge.

Con riguardo alla nozione di "*comunicazioni sociali previste dalla legge*" e dirette ai soci o al pubblico, si deve fare riferimento ai veicoli informativi contemplati dalla legge, anche se soltanto facoltativi. Tra le numerose comunicazioni sociali si citano, ad esempio, le relazioni di accompagnamento ai bilanci e le situazioni patrimoniali straordinarie, ovverosia i documenti contabili che gli amministratori sono tenuti a redigere in occasione di eventi, quali la diminuzione di oltre un terzo del capitale sociale o la distribuzione di acconti sui dividendi.

Non rientrano nella previsione in esame le comunicazione relative alla situazione patrimoniale della società, trasmesse a singoli destinatari (ad es., un'Autorità amministrativa o un istituto di credito).

La **fattispecie di cui all'art. 2635 c.c. terzo comma** si realizza quando un soggetto dia o prometta utilità a favore di soggetti societari di cui ai commi 1 e 2 dell'art. 2365 c.c. (amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori o soggetti sottoposti alla loro vigilanza) e costoro, a fronte della promessa o dazione di utilità, compiano od omettano atti, in violazione degli obblighi di fedeltà o inerenti al loro ufficio, con nocumento alla società (salvo che il fatto costituisca più grave reato).

Coerentemente all'impostazione complessiva del D. lgs. 231/2001, la ratio incriminatrice della norma va ravvisata nell'esigenza di reprimere le forme di "mala gestio" connesse ad un fenomeno di deviazione del buon andamento societario.

Esempio concreto può essere quello di un dirigente di Venis (corruttore) che, per procurare un vantaggio alla Società, fornisca denaro all'amministratore o ad un dirigente di una società cliente per falsificare dati economici e/o finanziari in suo possesso, rilevanti nella redazione del bilancio o di altri documenti contabili, con conseguente danno per la società cui appartiene viceversa il corrotto.

In questo caso, la responsabilità ex D. Lgs. 231/2001 sarebbe di Venis, società di cui farebbe parte il soggetto corruttore (il cui comportamento è diretto a procurare un vantaggio per la Società), sebbene il soggetto corrotto sia comunque punibile ai sensi dell'art. 2635 c.c. (corruzione tra privati) per il danno cagionato alla società cui si riferisce.

1.c) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello. Relativamente alla fattispecie di reato prevista, devono pertanto prendersi in considerazione unicamente le funzioni di Venis che, direttamente o indirettamente, possano partecipare alla predisposizione ed elaborazione di ogni dato economico, patrimoniale e/o finanziario sottostante alla redazione dei documenti contabili aziendali o informative societarie aventi tale funzione.

Esse ricomprendono:

- Assemblea

- Organo Amministrativo
- Collegio Sindacale e Revisore dei Conti
- Direzione Coordinamento Generale
- Funzione Finanza , Bilancio e Amministrazione del Personale
- Funzione Acquisti, Gare e Contratti
- Funzione Tecnologie, Servizi e Sviluppo
- Responsabile del Procedimento
- Funzione Comunicazione

Sono altresì interessati tutti i dirigenti e dipendenti preposti alla redazione dei documenti contabili societari, e tutti i dirigenti e dipendenti pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni, consulenti e partner operanti nelle fasi del processo di predisposizione ed elaborazione di ogni dato economico, patrimoniale e finanziario sottostante alla redazione dei documenti contabili o informativi aziendali.

1.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono costituiti da:

- Verifica del rispetto dei principi di legge e regolamentari, nazionali, comunitari e internazionali, ove applicabili, per la redazione del bilancio d’esercizio e relative comunicazioni obbligatorie;
- Verifica dell’adempimento da parte delle persone incaricate dell’attività di redazione del bilancio e di Funzioni aziendali delle regole comportamentali ispirate ai principi di collaborazione, completezza, trasparenza e chiarezza delle informazioni fornite;
- Controllo sulla tracciabilità delle operazioni di inserimento, modifica e cancellazione dei dati contabili;
- Verifica delle procedure e regole che identifichino ruoli e responsabilità, relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio dall’approvazione dell’Organo Amministrativo al deposito e pubblicazione (anche informatica) dello stesso e alla relativa archiviazione;
- Controllo sul comportamento degli amministratori, sindaci e i liquidatori, al fine di accertare la massima correttezza nella redazione delle comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico.

Con particolare riferimento alla nuova fattispecie di corruzione tra privati (art. 2635 c.c. terzo comma):

- Esame della documentazione aziendale rilevante in materia "anticorruzione" e valutazione dei presidi, delle procedure, dei controlli e delle prassi in materia esistenti all'interno della società, al fine di individuare eventuali lacune/punti deboli.

1.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi di redazione, elaborazione, calcolo o rendicontazione di informazioni di carattere contabile, finanziario o economico, ed in particolare nelle seguenti attività:

- elaborazione delle stime necessarie e delle valutazioni per la redazione di bilancio e degli altri documenti contabili;
- predisposizione ed elaborazione di ogni dato economico, patrimoniale e finanziario sottostante alla redazione dei documenti contabili;
- redazione del progetto di bilancio e relative informative di corredo;
- approvazione del progetto di bilancio da parte dell'Organo Amministrativo;
- deposito e pubblicazione delle relazioni di accompagnamento al bilancio, del bilancio e delle altre comunicazioni sociali previste dalla legge.

Con specifico riferimento alla fattispecie della corruzione tra privati (art. 2635 terzo comma):

- fornire una rappresentazione della realtà aziendale all'interno della quale individuare le criticità connesse al tema della corruzione tra privati e le aree aziendali in cui il rischio di corruzione è più concreto, con conseguente indicazione delle azioni correttive da intraprendere nell'ambito delle attività di formazione del personale sul Modello Organizzativo inserire un modulo formativo specifico sul tema dell'"anticorruzione".

1.F) INFORMATIVA VERSO L'ORGANISMO DI VIGILANZA

Il Responsabile della Funzione Generali Finanza e Bilancio deve comunicare, per quanto di competenza ed anche avvalendosi della collaborazione di altre Funzioni societarie coinvolte, quanto segue:

a. Informativa circa la formulazione di prospetti contabili o finanziari riferiti alle singole Funzioni aziendali, ai fini delle comunicazioni contabili obbligatorie;

b. Informativa sulle delibere assembleari e dell'Organo Amministrativo assunte per l'approvazione del bilancio e relative altre comunicazioni sociali.

1.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;

- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione.

2) “RESTITUZIONE DEI CONFERIMENTI”

2.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività svolte per la restituzione dei conferimenti ai soci ovvero alla liberazione dall’obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale.

Il processo si articola nelle seguenti fasi:

- predisposizione dei prospetti contabile per la redazione del bilancio;
- predisposizione del progetto di bilancio;
- approvazione del progetto di bilancio da parte dell’Organo Amministrativo;
- adozione da parte degli Amministratori di misure atte a restituire i conferimenti ai soci o liberare i medesimi dall’obbligo di effettuarli.

2.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, si può considerare il reato di **indebita restituzione dei conferimenti** (art. 2626 c.c.), che si configura nel caso in cui gli Amministratori della Società, anche per il tramite di delegati o di dipendenti della Società, restituiscano, anche simulatamente, i conferimenti ai soci, ovvero li liberino, anche simulatamente, dall’obbligo di versarli. Incriminando solo l’amministratore la legge non ha inteso punire anche il socio beneficiario della restituzione o della liberazione. Tuttavia, l’esclusione del concorso necessario non implica anche quella del concorso eventuale. Andrà comunque circoscritto il coinvolgimento dei soci nel fatto degli amministratori ai casi in cui gli stessi non si siano limitati a trarre giovamento dalla restituzione o dalla liberazione, ma abbiano fornito un effettivo contributo eziologico e di volontà, qualificabile in termini di determinazione, istigazione o rafforzamento del proposito criminoso dei titolari dei poteri di gestione.

Presupposto di carattere negativo, affinché il reato si produca è, come si è detto, che la condotta di restituzione o di liberazione avvenga fuori dai casi di legittima riduzione del capitale, con ciò intendendosi quindi il “capitale reale”.

In particolare, per quanto riguarda l’ipotesi di illecita restituzione dei conferimenti, essa potrebbe ricorrere, nei rapporti con i soci, nel caso di: concessione di mutui fittizi o senza serie possibilità di restituzione, di stipulazione di contratti di scambio che siano economicamente svantaggiosi per la società, di distribuzione di utili non effettivamente conseguiti, di illecito acquisto di azioni proprie da parte della società ovvero di versamento di onorari non congrui per prestazioni professionali, in modo da diminuire la garanzia patrimoniale effettiva dei creditori.

Quanto alla liberazione dei soci dall’obbligo di effettuare i conferimenti, essa ricorrerebbe ogniqualvolta siano poste in essere condotte idonee a svincolare i soci dall’obbligo di effettuare i relativi versamenti, quali, ad esempio, la compensazione del debito inerente il predetto conferimento con un credito fittizio verso la società o una dichiarazione mendace circa l’avvenuto conferimento da parte del socio.

2.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- Assemblea
- Organo Amministrativo
- Collegio Sindacale e Revisore dei Conti
- Direzione Coordinamento Generale
- Funzione Finanza e Bilancio
- Funzione Acquisti, Gare e Contratti

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni, consulenti e partner operanti nelle fasi del processo precedentemente individuate.

2.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Verifica del rispetto dei principi di legge e regolamentari, nazionali, comunitari e internazionali, ove applicabili, per la redazione del bilancio d'esercizio;
- Verifica dell'adempimento da parte delle persone incaricate dell'attività di redazione del bilancio d'esercizio delle regole comportamentali ispirate ai principi di collaborazione, completezza e chiarezza delle informazioni fornite;
- Controllo sulla tracciabilità delle operazioni di inserimento, modifica e cancellazione dei dati contabili, con particolare riferimento alla configurazione e calcolo del patrimonio sociale;
- Controllo sull'attività degli amministratori, delegati o collaboratori per l'adozione di misure o delibere inerenti alla restituzione di conferimenti ai soci o ad effettuare di attività di liberazione del soci dall'obbligo di eseguire i conferimenti;
- Verifica delle procedure che identifichino ruoli e responsabilità, relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio dall'approvazione dell'Organo Amministrativo al deposito e pubblicazione (anche informatica) dello stesso e alla relativa archiviazione;

- Controllo sul comportamento degli amministratori, sindaci e i liquidatori, al fine di accertare la massima correttezza nella redazione delle comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico.

2.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- predisposizione dei prospetti contabili ed informative per la redazione del bilancio e relativo progetto;
- analisi e controllo di delibere di approvazione del progetto di bilancio da parte dell’Organo Amministrativo ed Assemblea;
- adozione da parte degli Amministratori di misure atte a restituire i conferimenti ai soci o liberare medesimi dall’obbligo di effettuarli.

2.F) INFORMATIVA VERSO L’ORGANISMO DI VIGILANZA

Il Responsabile della Funzione Finanza e Bilancio deve comunicare, per quanto di competenza ed anche avvalendosi della collaborazione di altre Funzioni societarie coinvolte, quanto segue:

a. Prospetti contabili o finanziari elaborati dalle diverse Funzioni aziendali;

b. Informativa sulle ipotesi di delibere assembleari e dell’Organo Amministrativo con riferimento a restituzione o svincolo da obblighi di conferimento;

c. Informativa circa i provvedimenti sulla restituzione dei conferimenti ai soci o circa la liberazione dei medesimi dall’obbligo di effettuarli**.**

2.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione.

3) "RIPARTIZIONE DEGLI UTILI E DELLE RISERVE"

3.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività concernenti le operazioni finanziarie e contabili disposte dagli amministratori, anche per il tramite di delegati, la redazione del bilancio di esercizio e delle situazioni patrimoniali, il compimento di valutazioni estimative delle voci di bilancio, la tenuta delle scritture contabili.

Il processo si articola nelle seguenti fasi:

- tenuta delle scritture contabili;
- predisposizione dei prospetti contabili per la redazione del bilancio;
- predisposizione del progetto di bilancio;
- approvazione del progetto di bilancio da parte dell'Organo Amministrativo;;adozione da parte dell'Organo Aministrativo di misure di ripartizione degli utili o delle riserve.

3.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, può considerarsi il reato di **illegale ripartizione degli utili o delle riserve** (art. 2627 c.c.).

Detto reato si configura sia nel caso di ripartizione di "*utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva"*, sia nel caso di ripartizione di riserve, anche non costituite con utili, che non possano per legge essere distribuite, da parte degli amministratori, anche per il tramite di delegati o, comunque, di dipendenti della Società.

Il reato si consuma nel momento e nel luogo in cui il danaro (o altro valore) viene percepito o entra nella disponibilità del socio.

La norma prevede una speciale causa di estinzione del reato, costituita dalla restituzione degli utili o dalla ricostituzione delle riserve entro il termine previsto per l'approvazione del bilancio.

Riguardo alla prima condotta criminosa, è dibattuta la questione se per "utile" debba intendersi l'utile di esercizio o l'utile di bilancio o complessivo (differenza attiva tra patrimonio netto e capitale sociale, alla cui determinazione concorrono anche gli utili di esercizi passati accantonati a riserva e le riserve c.d. da capitale).

Considerato che il bene giuridico protetto è l'integrità del "*patrimonio sociale indisponibile*", sembra coerente riferirsi agli utili di bilancio non effettivamente conseguiti. Quanto agli utili "*destinati per legge a riserva*", essi coincidono con quegli utili sottoposti a vincolo di destinazione di fonte normativa e non statutaria.

Riguardo alla seconda condotta incriminata (illegale ripartizione delle riserve), le riserve alle quali la norma in esame si riferisce sono le riserve obbligatorie *ex lege*. Quanto ai comportamenti simulati ai quali fa riferimento la norma in esame, essi potrebbero, consistere, ad esempio, in erogazioni effettuate a titolo di prestito ai soci.

3.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate, individuate sulla base dell’Organigramma Venis allegato alla Parte Generale del presente Modello, sono:

- Assemblea
- Organo Amministrativo
- Collegio Sindacale e Revisore dei Conti
- Direzione Coordinamento Generale
- Funzione Finanza e Bilancio
- Funzione Acquisti, Gare e Contratti

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

3.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Verifica del rispetto dei principi di legge e regolamentari, nazionali, comunitari e internazionali, ove applicabili, per la redazione del bilancio d’esercizio, e sulla ripartizione degli utili e delle riserve;
- Verifica dell’adempimento da parte delle persone incaricate dell’attività di redazione del bilancio d’esercizio delle regole comportamentali ispirate ai principi di collaborazione, completezza, chiarezza delle informazioni fornite;
- Controllo sulla tracciabilità delle operazioni di inserimento, modifica e cancellazione dei dati contabili;
- Controllo sull’attività degli amministratori, delegati o collaboratori per l’adozione di misure sulla ripartizione degli utili e delle riserve;
- Verifica delle procedure che identifichino ruoli e responsabilità, relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio dall’approvazione dell’Organo Amministrativo al deposito e pubblicazione (anche informatica) dello stesso e alla relativa archiviazione.
- Controllo sul comportamento degli amministratori, sindaci e i liquidatori, al fine di accertare la massima correttezza nella redazione delle comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico.

3.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e al Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- tenuta delle scritture contabili;
- predisposizione dei prospetti contabile per la redazione del bilancio;
- predisposizione del progetto di bilancio;
- approvazione del progetto di bilancio da parte dell'Organo Amministrativo;;
- adozione da parte degli Amministratori di misure di ripartizione degli utili e delle riserve.

3.F) INFORMATIVA VERSO L'ORGANISMO DI VIGILANZA

Il Responsabile della Funzione Finanza e Bilancio deve comunicare, per quanto di competenza ed anche avvalendosi della collaborazione di altre Funzioni societarie coinvolte, quanto segue:

a. Prospetti contabili elaborati dalle diverse Funzioni aziendali

b. Informativa sulle delibere assembleari e dell'Organo Amministrativo sull'approvazione del bilancio e sulla relazione di accompagnamento;

c. Informativa sulle misure di ripartizione degli utili e delle riserve.

3.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione.

4) "OPERAZIONI SUL CAPITALE E DESTINAZIONE DEGLI UTILI"

4.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività concernenti le operazioni finanziarie e contabili disposte dagli amministratori, anche per il tramite di delegati, la redazione del bilancio di esercizio e delle situazioni patrimoniali, e la richiesta di prestiti a istituti di credito.

Il processo si articola nelle seguenti fasi:

- tenuta delle scritture contabili;
- predisposizione dei prospetti contabile per la redazione del bilancio;
- predisposizione del progetto di bilancio;
- approvazione del progetto di bilancio da parte dell'Organo Amministrativo; ;
- adozione da parte degli Amministratori o Procuratori speciali di misure non conformi o di richieste di prestiti ad istituti di credito o destinazioni non riferibili a voci contabili di riferimento.

4.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, possiamo considerare il reato di **illecite operazioni sulle azioni della società o della controllante** (art. 2628 c.c.).

Detto reato si configura nel caso di sottoscrizione di azioni proprie, al di fuori dai casi consentiti ai sensi dell'art. 2357 c.c. (azioni che siano "*interamente liberate*" e "*nei limiti degli utili distribuibili e delle riserve disponibili*"), da parte degli amministratori, anche per il tramite di delegati o procuratori *ad negotia*, o comunque per il tramite di dipendenti della Società.

L'ipotesi criminosa prevista dal secondo comma del medesimo articolo è incentrata, invece, sull'acquisto o sottoscrizione di azioni emesse dalla società controllante, al di fuori dei casi consentiti ai sensi dell'art. 2359 bis c.c. (azioni della società controllante che siano "*interamente liberate*" e sempre che l'acquisto avvenga "*nei limiti degli utili distribuibili e delle riserve disponibili*"), da parte degli amministratori, anche per il tramite di delegati o, comunque, di dipendenti della società, nonché "*per il tramite di società fiduciarie o per interposta persona*".

Ai fini della configurabilità di entrambe le ipotesi delittuose, occorre che si sia verificata una lesione del capitale sociale o delle riserve non distribuibili per legge.

Anche questo articolo prevede, al terzo comma, una causa di estinzione del reato identica a quella di cui all'art. 2627 c.c., ovverosia la ricostituzione del capitale sociale o delle riserve prima del termine fissato per l'approvazione del bilancio.

4.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- Assemblea
- Organo Amministrativo
- Collegio Sindacale e Revisore dei Conti

- Direzione Coordinamento Generale
- Funzione Finanza e Bilancio
- Funzione Acquisti, Gare e Contratti

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

4.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Verifica del rispetto dei principi di legge e regolamentari, nazionali, comunitari e internazionali, ove applicabili, per la redazione del bilancio d’esercizio, e sulla sottoscrizione di azioni proprie;
- Verifica dell’adempimento da parte delle persone incaricate dell’attività di redazione del bilancio d’esercizio delle regole comportamentali ispirate ai principi di collaborazione, completezza, chiarezza delle informazioni fornite;
- Controllo sulla tracciabilità delle operazioni di inserimento, modifica e cancellazione dei dati contabili;
- Controllo sull’attività degli amministratori, delegati o collaboratori per l’adozione di misure sulla sottoscrizione di azioni proprie;
- Verifica delle procedure che identifichino ruoli e responsabilità, relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio dall’approvazione dell’Organo Amministrativo al deposito e pubblicazione (anche informatica) dello stesso e alla relativa archiviazione.
- Controllo sul comportamento degli amministratori, sindaci e i liquidatori, al fine di accertare la massima correttezza nella redazione delle comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico.

4.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- tenuta delle scritture contabili;
- predisposizione dei prospetti contabile per la redazione del bilancio;

- predisposizione del progetto di bilancio;
- approvazione del progetto di bilancio da parte dell'Organo Amministrativo;
- adozione da parte degli Amministratori di azioni finalizzate alla sottoscrizione di azioni proprie.

4.F) INFORMATIVA VERSO L'ORGANISMO DI VIGILANZA

Il Responsabile della Funzione Generali Finanza e Bilancio deve comunicare, per quanto di competenza ed anche avvalendosi della collaborazione di altre Funzioni societarie coinvolte, quanto segue:

a. Prospetti contabili elaborati dalle diverse Funzioni aziendali;

b. Informativa sulle delibere assembleari e dell'Organo Amministrativo sull'approvazione del bilancio e sulla relazione di accompagnamento;

c. Informativa sulle azioni di sottoscrizione di azioni proprie.

4.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione.

5) "RIDUZIONE DEL CAPITALE SOCIALE, FUSIONI E SCISSIONI" ED "AUMENTO DEL CAPITALE SOCIALE"

5.A) DESCRIZIONE DEI PROCESSI

I processi si riferiscono segnatamente:

1) alle attività concernenti le operazioni di riduzione del capitale sociale, fusioni e scissioni;

2) alle attività concernenti le operazioni di aumento del capitale sociale

I processi si articolano nelle seguenti fasi:

- tenuta delle scritture contabili;
- predisposizione dei prospetti contabile per la redazione del bilancio;
- predisposizione del progetto di bilancio;
- approvazione del progetto di bilancio da parte dell'Organo Amministrativo;

- approvazione da parte dell'Organo Amministrativo di delibere di fusione o scissione aventi per effetto la riduzione di capitale sociale;

- adozione della delibera di riduzione del capitale sociale, fusione o scissione o adozione della delibera di aumento del capitale sociale

5.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, possiamo considerare, con particolare riferimento alle attività concernenti le operazioni di riduzione del capitale sociale, fusioni e scissioni, il reato di **operazioni in pregiudizio ai creditori** (art. 2629 c.c.).

L'art. 2629 c.c. incrimina gli amministratori – anche laddove agiscano per il tramite di delegati o di dipendenti della Società – i quali effettuino riduzioni del capitale sociale, fusioni con altre società, scissioni, in violazione delle disposizioni di legge. Tali ipotesi sono considerate tassative dalla giurisprudenza, e quindi non risulterebbero estensibili ad altri tipi di operazione societarie di carattere straordinario (quale l'affitto di ramo d'azienda).

Affinché si produca il reato in esame, è necessario che si verifichi un danno per i creditori. La norma in esame prevede, quale causa estintiva del reato, il risarcimento del danno ai creditori prima del giudizio.

In particolare, il reato si realizza laddove gli amministratori non osservino le disposizioni di legge poste a tutela dei creditori, tra le quali si segnalano, gli artt. 2445, c. 3, e 2503 c.c., i quali riconoscono ai creditori il diritto di fare opposizione entro tre mesi dal giorno in cui la delibera di riduzione del capitale sociale, di fusione o di scissione è stata iscritta nel registro delle imprese; gli articoli 2501 bis c.c., relativamente alla redazione del progetto di fusione, 2501 ter c.c., relativamente alla redazione della situazione patrimoniale, 2501 quater c.c., relativamente alla relazione degli Amministratori sul rapporto di concambio delle azioni.

Gli amministratori non possano addurre a propria scusante il fatto di aver agito "per ordine" dell'assemblea, ovvero in esecuzione di specifico mandato. Ferme restando, comunque, situazioni di concorso eventuale di persone nel reato a carico dei soci che abbiano consapevolmente votato le statuizioni illegali.

Con attenzione, invece, alle attività concernenti le operazioni di aumento del capitale sociale, tra i reati ipotizzabili, si può considerare il reato di **formazione fittizia del capitale** (art. 2632 c.c.), che si configura nel caso: (a) di "*attribuzione di azioni per somma inferiore al loro valore nominale*"; (b) di "*sottoscrizione reciproca di azioni*"; e (c) di "*sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della Società in caso di trasformazione*", da parte degli Amministratori, anche per il tramite di delegati, dipendenti e/o consulenti.

Nel primo caso, il reato si consuma laddove gli Amministratori attribuiscono azioni a fronte di conferimenti, in danaro o in altri beni, di valore inferiore a quella parte del capitale sociale che le azioni rappresentano.

Nel secondo caso, il reato si consuma al momento della sottoscrizione.

In ordine alla stima o eventuale sovrastima dei conferimenti, è necessario fare riferimento alla procedura descritta dagli artt. 2343 e 2440 c.c., e quindi alla necessità che chi conferisca beni in natura o crediti in Venis debba presentare una relazione giurata di esperto con relativa descrizione e attestazione di valore ai fini dell'attribuzione e determinazione del capitale sociale, con annesso eventuale calcolo di sovrapprezzo. Gli Amministratori, nei

termini indicati dalle norme, sono tenuti al controllo della valutazione dei beni, anche ai fini di eventuale riduzione di capitale nel caso emergano valori inferiori.

5.C) FUNZIONI INTERESSATE

Le Funzioni interessate da entrambe le attività sopra contemplate sono state individuate sulla base dell’Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- Assemblea
- Organo Amministrativo
- Collegio Sindacale e Revisore dei Conti
- Direzione Coordinamento Generale
- Funzione Finanza e Bilancio
- Funzione Acquisti, Gare e Contratti

la Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi dei processi precedentemente individuate.

5.D) SISTEMA DI CONTROLLO

Il sistema di controllo per entrambi i processi si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Verifica del rispetto dei principi di legge e regolamentari, nazionali, comunitari e internazionali, ove applicabili, per la redazione del bilancio d’esercizio, e sulle operazioni di riduzione del capitale sociale, fusione e scissione, anche relativamente alla reportistica ed informativa dovuta ai soci ed all’Assemblea;
- Verifica dell’adempimento da parte delle persone incaricate dell’attività di redazione del bilancio d’esercizio delle regole comportamentali ispirate ai principi di collaborazione, completezza e trasparenza delle informazioni fornite;
- Controllo sulla tracciabilità delle operazioni di inserimento, modifica e cancellazione dei dati contabili;
- Controllo sull’attività degli amministratori, delegati o collaboratori per l’adozione di misure sulla sottoscrizione di azioni proprie;
- Verifica delle procedure che identifichino ruoli e responsabilità, relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio dall’approvazione dell’Organo Amministrativo al deposito e pubblicazione (anche informatica) dello stesso e alla relativa archiviazione;

- Controllo sul comportamento degli amministratori, consulenti, sindaci e i liquidatori, al fine di accertare la massima correttezza nella redazione delle comunicazioni su operazioni societarie straordinarie, così come su informazioni obbligatorie anche periodiche ed imposte o comunque previste dalla legge e dirette ai soci o al pubblico (ad es. agli organismi di vigilanza quali l’AVCP o l’Agcom).

5.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- tenuta delle scritture contabili;
- predisposizione dei prospetti contabile per la redazione del bilancio;
- predisposizione del progetto di bilancio;
- approvazione del progetto di bilancio o di delibere di fusione o scissione con riduzione di capitale sociale da parte dell’Organo Amministrativo;
- adozione da parte degli Amministratori di azioni finalizzate alla riduzione del capitale sociale, fusione e scissione, o all’aumento del capitale sociale.
- delibere dell’Assemblea in merito ad aumenti di capitale per conferimento di beni.

5.F) INFORMATIVA VERSO L’ORGANISMO DI VIGILANZA

Il Responsabile della Funzione Finanza e Bilancio deve comunicare, per quanto di competenza ed anche avvalendosi della collaborazione di altre Funzioni societarie coinvolte, quanto segue:

a. Prospetti contabili elaborati dalle diverse Funzioni aziendali;

b. Informativa sulle delibere assembleari e dell’Organo Amministrativo sull’approvazione del bilancio e sulla relazione di accompagnamento;

c. Informativa sulle azioni di riduzione del capitale sociale, fusione e scissione o sull’aumento di capitale.

5.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione.

6) "RIPARTIZIONE DEI BENI SOCIALI DA PARTE DEI LIQUIDATORI"

6.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività concernenti il processo di ripartizione dei beni sociali da parte dei liquidatori.

Il processo si articola nelle seguenti fasi:

- verifica scritture contabili
- verifica del bilancio;
- accantonamento delle somme necessarie ai fini di soddisfazione dei creditori sociale regolarmente censiti;
- pagamento dei creditori sociali;
- ripartizione dei beni sociali tra i soci e chiusura di liquidazione.

6.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, possiamo considerare il reato di **indebita ripartizione dei beni sociali da parte dei liquidatori** (art. 2633 c.c.).

Il reato di cui all'articolo 2633, c.c. si configura nel caso di ripartizione di beni sociali, da parte dei liquidatori, prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, laddove sia cagionato un danno ai creditori. La *ratio* della previsione in esame è infatti, la protezione delle ragioni dei creditori, i quali vantano sui beni sociali un diritto di prelazione.

Trattandosi di un reato di evento, il momento di consumazione del reato coincide con il verificarsi del danno in capo ai creditori. A questo riguardo, va, pero, precisato che, affinché il reato si produca,è sufficiente che sia stato effettuato anche soltanto il primo dei pagamenti in favore dei soci, sempre che questo comporti un danno nella sfera patrimoniale dei creditori sociali.

6.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono,:

- Assemblea
- Liquidatori
- Collegio Sindacale e Revisore dei Conti.

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni, consulenti e partner operanti nelle fasi del processo precedentemente individuate.

6.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Verifica del rispetto dei principi di legge e regolamentari, nazionali, comunitari e internazionali, ove applicabili, per la redazione del bilancio d’esercizio;
- Verifica dell’adempimento da parte delle persone incaricate dell’attività di redazione del bilancio d’esercizio delle regole comportamentali ispirate ai principi di collaborazione, completezza, chiarezza delle informazioni fornite;
- Controllo sulla tracciabilità delle operazioni di inserimento, modifica e cancellazione dei dati contabili;
- Controllo sull’attività di accantonamento delle somme per pagare i creditori sociali e di pagamento dei creditori sociali;
- Verifica delle procedure di ripartizione dei beni sociali tra i soci.
- Controllo sul comportamento dei sindaci e liquidatori, al fine di accertare la massima correttezza nella redazione delle comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico

6.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- verifica delle scritture contabili;
- verifica del bilancio e redazione del bilancio di liquidazione;
- verifica delle poste di riserva e ricostruzione degli accantonamenti necessari per soddisfare i creditori sociali;
- pagamento dei creditori sociali;
- ripartizione dei beni sociali tra i soci ed approvazione del bilancio di chiusura.

6.F) INFORMATIVA VERSO L'ORGANISMO DI VIGILANZA

Il Liquidatore ed il Presidente del Collegio Sindacale devono comunicare, per quanto di competenza ed anche avvalendosi della collaborazione di altre Funzioni societarie coinvolte, quanto segue:

a. Prospetti contabili;

b. Informativa sull'accantonamento delle somme per pagare i creditori sociali;

c. Informativa sul pagamento dei creditori sociali;

d. Informativa sulle ripartizioni dei beni sociali tra i soci.

6.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione.

7) "LAVORI DELL'ASSEMBLEA"

7.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle corrette attività concernenti il funzionamento dell'assemblea, dalla sua convocazione, informative, ponderazioni sino all'assunzione delle delibere.

Il processo si articola nelle seguenti fasi:

- convocazione dell'assemblea;
- costituzione dell'assemblea;
- regolare tenuta dei consessi, ordinato svolgersi ed adozione di delibere.

7.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, possiamo considerare il reato di **illecita influenza sull'assemblea** (art. 2636 c.c.).

Il reato di illecita influenza sull'assemblea si configura nel caso in cui Amministratori, Direttori Generali, Liquidatori o soggetti sottoposti alla loro vigilanza, determino il formarsi della maggioranza assembleare per il tramite di "*atti simulati o fraudolenti*", allo scopo di procurare, a sé o ad altri, un ingiusto profitto.

Per la consumazione del reato è richiesto che la condotta determini effettivamente la maggioranza assembleare.

Quanto agli atti simulati o fraudolenti, questi possono consistere, ad esempio: a) nella cessione, solo apparente, ad un prestanome delle proprie azioni, allo scopo di esercitare il voto in assemblea anche in presenza di un personale conflitto di interesse; b) nell'utilizzo di azioni non legittimamente emesse; c) nella "compravendita" di diritti di voto; d) nella falsificazione del verbale di assemblea al fine di far figurare come presenti e votanti soci che in realtà non sono intervenuti o che non hanno votato o che hanno votato in maniera diversa.

In dottrina, si è giustamente posto il dubbio se, dalla commissione del reato in esame, possa scaturire la responsabilità amministrativa della Società ai sensi del Decreto. Crea qualche perplessità, infatti, la possibilità che una condotta volta ad alterare il corretto funzionamento di un organo della Società sia posta in essere nell'interesse di quest'ultima.

7.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- Assemblea
- Organo Amministrativo
- Collegio Sindacale e Revisore dei Conti
- Direzione Coordinamento Generale

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

7.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Verifica del rispetto dei principi di legge e regolamentari, nazionali, comunitari e internazionali, ove applicabili, per la convocazione e costituzione dell'assemblea;
- Verifica del rispetto dei principi di legge e regolamentari nazionali, comunitari ed internazionali, ove applicabili, sull'adozione delle delibere assembleari.

Controllo sul comportamento degli amministratori, sindaci e/o i liquidatori, al fine di accertare la massima correttezza nella redazione delle comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico.

7.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- Convocazione dell'assemblea;
- Costituzione dell'assemblea;
- Approvazione delle delibere assembleari.

7.F) INFORMATIVA VERSO L'ORGANISMO DI VIGILANZA

Il Segretario dell'Assemblea deve comunicare, per quanto di competenza all'Organismo di Vigilanza, quanto segue:

a. informativa sulla convocazione dell'assemblea;

b. informativa sulla costituzione dell'assemblea e sulle relative delibere assembleari.

7.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione.

8) "RELAZIONI TRA GLI AMMINISTRATORI E IL COLLEGIO SINDACALE INCARICATO DELLA REVISIONE DEI CONTI IN MERITO ALL'ATTIVITÀ DI CONTROLLO E DI REVISIONE DI QUEST'ULTIMI"

8.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce alle attività concernenti le relazioni tra gli amministratori, da una parte, ed il collegio sindacale con funzioni di revisore dei conti, dall'altra, per quanto attiene allo svolgimento delle attività di controllo sull'amministrazione della società, di vigilanza sull'osservanza della legge e dell'atto costitutivo e di accertamento e revisione della gestione contabile – amministrativa, attribuite al collegio sindacale.

Il processo si articola nelle seguenti fasi:

- Attività relative alle tenute delle scritture contabili da parte degli amministratori, anche per il tramite degli addetti alla contabilità;
- Controlli effettuati dal collegio sindacale sui documenti contabili;

- Richieste di esibizioni di libri e scritture, le richieste di informazioni, di chiarimenti e di rendiconti.

8.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, possiamo considerare il reato di **impedito controllo** (art. 2625, comma 2, c.c.), ovverossia il caso di occultamento di documenti, o l'adozione di altre condotte artificiose poste in essere dagli Amministratori, anche per il tramite di delegati o, comunque, di dipendenti della Società, che siano strumentali ad impedire, ma anche solo ad ostacolare, l'esercizio delle attività di controllo e di revisione da parte del Collegio Sindacale.

Affinché si produca il reato in esame, è necessario che derivi un danno patrimoniale in capo ai soci.

Per quanto riguarda le modalità attuative, il reato potrebbe realizzarsi non solo nel caso di nascondimento, sia temporaneo che definitivo, di documenti rilevanti ai fini del controllo e della revisione, ma anche ogniqualvolta siano poste in essere condotte idonee a simulare una situazione aziendale inesistente ovvero a dissimulare una situazione aziendale esistente, al fine di creare una falsa apparenza materiale.

8.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell'Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- Assemblea
- Organo Amministrativo
- Collegio Sindacale e Revisore dei Conti
- Direzione Coordinamento Generale
- Funzione Finanza e Bilancio
- Funzione Acquisti, Gare e Contratti

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

8.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Verifica del rispetto dei principi di legge e regolamentari, nazionali, comunitari e internazionali, ove applicabili, per le attività relative alle tenuta dei libri e delle scritture contabili da parte degli amministratori, anche il tramite degli addetti alla contabilità;

- Verifica del rispetto dei principi di legge e regolamentari nazionali, comunitari ed internazionali, ove applicabili, da parte del collegio sindacale sui controlli effettuati in merito alla regolarità della tenuta delle scritture contabili;

- Verifica del rispetto dei principi di legge e regolamentari nazionali, comunitari ed internazionali, ove applicabili, sulle richieste di esibizione di libri e scritture, e sulle le richieste di informazioni, di chiarimenti e di rendiconti.

- Controllo sul comportamento degli amministratori, sindaci e liquidatori, al fine di accertare la massima correttezza nella redazione delle comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico

8.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- Attività relative alle tenute delle scritture contabili da parte degli amministratori, anche per il tramite degli addetti alla contabilità;

- Controlli effettuati dal collegio sindacale sui documenti contabili;

- Richieste di esibizioni di libri e scritture, le richieste di informazioni, di chiarimenti e di rendiconti.

8.F) INFORMATIVA VERSO L’ORGANISMO DI VIGILANZA

Il Responsabile della Funzione Finanza e Bilancio deve comunicare, per quanto di competenza quanto segue:

a. informativa sulla tenute delle scritture contabili da parte degli amministratori, anche per il tramite degli addetti alla contabilità;

b. informativa sui Controlli effettuati dal collegio sindacale sui documenti contabili.

8.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;

- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione.

9) "RAPPORTI CON ORGANISMI DI VIGILANZA RELATIVI ALLO SVOLGIMENTO DI ATTIVITÀ REGOLATE DALLA LEGGE"

9.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce ai rapporti tra la Società e le Autorità pubbliche di Vigilanza nell'esercizio delle loro funzioni.

Il processo si articola nelle seguenti fasi:

- Attività relative alle tenute delle scritture contabili da parte degli amministratori, anche per il tramite degli addetti alla contabilità;
- Controlli effettuati dal collegio sindacale sui documenti contabili;
- Predisposizione di informative o comunicazioni, anche periodiche, necessarie o richieste da Autorità di Vigilanza nell'esercizio delle funzioni aziendali;
- Richieste di esibizioni di libri e scritture, le richieste di informazioni, di chiarimenti e di rendiconti.

9.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, possiamo considerare il reato di **ostacolo alle funzioni delle Autorità di Vigilanza** (art. 2638 c.c.), per ciò intendendosi ogni tipo di Autorità preposta ai controlli di attività o conduzione della Società, e quindi in particolare nel rispetto delle formalità dovute nei casi di gare ad evidenza pubblica (laddove Venis rivesta la qualifica di stazione appaltante), rendicontazione di gestione (Comune di Venezia ed eventuale Corte dei Conti) o attività sociale (Agcom, AVCP, Co.Re.Com. competente, Garante per la Protezione dei Dati Personali, etc.) per l'erogazione di servizi di comunicazione elettronica al pubblico.

L'articolo prevede due figure autonome di reato, entrambe particolarmente importanti per Venis, tenuto conto della sua particolare attività e natura di operatore di comunicazioni soggetto a regolamentazione di settore.

La prima di mera condotta e a dolo specifico, costruito al fine di ostacolare l'esercizio delle funzioni di vigilanza; la seconda a forma libera e ad evento naturalistico di ostacolo delle funzioni delle autorità pubbliche di vigilanza. Il medesimo elemento (l'ostacolo) equipara il disvalore dell'intenzione ed il disvalore di evento, individuato nella prima ipotesi come oggetto del dolo specifico e nella seconda quale evento di fatto. La condotta criminosa si realizza attraverso l'esposizione nelle comunicazioni alle Autorità di Vigilanza previste dalla legge, al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, che abbiano un riflesso diretto sulla situazione economica, patrimoniale o finanziaria della Società ovvero attraverso l'occultamento con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima.

Il reato si configura, in queste prime ipotesi, avendo riferimento alla situazione dei dati economici, patrimoniali e/o finanziari soggetti a comunicazione, alterati o omessi secondo la fattispecie prevista. Quindi interessa, in tali

primi casi, tipicamente le funzioni aziendali preposte alla redazione e predisposizione di atti informativi di natura contabile.

Tuttavia, il secondo comma dell’articolo sanziona ed estende l’illecito anche ai comportamenti che riguardino obblighi di comunicazioni o informazioni della Società rivolti in generale agli organi generali di controllo di settore o di vigilanza, e quindi interessa trasversalmente numerose funzioni di Venis incaricate sia di informare su singole attività operative (ad es. le comunicazioni ad organismi di controllo sulle gare ed appalti pubblici laddove la Società rivesta il ruolo di stazione appaltante, quali, a titolo d’esempio, l’AVCP o l’Osservatorio regionale/centrale sui contratti pubblici) sia delle comunicazioni periodiche o meno sulla propria attività di settore nell’offerta di servizi di comunicazioni (quali l’Autorità per le Garanzie nelle Comunicazioni o il Garante per la Protezione dei Dati Personali).

La condotta criminosa si realizza, in tali casi, quando siano, in qualsiasi forma, anche mediante omissione delle comunicazioni dovute, intenzionalmente ostacolate le funzioni delle autorità di vigilanza. L’art. 2638 c.c. delinea un reato proprio, ascrivibile ad amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci, liquidatori di società o enti, nonché più genericamente nei confronti di tutti i soggetti che *ex lege* siano sottoposti alle autorità pubbliche di vigilanza ovvero abbiano specifici obblighi di rendicontazione anche eventualmente indiretta nei loro confronti (quali, nel caso concreto, la funzione Tecnologie, Servizi e Sviluppo, la Funzione Finanza e Bilancio, la Funzione Acquisti, Gare e Contratti, interagenti a titolo diverso con Autorità esterne di controllo o vigilanza).

Il reato in questione interessa pertanto la quasi totalità delle funzioni apicali aziendali, e si configura nel caso: (i) di comunicazione alle Autorità di Vigilanza, al fine di ostacolare l’esercizio delle funzioni, di fatti materiali non rispondenti al vero in merito alla situazione patrimoniale, economica e finanziaria della Società, ovvero di occultamento fraudolento di informazioni e dati rilevanti in merito alla predetta situazione; (ii) di condotte, anche omissive, che ostacolino le attività ispettive e di controllo delle Autorità di Vigilanza; in generale, di qualsiasi condotta ostruzionistica, di opposizione, di mancata collaborazione, che impedisca o renda difficoltoso l’esercizio delle funzioni di vigilanza.

In particolare, quanto alle modalità attuative delle condotte tipiche individuate dalla norma, è necessario tenere presente che il reato potrebbe realizzarsi non solo nel caso di false o mancate comunicazioni all’Autorità ad esito di specifiche richieste o istruzioni da questa formulate nell’esercizio dei suoi poteri ed in relazione a singole circostanze o operazioni economiche, ma anche nel caso in cui, più genericamente, si cerchi di simulare una situazione aziendale inesistente ovvero di dissimularne una esistente.

9.c) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell’Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- Organo Amministrativo
- Collegio Sindacale e Revisore dei Conti
- Direzione Coordinamento Generale

- Funzione Finanza e Bilancio
- Funzione Acquisti, Gare e Contratti
- Funzione Tecnologie, Servizi e Sviluppo

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

9.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Verifica del rispetto dei principi di legge e regolamentari, nazionali, comunitari e internazionali, ove applicabili, per le attività relative alle tenuta dei libri e delle scritture contabili da parte degli amministratori, anche il tramite degli addetti alla contabilità;
- Verifica del rispetto dei principi di legge e regolamentari nazionali, comunitari ed internazionali, ove applicabili, da parte del collegio sindacale sui controlli effettuati in merito alla regolarità della tenuta delle scritture contabili;
- Verifica del rispetto dei principi di legge e regolamentari nazionali, comunitari ed internazionali, ove applicabili, sulle richieste di esibizione di libri e scritture, e sulle le richieste di informazioni, di chiarimenti e di rendiconti.

Controllo sul comportamento degli amministratori, sindaci e liquidatori, al fine di accertare la massima correttezza nella redazione delle comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico

9.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- Attività relative alle tenute delle scritture contabili da parte degli amministratori, anche per il tramite degli addetti alla contabilità;
- Controlli effettuati dal collegio sindacale sui documenti contabili;
- Predisposizione di informative consuntive, preventive o periodiche di rito alle Autorità di Vigilanza;
- Richieste di esibizioni di libri e scritture, le richieste di informazioni, di chiarimenti e di rendiconti.

9.F) INFORMATIVA VERSO L'ORGANISMO DI VIGILANZA

Il Responsabile della Funzione Finanza e Bilancio e la Funzione Acquisti, Gare e Contratti devono comunicare, per quanto di competenza quanto segue:

a. informativa sulla tenute delle scritture contabili da parte degli amministratori e sulle rendicontazioni obbligatorie dovute dalla Società, anche per il tramite degli addetti alla contabilità;

b. informativa sui controlli effettuati dal collegio sindacale sui documenti contabili;

c. informativa generale sugli obblighi di rendicontazione periodica, preventiva o consuntiva alle Autorità di Vigilanza

d. informativa consuntiva annuale sulle relazioni prodotte e sui controlli effettuati dalle Autorità di Vigilanza.

9.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione.

10) "EMISSIONE DI STRUMENTI FINANZIARI PROPRI"

10.A DESCRIZIONE DEL PROCESSO

Il processo si riferisce all'attività di emissione di strumenti finanziari propri.

Il processo si articola nelle seguenti fasi:

- predisposizione ed elaborazione di ogni dato economico, patrimoniale e finanziario sottostante alla redazione dei documenti contabili;
- redazione del progetto di bilancio;
- approvazione del progetto di bilancio da parte dell'Organo Amministrativo;
- delibera di approvazione della decisione di emissione di strumenti finanziari propri;
- preparazione e redazione delle relazioni di accompagnamento al bilancio e delle altre comunicazioni sociali previste dalla legge;
- deposito delle comunicazioni sociali.

10.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Tra i reati ipotizzabili, possiamo considerare l’**aggiotaggio** di cui all’art. 2637 c.c..

Trattasi di reato di pericolo concreto, che si realizza attraverso la diffusione di notizie false ovvero attraverso operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati oppure per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull’affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

Circa i soggetti attivi, la fattispecie si presenta come reato comune, e quindi potrebbe teoricamente interessare trasversalmente tutte le funzioni apicali di Venis detentrici di informazioni che possano rivestire una qualche incidenza sulla percezione aziendale sul mercato, nel caso teorico in cui Venis intenda dar vita all’emissione di strumenti finanziari propri.

10.C) FUNZIONI INTERESSATE

Le Funzioni interessate dalle attività sopra contemplate sono state individuate sulla base dell’Organigramma Venis allegato alla Parte Generale del presente Modello.

Esse ricomprendono:

- Assemblea
- Organo Amministrativo
- Collegio Sindacale e Revisore dei Conti
- Direzione Coordinamento Generale
- Funzione Finanza e Bilancio
- Funzione Acquisti, Gare e Contratti

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate, nonché collaboratori esterni e partner operanti nelle fasi del processo precedentemente individuate.

10.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi qualificanti della **formalizzata separazione di ruolo** nelle fasi chiave dei processi e della **tracciabilità degli atti**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Verifica delle attività sottostanti all’emissione di emissione di strumenti finanziari propri;

- Verifica del rispetto dei principi di legge e regolamentari, nazionali, comunitari e internazionali, ove applicabili, per le attività relative alle tenuta dei libri e delle scritture contabili da parte degli amministratori, anche il tramite degli addetti alla contabilità;

- Verifica del rispetto dei principi di legge e regolamentari nazionali, comunitari ed internazionali, ove applicabili, sulle richieste di esibizione di libri e scritture, e sulle le richieste di informazioni, di chiarimenti e di rendiconti.

Controllo sul comportamento degli amministratori, sindaci e i liquidatori, al fine di accertare la massima correttezza nella redazione delle comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico

10.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e ai Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi dei processi ed in particolare nelle seguenti attività:

- Attività relative alle tenuta delle scritture contabili da parte degli amministratori, anche per il tramite degli addetti alla contabilità;

- Controlli effettuati sulle attività sottostanti l’emissione di strumenti finanziari propri;

- Controlli sul comportamento degli amministratori, sindaci e i liquidatori, e sulle informazioni rese all’esterno della Società dagli stessi al fine di accertare la massima correttezza nella redazione delle comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico.

10.F) INFORMATIVA VERSO L’ORGANISMO DI VIGILANZA

Il Responsabile della Funzione Finanza e Bilancio deve comunicare, per quanto di competenza quanto segue:

a. informativa sulle attività sottostanti l’emissione di strumenti finanziari propri;

b. report sulle informazioni rese all’esterno sull’andamento della Società.

10.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;

- Protocollo Generale di Comportamento e nei Rapporti con la Pubblica Amministrazione.

PARTE SETTIMA – DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO

(art. 25 quater del Decreto)

Nel fare riferimento ai delitti con finalità di terrorismo o di eversione dell'ordine democratico, l'art. 25 quater del Decreto non elenca specificamente i reati per i quali è prevista la responsabilità dell'ente, limitandosi a richiamare, al primo comma, i delitti previsti dal codice penale e dalle leggi speciali ed, al terzo comma, i delitti diversi da quelli disciplinati al comma 1 ma posti in essere in violazione di quanto stabilito dall'art. 2 della Convenzione di New York.

Di seguito, sono elencate le aree di attività "a rischio" e le eventuali modalità attuative dei reati di cui all'articolo 25 quater del Decreto ritenuti rilevanti in rapporto alle attività di Venis.

Aree a rischio

A titolo meramente esemplificativo, sono da considerarsi a rischio le seguenti attività:

1) Acquisti di beni e servizi;

2) Rapporti finanziari con terzi (selezione di partner commerciali, mediante la procedure di cui al D. Lgs. n. 163/2006 e D.P.R. n. 207/2010 e s.m.i recanti "Codice degli Appalti pubblici" e "Regolamento di Attuazione")

3) Fornitura di servizio di accesso al pubblico ad Internet in modalità Wi-Fi;

4) Gestione di applicativi del Comune di Venezia o di portali web o di gestione degli spazi su portali pubblici e di pubblicazione di contenuti;

5) Gestione del Personale (selezione ed assunzione e gestione amministrativa).

1) "ATTIVITÀ RILEVANTI IN MATERIA DI TERRORISMO ED EVERSIONE"

1.A) DESCRIZIONE DEI PROCESSI

I processi si riferiscono:

- allo svolgimento delle attività di impresa ed alle relazioni finanziarie con partner commerciali;
- alle attività riguardanti il corretto adempimento degli obblighi legislativi e regolamentari finalizzati a promuovere le attività di prevenzione dei reati di cui all'art. 25 quater del Decreto.

1.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

I **delitti aventi finalità di terrorismo o di eversione dell'ordine democratico**, previsti dal codice penale e dalle leggi speciali; i delitti, diversi dai precedenti, che siano stati comunque posti in essere in **violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento al terrorismo**.

Quanto ai reati previsti in materia dalle disposizioni contenute nelle leggi speciali, si ricorda l'art. 1 della Legge 6 febbraio 1980, n. 15, che prevede, come circostanza aggravante applicabile a qualsiasi reato, il fatto che il reato stesso sia stato "commesso per **finalità** di terrorismo o di eversione dell'ordine democratico". Ne consegue che **qualsiasi delitto** previsto dal Codice Penale o dalle leggi speciali, anche diverso da quelli espressamente riguardanti il terrorismo, può diventare, purché commesso con dette finalità, uno di quelli suscettibili di costituire, a norma dell'art. 25 quater, presupposto per l'affermazione della responsabilità dell'Ente.

I reati di cui al terzo comma dell'art. 25 quater del Decreto, rientranti nell'ambito di applicazione della Convenzione di New York, sono invece quelli diretti a **fornire, direttamente o indirettamente, ma comunque volontariamente, fondi a favore di soggetti che intendano porre in essere reati di terrorismo**. In particolare, la Convenzione rinvia ai reati previsti da altre convenzioni internazionali, tra i quali: il **dirottamento di aeromobili**, gli **attentati contro personale diplomatico**, il **sequestro di ostaggi**, l'**illecita realizzazione di ordigni nucleari**, i **dirottamenti di navi**, l'**esplosione di ordigni**, etc.

La responsabilità amministrativa della Società potrebbe sorgere laddove gli amministratori, i direttori generali, i liquidatori, ovvero le persone sottoposte alla loro vigilanza rimangano coinvolti nella commissione dei reati precedente indicati; in particolare, se una unità organizzativa della Società venisse stabilmente utilizzata allo scopo unico o prevalente di consentire o agevolare la commissione dei predetti reati ovvero in caso di finanziamenti occulti aventi tali fini.

1.C) FUNZIONI INTERESSATE

Gli ambiti aziendali potenzialmente interessati dalle attività a rischio di commissione dei reati in parola sono stati individuati sulla base dell'Organigramma Venis allegato alla Parte Generale del Presente Modello.

Essi ricomprendono:

- l'Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza, Bilancio e Amministrazione del Personale
- la Funzione Acquisti, Gare e Contratti
- la Funzione Tecnologie, Servizi e Sviluppo
- la Funzione Comunicazione, Sviluppo Personale e Qualità

Sono altresì interessati tutti i dirigenti e dipendenti, nonché collaboratori e partner, pur non ricompresi nelle Funzioni sopra elencate, operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

1.D) SISTEMA DI CONTROLLO

Il sistema di controllo applicabile unitariamente per le diverse aree a rischio si basa essenzialmente sugli elementi della **separazione di ruolo** nelle fasi chiave del processo e della **tracciabilità delle fasi del processo**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- La segregazione delle responsabilità tra le aree/soggetti che svolgono le attività di:
    - autorizzazione,
    - esecuzione,
    - contabilizzazione,
    - controllo

  di una determinata operazione, in modo tale che nessuno possa gestire in autonomia un intero processo;

- deve essere effettuata la formalizzazione delle attività, evidenziando gli opportuni punti di controllo. Le operazioni aziendali devono essere regolate da una procedura definita e le attività estemporanee devono ottemperare almeno al principio della verificabilità;

- il sistema delle deleghe interne e delle procure ad agire verso l’esterno deve essere coerente con le responsabilità organizzative e gestionali assegnate e prevedere una puntuale indicazione delle soglie di approvazione delle spese;

- è escluso effettuare prestazioni in favore dei consulenti, dei partner e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere;

- garantire la tracciabilità: ogni operazione, transazione, pagamento e azione deve essere verificabile, documentata, coerente e congrua in modo tale che sia possibile in ogni momento l’effettuazione di controlli che attestino le caratteristiche e le motivazioni alla base delle scelte. Tutta la documentazione riguardante ogni singola attività dei processi sopra considerati deve esser periodicamente aggiornata ed adeguatamente archiviata e conservata;

- deve esistere un sistema di controllo di gestione in grado di segnalare l’insorgere di situazioni di criticità ed anomalie;

- deve essere predisposto ed organizzato un piano di formazione del personale in azienda e di comunicazione interna sui contenuti del Decreto e del Modello.

1.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo.

In particolare i principi procedurali che devono essere implementati per prevenire la fattispecie di reato considerate sono i seguenti:

- qualunque transazione finanziaria deve presupporre la conoscenza del beneficiario della relativa somma;
- nessun pagamento potrà essere effettuato in un paese terzo rispetto a quello delle parti contraenti o quello di esecuzione del contratto;
- qualunque pagamento effettuato su conti correnti di banche appartenenti od operanti in paesi elencati tra c.d. "paradisi fiscali", o in favore di società *off shore* è vietato;
- ogni tipo di immissione di qualsivoglia tipo di informative o *files* in sistemi remoti gestiti dalla Società per terzi deve essere inibito elettronicamente, e comunque non operabile in assenza di preventiva o parallela autorizzazione con sistemi di *strong authentication* dai responsabili delle Funzioni Sistemi e Servizi Tecnologici o Funzione Tecnologie, Servizi e Sviluppo;
- le operazioni la cui entità è definita significativa nell'ambito delle procedure vigenti devono essere concluse con persone fisiche e giuridiche verso le quali siano state preventivamente svolte idonee verifiche, controlli e accertamenti
- nel caso il cui nelle operazioni siano coinvolti soggetti a rischio, le operazioni dovranno essere sospese e sottoposte alla valutazione interna dell'Organo di Vigilanza;
- i dati raccolti relativamente ai rapporti con clienti, consulenti e partner devono essere completi e aggiornati, sia per la corretta e tempestiva individuazione dei medesimi, sia per una valida valutazione del loro profilo;
- nei contratti con i partner, fornitori e consulenti deve essere contenuta apposita dichiarazione dei medesimi di non aver mai subito condanne con sentenza passata in giudicato o provvedimenti equiparati in procedimenti giudiziari relativi ai reati ivi contemplati.

1.F) INFORMATIVA VERSO L'ORGANISMO DI VIGILANZA

Non sono previsti flussi informativi specifici ma l'accesso ai documenti deve essere sempre consentito all'Organismo di Vigilanza senza alcun obbligo di preavviso.

1.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Principi di Comportamento Generali e nei rapporti con la Pubblica Amministrazione.

PARTE OTTAVA – PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI

(art. 25 quater 1 del Decreto)

La Legge 9 gennaio 2006, n 5, sanziona penalmente la violazione del divieto di praticare attività di mutilazione degli organi genitali femminili e individua tali fattispecie come reati-presupposto della responsabilità amministrativa di società ed enti. L’estensione della responsabilità amministrativa delle società e degli enti alle ipotesi di commissione di tali reati risponde all’esigenza avvertita dal legislatore di scoraggiare, con tutti i mezzi possibili, lo svolgimento di pratiche vietate. Si ritiene, comunque, che data la peculiarità dei reati in questione, caratterizzati da particolari modalità di condotta e da finalità fortemente tipizzate culturalmente, il rischio di commissione degli stessi da parte di Venis sia del tutto inesistente.

PARTE NONA – DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE

(art. 25 quinquies del Decreto)

L'art. 5 della Legge 11 agosto 2003, n. 228, in tema di misure contro la tratta delle persone, ha inserito nel Decreto l'articolo 25 quinquies, che prevede l'applicazione di sanzioni amministrative alle persone giuridiche, società e associazioni per la commissione di delitti contro la personalità individuale. L'art. 25 quinquies è stato successivamente integrato ad opera dell'art. 10, Legge n. 38 del 6 febbraio 2006, contenente "*Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedo-pornografia anche a mezzo Internet*", che ha modificato l'ambito di applicazione dei delitti di pornografia minorile e detenzione di materiale pornografico (artt. 600 ter e 600 quater c.p.), includendo anche le ipotesi in cui tali illeciti siano commessi mediante l'utilizzo di materiale pornografico raffigurante immagini virtuali di minori degli anni diciotto o parti di esse (c.d. "pedo-pornografia virtuale", ai sensi del rinvio al nuovo art. 600 quater 1 c.p.). La citata Legge n. 38/2006 è intervenuta anche a modificare le disposizioni di cui agli artt. 600 bis, 600 ter e 600 quater c.p., relativi ai delitti di prostituzione minorile, pornografia minorile e detenzione di materiale pornografico, per i quali era già prevista la responsabilità amministrativa degli enti.

Occorre dare atto, per completezza, del fatto che la recente L. 1 ottobre 2012 n. 172 ha introdotto nel Codice Penale, al Libro Secondo, Titolo V, il nuovo articolo 414 bis, Rubricato "*Istigazione a pratiche di pedofilia e pedopornografia*". L'articolo prevede che, salvo che il fatto costituisca più grave reato, chiunque, con qualsiasi mezzo e con qualsiasi forma di espressione, pubblicamente istiga a commettere, in danno di minorenni, uno o più delitti previsti dagli art. li 600 *bis*, 600 *ter* e 600 *quater*, anche se relativi al materiale pornografico di cui all'art. 600 *quater.1*, 600 *quinques*, 609 *bis*, 609 *quater* e 609 *quinques* (pornografia virtuale) è punito con la reclusione da un anno e sei mesi a cinque anni. Alla stessa pena soggiace chi pubblicamente fa l'apologia di uno o più dei delitti previsti. L'ultimo comma dell'articolo precisa che non possono essere invocate, come scusanti, ragioni o finalità di carattere artistico, letterario, storico o di costume.

Con l'introduzione di questo articolo, il sistema penale interviene quindi per punire anche l'istigazione alla commissione di determinati reati, estendendo l'ambito della condotta penalmente rilevante in materia di pornografia minorile.

Sebbene sia opportuno tenere conto della novella legislativa nella politica aziendale di gestione delle risorse di rete, si segnala che l'introduzione del nuovo articolo non ha tuttavia incidenza diretta in materia di D. Lgs 231/2001, restando ad oggi inalterata la formulazione dell'art. 25 *quinquies* e con esso il novero dei delitti in essa richiamati.

In relazione ai reati sopra considerati, le aree ritenute più specificamente a rischio risultano essere le seguenti.

Aree a rischio

1) Selezione, assunzione e gestione amministrativa del personale;

2) Gestione di portali web con attività di gestione degli spazi sul portale e pubblicazione di contenuti;

3) Gestione dei sistemi informativi interni (attività di gestione degli accessi alle risorse di rete).

Inoltre, vengono in rilievo tutte le attività che la Società – che presta un "servizio della società dell'informazione" secondo quanto disposto dal Decreto legislativo 9 aprile 2003, n. 70 – è tenuta a porre in essere al fine di

prevenire la distribuzione, la divulgazione o la pubblicizzazione, con qualsiasi mezzo, anche per via telematica, di materiale pornografico attinente i minori.

1) "ATTIVITÀ RILEVANTI IN MATERIA DI TUTELA DELLA PERSONALITÀ INDIVIDUALE"

1.A) DESCRIZIONE DEI PROCESSI

I processi si riferiscono a tutte le attività d'impresa inerenti l'assunzione e la gestione del personale, nonché alle attività di gestione degli spazi sul portale, con attenzione alla pubblicazione dei contenuti e di gestione degli accessi alle risorse di rete.

Con particolare riferimento alle attività di prevenzione della distribuzione, della divulgazione o della pubblicizzazione, con qualsiasi mezzo, anche per via telematica, di materiale pornografico attinente ai minori, il processo si articola essenzialmente in due fasi:

- Nomina di un "Referente aziendale" incaricato di gestire rapporti e flussi informativi con la Polizia Postale e delle Comunicazioni (come tale, assume la qualifica di "Referente per la Polizia Postale');
- Segnalazione, in corso di accertamento di rischio di illecito, alla Polizia Postale.

1.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Il rischio di commissione di delitti contro la personalità individuale nell'ambito dello svolgimento delle attività aziendali della Società è fortemente ridotto, sia in ragione della tipologia di attività svolta dalla Società che in ragione della tipologia stessa dei reati, trattandosi di fattispecie criminose relativamente alle quali è difficile individuare la sussistenza di un interesse o di un vantaggio per l'ente.

Con particolare riferimento ai reati di: **Riduzione o mantenimento in schiavitù o in servitù** (art. 600 c.p.), **Tratta di persone** (art. 601 c.p.) e **Acquisto e alienazione di schiavi** (art. 602 c.p.), il rischio è **ASTRATTAMENTE SUSSISTENTE, SEPPURE IN MISURA MINIMA**, in quanto si tratta di reati che potrebbero essere commessi da soggetti terzi in rapporti con la Società, senza che quest'ultima ne sia consapevole. Al fine di evitare ogni coinvolgimento, Venis vigila ed adotta misure preventive, anche attraverso idonee previsioni contrattuali e/o direttive aziendali, affinché non vengano assunte condotte finalizzate alla commissione di questi ultimi reati, con particolare riferimento ai rapporti con collaboratori, mediatori ed altre controparti contrattuali della Società.

Con riferimento alle modalità attuative, si consideri che la **riduzione e il mantenimento in schiavitù** possono verificarsi laddove su una determinata persona vengano esercitati poteri corrispondenti a quelli del diritto di proprietà ovvero laddove una determinata persona venga ridotta in uno stato di soggezione continuativa, mediante la costrizione a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento. La riduzione o il mantenimento nello stato di schiavitù hanno luogo quando la condotta è attuata mediante violenza, minaccia, inganno, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha autorità sulla persona.

Quanto alla **tratta di persone**, le possibili modalità attuative del reato consistono nel costringere - mediante violenza, minaccia, inganno, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi - persone ridotte e/o mantenute in schiavitù a fare ingresso o a soggiornare o a uscire dal territorio dello Stato o a trasferirsi al suo interno.

Le condotte rilevanti consistono non solo nella realizzazione dei comportamenti sopra descritti, ma anche nello svolgimento di tutte le attività – prodromiche e non – di procacciamento di fondi e finanziamenti che consentano l'agevolazione, anche solo potenziale, delle attività riduzione o mantenimento in schiavitù, di acquisto e alienazione di schiavi, di tratta di persone. Si pensi al procacciamento illegale di forza lavoro, attraverso il traffico di migranti, alla creazione di fondi neri e/o alla corresponsione di retribuzioni a collaboratori, mediatori, fornitori ed altre controparti contrattuali della Società che, in ipotesi, commettano i suddetti reati a vantaggio della Società.

Con particolare riferimento ai reati di: **Prostituzione minorile** (art. 606 bis c.p.); **Detenzione di materiale pornografico** (art. 600 quater c.p.); **Pornografia individuale** (art. 600 quater 1 c.p.); **Iniziative turistiche volte allo sfruttamento della prostituzione** (art. 600 quinquies c.p.) il **RISCHIO È DA RITENERSI PRESSOCHÉ INESISTENTE**.

Oggetto di trattazione separata ed approfondita sarà invece il reato di **Pornografia minorile** (art. 600 ter c.p.), in considerazione dell'attività che Venis, che presta un "servizio della società dell'informazione", è tenuta a porre in essere al fine di prevenire la distribuzione, la divulgazione o la pubblicizzazione di materiale pornografico attinente i minori. In particolare, il reato maggiormente ipotizzabile è, in linea di principio, il **concorso nel reato di pornografia minorile** (art. 600 ter c.p.[12]) del Referente per la Polizia Postale.

Nel caso di specie, il concorso nel reato di pornografia minorile potrebbe ricorrere nell'ipotesi di omessa comunicazione alla Polizia Postale di accertamenti positivi – da parte del Referente aziendale per la Polizia Postale – di rischi di illecito di terzi collegati ad attività relative a materiale pornografico attinente ai minori, a seguito sia di segnalazione di clienti che di riscontro diretto a mezzo di tool/software in dotazione.

1.c) FUNZIONI INTERESSATE

Gli ambiti aziendali teoricamente interessati dalle attività a rischio di commissione dei reati in parola sono stati individuati sulla base dell'Organigramma Venis allegato alla Parte Generale del Presente Modello.

Essi ricomprendono:

- la Direzione Coordinamento Generale
- la Funzione Tecnologie, Servizi e Sviluppo
- la Funzione Comunicazione, Sviluppo Personale e Qualità

Sono altresì interessati tutti i dirigenti, dipendenti e collaboratori, pur non ricompresi nelle Funzioni sopra

[12] Si richiama, in particolare, il testo del 2° comma dell'art. 600 ter c.p.: "*Chiunque* […] *con qualsiasi mezzo, anche per via telematica, distribuisce, divulga o pubblicizza il materiale pornografico di cui al primo comma (materiale di pornografia minorile), ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto è punito con la reclusione da uno a cinque anni e con la multa da Euro 2.582 a Euro 51.645*"

elencate, operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

1.D) SISTEMA DI CONTROLLO

Con riferimento ai reati di riduzione o mantenimento in schiavitù o in servitù, alla tratta di persone e all'acquisto e alienazione di schiavi, il sistema di controllo si basa essenzialmente sull'adozione di specifiche misure preventive quali l'introduzione di idonee **previsioni contrattuali** e/o **direttive aziendali** nei rapporti con collaboratori, mediatori ed altre controparti contrattuali della Società.

Con riferimento al concorso nel reato di pornografia minorile di cui all'art. 600 ter c.p., invece, il sistema di controllo si basa fondamentalmente sulla **tracciabilità delle attività di verifica e controllo** di competenza del presidio aziendale, volto a supportare la Polizia Postale e delle Comunicazioni, nonché l'Autorità Giudiziaria, nella prevenzione e repressione del reato di pornografia minorile.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati:

- Adozione di adeguati meccanismi di riscontro del Referente al segnalante circa la ricezione della segnalazione;
- Adozione di adeguati meccanismi di riscontro da parte della Polizia Postale circa la ricezione dell'informativa aziendale (es. firma digitale);
- Archiviazione degli atti e documenti aziendali ufficiali diretti e ricevuti dalla Polizia Postale e delle Comunicazioni e dall'Autorità Giudiziaria;
- Ricorso a puntuali iniziative formative specialistiche dirette al personale prescelto per l'attività di Referente aziendale per la Polizia Postale;
- Presenza di direttive aziendali sulle modalità di condotta operativa da adottare nei rapporti intercorrenti con la Polizia Postale e delle Comunicazioni, con l'Autorità Giudiziaria e con altri soggetti pubblici;
- Tracciabilità delle attività, degli atti e delle fonti informative/segnalazioni/comunicazioni nelle singole fasi del processo.

1.E) PROTOCOLLO COMPORTAMENTALE

Non porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che – considerati individualmente o collettivamente – integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle contemplate dall'art. 25 quinques del Decreto.

Non adottare comportamenti a rischio di concorso nel reato di pornografia minorile o comunque contrari al Presente Modello, al Codice Etico ed al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione in tutte le fasi del processo ed in particolare nelle seguenti attività:

- in sede di gestione delle attività di competenza del Referente per la Polizia Postale, laddove vengano adottate condotte omissive e/o comunque contrarie ai doveri d'ufficio nelle fasi di accertamento di

segnalazioni da parte di clienti in tema di pubblicazione di materiale pornografico attinente ai minori o di pubblicità riguardante tale materiale;

- in sede di gestione delle attività di competenza del Referente per la Polizia Postale, laddove vengano adottate condotte omissive e/o comunque contrarie ai doveri d’ufficio nella fase di diretto riscontro, a mezzo tool/software in dotazione, di pubblicazione di materiale pornografico attinente ai minori o di pubblicità riguardante tale materiale attività;

- in sede di attività di competenza del Referente per la Polizia Postale, laddove vengano adottate condotte omissive e/o comunque contrarie ai doveri d’ufficio nella fase di trasmissione di comunicazioni/informative alla Polizia Postale;

- in sede di ispezioni/accertamenti da parte della Polizia Postale e delle Comunicazioni, laddove vengano adottate dal Referente per la Polizia Postale condotte finalizzate ad influenzare, nell’interesse della Società, il giudizio/parere dei rappresentanti pubblici intervenuti.

1.F) FLUSSI INFORMATIVI VERSO L’ORGANISMO DI VIGILANZA

Il Referente per la Polizia Postale deve comunicare:

Flusso 1: l’elenco delle comunicazioni/informative trasmesse alla Polizia Postale e delle Comunicazioni (pornografia minorile);

Il Referente deve inoltre informare l’Organismo di Vigilanza sulle misure adottate dalla Società a seguito di eventuali provvedimenti dell’Autorità Giudiziaria.

1.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;

- Principi di Comportamento Generali e nei rapporti con la Pubblica Amministrazione.

PARTE DECIMA – ABUSI DI MERCATO

(art. 25 sexies del Decreto)

Nel fare riferimento agli abusi di mercato, l'art. 25 sexies del Decreto rinvia ai reati di abuso di informazioni privilegiate e di manipolazione del mercato previsti dalla parte V, titolo I bis, capo II, del Testo Unico Finanza (anche "T.U.F.", di cui al Decreto Legislativo 24 febbraio 1998, n. 58).

1) "ABUSO DI INFORMAZIONI PRIVILEGIATE"

E' necessario distinguere tra il **reato di abuso di informazioni privilegiate** (art. 184 T.U.F.) e l'**illecito amministrativo di abuso di informazioni privilegiate** (art. 187 bis T.U.F.)

Il **reato** di abuso di informazioni privilegiate può verificarsi laddove un esponente della Società, sia esso un soggetto apicale o un suo sottoposto, essendo in possesso di informazioni privilegiate (in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo emittente Strumenti Finanziari, della partecipazione al capitale dell'emittente stesso, ovvero, dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio):

- acquista, venda o compia altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, sugli Strumenti Finanziari utilizzando le informazioni medesime;
- comunichi tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;
- raccomandi o induca altri, sulla base di esse, al compimento di taluna delle operazioni indicate nel precedente primo punto.

Analogamente, è punito chiunque, essendo in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose, compia taluna delle azioni di cui ai precedenti tre punti.

Ai fini delle predette disposizioni, per "*informazione privilegiata*" si deve intendere "*un'informazione di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari*".

Fatte salve le sanzioni penali quando il fatto costituisce reato, l'**illecito amministrativo** di di abuso di informazioni privilegiate si configura in presenza della medesima condotta prevista dall'art. 184 T.U.F. nonché quando le condotte suddette siano poste in essere con colpa, ovverosia, per negligenza, imprudenza o imperizia ovvero per inosservanza di leggi, regolamenti, ordini o discipline e, in particolare, quando conoscendo o potendo conoscere in base all'ordinaria diligenza il carattere privilegiato delle informazioni di cui si è entrati in possesso, si compia taluno dei fatti di cui ai tre punti riportati precedentemente.

Anche la commissione del predetto illecito amministrativo costituisce presupposto per l'eventuale responsabilità amministrativa della Società ai sensi del Decreto, in applicazione degli articoli 187 bis e ss. T.U.F. e dei principi generali del medesimo Decreto.

Se la fattispecie di illecito presupposto assume rilevanza penale, l'eventuale responsabilità dell'ente sarà accertata

in sede giudiziaria; se invece il fatto costituisce illecito amministrativo – posto in essere comunque nell'interesse o a vantaggio dell'Ente – l'accertamento dell'illecito e l'applicazione delle relative sanzioni è riservato alla CONSOB. Al riguardo, il T.U.F. chiarisce i rapporti tra i procedimenti amministrativo e penale. In particolare, con riferimento ai profili di accertamento delle responsabilità dei soggetti coinvolti, l'art. 187 duodecies stabilisce che: "*Il procedimento amministrativo di accertamento e il procedimento di opposizione di cui all'art. 187-septies non possono essere sospesi per la pendenza del procedimento penale avente ad oggetto i medesimi fatti o fatti dal cui accertamento dipende la relativa definizione*". Pertanto, per i medesimi fatti potrebbero essere contestualmente promossi un procedimento penale dinanzi al giudice ordinario ed un procedimento amministrativo presso la CONSOB, con conseguente eventuale accertamento della responsabilità amministrativa della Società ai sensi del Decreto per la medesima fattispecie, sia in sede giudiziaria che amministrativa.

Si precisa, infine, che, ai fini delle disposizioni relative al reato ed all'illecito amministrativo in esame, per "Strumenti Finanziari" si devono intendere anche "*gli strumenti finanziari di cui all'articolo 1, comma 2, del predetto decreto, il cui valore dipenda da uno Strumento Finanziario*".

Nelle Linee Guida di Confindustria e nel documento del CESR del luglio 2007 ("*Market Abuse Directive. Level 3 – Second Set of CESR Guidance and Information on the Common Operation of the Directive to the Market*" – CESR/06-562b, section 1.15) sono, infine, indicati, a titolo esemplificativo, alcuni eventi ed informazioni che possono assumere rilievo, ove relativi agli Strumenti Finanziari o all'emittente gli Strumenti Finanziari, ai fini della configurazione del reato e dell'illecito amministrativo sopra illustrati. Tra questi, in particolare: andamento del business operativo; cambiamenti nel controllo e/o nei patti di controllo; variazioni nel management; operazioni che coinvolgono il capitale o emissione di strumenti di debito o di strumenti che danno diritto a comprare o sottoscrivere titoli; decisioni in merito alla variazione del capitale sociale; fusioni e scissioni; acquisti o disposizioni su azioni, attività o rami di azienda; ristrutturazioni e/o riorganizzazioni aziendali che hanno un effetto sulle attività, sulle passività, sulla posizione finanziaria o sul conto economico; revoca o cancellazione delle linee di credito da parte del sistema bancario; contenzioso legale e/o risoluzione di contratti di particolare rilevanza; insolvenza da parte di debitori rilevanti; danni ambientali; cambiamenti nei profitti e/o nelle perdite attese; informazioni sui dividendi (data del pagamento, data dello stacco, cambiamenti nella politica dei dividendi).

Il reato e l'illecito amministrativo di "*abuso di informazioni privilegiate*" sono puniti secondo la legge italiana anche se commessi all'estero, qualora attengano a strumenti finanziari ammessi o per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano.

Concludendo e per quanto di nostro interesse, si osserva che l'attuazione del reato e dell'illecito amministrativo di abuso di informazioni privilegiate è normalmente ipotizzabile in capo ad un emittente i richiamati "Strumenti Finanziari" ovvero alla società che controlla o detiene una partecipazione rilevante in un siffatto emittente. E' ipotizzabile, inoltre, in quelle società che, per finalità di gestione della tesoreria, operano molto attivamente sui mercati regolamentati per il tramite di intermediari autorizzati. Le descritte condotte illecite possono, infine, essere ipotizzate e potrebbero astrattamente essere occasionate dalla circostanza che tra la Società e l'emittente gli Strumenti Finanziari intercorrono rapporti di partecipazione azionaria ovvero di *partnership* – anche tramite *joint ventures*, società di progetto o consorzi – in operazioni di investimento o per la realizzazione di appalti o altri lavori.

- Gli ambiti aziendali maggiormente interessati da questo genere di reati possono essere in generale l'Assemblea, il l'Organo Amministrativo; il Collegio Sindacale, le Funzioni Finanza e Bilancio, nonché Affari legali e societari quando presenti.

NEL CASO DI VENIS, TENUTO CONTO DEGLI STRUMENTI FINANZIARI DALLA STESSA ATTUALMENTE

EMESSI, ED OPERAZIONI DI INVESTIMENTO ATTUALMENTE IN ESSERE, IL RISCHIO DI COMMISSIONE DEL REATO E DELL'ILLECITO AMMINISTRATIVO IN ESAME È DA CONSIDERARSI POCO SIGNIFICATIVO.

2) "MANIPOLAZIONE DEL MERCATO"

Anche in questo caso è necessario distinguere tra il **reato di manipolazione del mercato** (art. 185 T.U.F.) e l'**illecito amministrativo di manipolazione del mercato** (art. 187 ter T.U.F.).

Il **reato** di manipolazione del mercato si verifica nel caso di diffusione di notizie false o nel caso di effettuazione di operazioni simulate o altri artifici, che siano concretamente idonei a provocare una sensibile alterazione del prezzo degli strumenti finanziari, emessi da terzi, di cui all'art. 1, comma 2, T.U.F., ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di altro Paese dell'UE (di seguito, anche "Strumenti Finanziari").

Si tratta di un reato di pericolo: non è richiesto, dunque, ai fini del perfezionamento della fattispecie, che gli eventi sopra menzionati si verifichino, essendo sufficiente la diffusione delle notizie o, in alternativa, il compimento delle operazioni simulate o degli artifici inerenti gli "Strumenti Finanziari". Il pericolo va, però, valutato in concreto. Nel caso in esame, affinché il reato si verifichi, occorre che sia posto in essere dagli amministratori, dai direttori generali, dai liquidatori o da persone sottoposte alla loro vigilanza.

Fatte salve le sanzioni penali quando il fatto costituisce reato, l'illecito amministrativo manipolazione del mercato si configura nel caso:

- di diffusione di informazioni, notizie o voci false o fuorvianti che forniscano o siano suscettibili di fornire indicazioni false o fuorvianti in merito agli Strumenti Finanziari;
- operazioni od ordini di compravendita che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di Strumenti Finanziari;
- operazioni od ordini di compravendita che consentano, tramite l'azione di una o di più persone che agiscono di concerto, di fissare il prezzo di mercato di uno o più Strumenti Finanziari ad un livello anomalo o artificiale;
- operazioni od ordini di compravendita che utilizzino artifizi od ogni altro tipo di inganno o di espediente;
- altri artifizi idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di Strumenti Finanziari.

Le suddette condotte rilevano anche se poste in essere con colpa, ovverosia, per negligenza, imprudenza o imperizia ovvero per inosservanza di leggi, regolamenti, ordini o discipline.

Anche la commissione del predetto illecito amministrativo costituisce presupposto per l'eventuale responsabilità amministrativa della Società ai sensi del Decreto, in applicazione degli artt. 187-bis e ss. T.U.F. e dei principi generali del medesimo Decreto.

Se la fattispecie di illecito presupposto assume rilevanza penale, l'eventuale responsabilità dell'ente sarà accertata

in sede giudiziaria; se invece il fatto costituisce illecito amministrativo – posto in essere comunque nell'interesse o a vantaggio dell'ente – l'accertamento dell'illecito e l'applicazione delle relative sanzioni è riservato alla CONSOB. Al riguardo, il T.U.F. chiarisce i rapporti tra i procedimenti amministrativo e penale. In particolare, con riferimento ai profili di accertamento delle responsabilità dei soggetti coinvolti, l'art. 187 duodecies stabilisce che: "*Il procedimento amministrativo di accertamento e il procedimento di opposizione di cui all'art. 187-septies non possono essere sospesi per la pendenza del procedimento penale avente ad oggetto i medesimi fatti o fatti dal cui accertamento dipende la relativa definizione*". Pertanto, per i medesimi fatti potrebbero essere contestualmente promossi un procedimento penale dinanzi al giudice ordinario ed un procedimento amministrativo presso la CONSOB, con conseguente eventuale accertamento della responsabilità amministrativa della Società ai sensi del Decreto per la medesima fattispecie, sia in sede giudiziaria che amministrativa.

Le modalità attuative del reato e dell'illecito amministrativo di manipolazione del mercato astrattamente configurabili, per quanto concretamente di difficile verificazione all'interno di Venis, possono essere ricondotte:

- nella categoria delle operazioni o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo degli Strumenti Finanziari, con ciò riferendosi alle operazioni false o fuorvianti (in particolare, quelle fittizie o da non eseguirsi), alle operazioni che fissano i prezzi a livelli anomali o artificiali (ad esempio, effettuando operazioni volte a costituire una soglia minima al corso dei prezzi di uno Strumento Finanziario) ed alle operazioni che utilizzano artifizi, inganni o espedienti (ad esempio, al fine di apparire sul mercato come il soggetto che detiene una partecipazione in un emittente Strumenti Finanziari, celando al pubblico l'identità del vero proprietario), così come più ampiamente precisato nell'art. 43 del Regolamento CONSOB n. 16191 del 29 ottobre 2007, nella Comunicazione Consob n. DME/5078692 del 29 novembre 2005 che, a sua volta, si rifà al documento del CESR del luglio 2007 "*Market Abuse Directive. Level 3 – First set of CESR guidance and information on the common operation of the directive*" – e nelle Linee Guida di Confindustria;

- nelle ipotesi di diffusione di notizie false o fuorvianti che siano concretamente idonee a provocare una sensibile alterazione del prezzo degli Strumenti Finanziari, senza effettuare necessariamente operazioni su tali Strumenti Finanziari, quali, in particolare, la diffusione, tramite Internet o comunicati stampa, di informazioni false o fuorvianti in merito (a) a Strumenti Finanziari di un emittente ovvero (b) all'emittente degli Strumenti Finanziari (relativamente, ad esempio, ad acquisizioni, dismissioni, operazioni sul capitale, redazione dei bilanci e dei documenti che rappresentano l'andamento economico, patrimoniale e finanziario dell'emittente) ovvero ancora (c) alla possibile acquisizione o dismissione di quest'ultimo, occasionate, ad esempio, dalla circostanza che tra la Società e l'emittente stesso intercorrono rapporti di partecipazione azionaria ovvero di *partnership* – anche tramite *joint ventures*, società di progetto o consorzi – in operazioni di investimento o per la realizzazione di appalti o altri lavori; anche in tal caso, si richiamano le ulteriori possibili modalità attuative del reato in esame indicate nell'art. 43 del Regolamento CONSOB n. 16191 del 29 ottobre 2007, nella Comunicazione Consob n. DME/5078692 del 29 novembre 2005 – che, a sua volta, si rifà al documento del CESR del luglio 2007 "*Market Abuse Directive. Level 3 – First set of CESR guidance and information on the common operation of the directive*" – e nelle Linee Guida di Confindustria.

Il reato e l'illecito amministrativo di "manipolazione del mercato" sono puniti secondo la legge italiana anche se commessi all'estero, qualora attengano a strumenti finanziari ammessi o per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano.

Si precisa, infine, per quanto di nostro interesse e con riferimento all'attività di Venis, che l'attuazione del reato e dell'illecito amministrativo in esame è normalmente ipotizzabile in capo ad un emittente i richiamati "Strumenti Finanziari" ovvero alla società che controlla o detiene una partecipazione rilevante in un siffatto emittente. E'

ipotizzabile, inoltre, in quelle società che, per finalità di gestione della tesoreria, operano molto attivamente sui mercati regolamentati per il tramite di intermediari autorizzati. Le descritte condotte illecite possono, infine, essere ipotizzate e potrebbero astrattamente essere occasionate dalla circostanza che tra la Società e l’emittente gli Strumenti Finanziari intercorrono rapporti di partecipazione azionaria ovvero di *partnership* – anche tramite *joint ventures*, società di progetto o consorzi – in operazioni di investimento o per la realizzazione di appalti o altri lavori.

- Gli ambiti aziendali maggiormente interessati da questo genere di reati possono essere in generale l’Assemblea, il l’Organo Amministrativo, il Collegio Sindacale, le Funzioni Finanza e Bilancio, nonché Affari legali e societari quando presenti.

NEL CASO DI VENIS, TENUTO CONTO DEGLI STRUMENTI FINANZIARI DALLA STESSA ATTUALMENTE EMESSI, ED OPERAZIONI DI INVESTIMENTO ATTUALMENTE IN ESSERE, IL RISCHIO DI COMMISSIONE DEL REATO E DELL’ILLECITO AMMINISTRATIVO IN ESAME È DA CONSIDERARSI POCO SIGNIFICATIVO.

PARTE UNDICESIMA – OMICIDIO COLPOSO O LESIONI GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

(art. 25 septies del Decreto)

La Legge 3 agosto 2007, n. 123 (Legge Delega per il testo unico in materia di salute e sicurezza sui luoghi di lavoro) ed il successivo Decreto Legislativo attuativo dell'art. 1 (Decreto Legislativo 9 aprile 2008, n. 81), hanno inserito nel Decreto l'art. 25 septies, estendendo la responsabilità dell'ente ai reati di omicidio colposo e lesioni colpose gravi e gravissime commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro.

Si precisa che l'elemento essenziale ed unificante delle varie forme di responsabilità del datore di lavoro ai fini dell'applicabilità dell'art. 25 septies del Decreto è rappresentato dalla mancata adozione di tutte le misure di sicurezza e prevenzione tecnicamente possibili e concretamente attuabili alla luce dell'esperienza e delle più avanzate conoscenze tecnico – scientifiche.

E' il Decreto Legislativo 9 aprile 2008, n. 81 (di seguito, il "TU Sicurezza"), ad indicare, all'art. 15, quali sono le misure generali di tutela della salute e della sicurezza dei lavoratori nei luoghi di lavoro:

a) "*la valutazione di tutti i rischi per la salute e sicurezza;*

b) *la programmazione della prevenzione, mirata ad un complesso che integri in modo coerente nella prevenzione le condizioni tecniche produttive dell'azienda nonché l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro;*

c) *l'eliminazione dei rischi e, ove ciò non sia possibile, la loro riduzione al minimo in relazione alle conoscenze acquisite in base al progresso tecnico;*

d) *il rispetto dei principi ergonomici nell'organizzazione del lavoro, nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro e produzione, in particolare al fine di ridurre gli effetti sulla salute del lavoro monotono e di quello ripetitivo;*

e) *la riduzione dei rischi alla fonte;*

f) *la sostituzione di ciò che è pericoloso con ciò che non lo è, o è meno pericoloso;*

g) *la limitazione al minimo del numero dei lavoratori che sono, o che possono essere, esposti al rischio;*

h) *l'utilizzo limitato degli agenti chimici, fisici e biologici sui luoghi di lavoro;*

i) *la priorità delle misure di protezione collettiva rispetto alle misure di protezione individuale;*

j) *il controllo sanitario dei lavoratori;*

k) *l'allontanamento del lavoratore dall'esposizione al rischio per motivi sanitari inerenti la sua persona e l'adibizione, ove possibile, ad altra mansione;*

l) *l'informazione e formazione adeguate per i lavoratori;*

m) *l'informazione e formazione adeguate per dirigenti e i preposti;*

n) *l'informazione e formazione adeguate per i rappresentanti dei lavoratori per la sicurezza;*

o) *le istruzioni adeguate ai lavoratori;*

p) *la partecipazione e consultazione dei lavoratori;*

q) *la partecipazione e consultazione dei rappresentanti dei lavoratori per la sicurezza;*

r) *la programmazione delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, anche attraverso l'adozione di codici di condotta e di buone prassi;*

s) *le misure di emergenza da attuare in caso di primo soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato;*

t) *l'uso di segnali di avvertimento e di sicurezza;*

u) *la regolare manutenzione di ambienti, attrezzature, impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alla indicazione dei fabbricanti*".

Lo stesso TU Sicurezza ha stabilito un contenuto minimo essenziale del Modello in materia di sicurezza sul lavoro. Infatti, l'articolo 30 rubricato "Modelli di organizzazione e di gestione" dispone che "*Il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al decreto legislativo 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:*

v) *al rispetto degli standard tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;*

w) *alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;*

x) *alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;*

y) *alle attività di sorveglianza sanitaria;*

z) *alle attività di informazione e formazione dei lavoratori;*

aa) *alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;*

bb) *alla acquisizione di documentazioni e certificazioni obbligatorie di legge;*

cc) *alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.*

Il modello organizzativo e gestionale di cui al comma 1 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1.

Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo

devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico".

Venis, al fine di garantire l'adozione di un valido presidio idoneo a prevenire l'insorgenza di reati di cui al citato art. 25 septies del Decreto, ha individuato le aree a rischio ed adottato specifiche procedure e flussi informativi, anche tenendo conto delle indicazioni fornite dai Ministeri competenti e dalle Linee Guida Uni-Inail oltre che delle norme cogenti.

Aree a rischio

In relazione ai reati ed alle condotte criminose previste dall'art. 25 *septies* del Decreto, l'individuazione delle aree a rischio è stata effettuata sulla base della considerazione che, a differenza degli altri reati presupposto di cui al Decreto, ciò che rileva in tale ambito è la mera inosservanza di norme poste a tutela della salute e sicurezza dei lavoratori da cui deriva l'evento dannoso (morte o lesioni colpose) e non l'elemento psicologico del dolo.
Pertanto, tutte le Aree aziendali sono da considerarsi a rischio, così come tutte le attività aziendali svolte:

- presso la sede centrale;
- presso le unità produttive o cantieri, stabili od occasionali, anche decentrate.

1) "ATTIVITÀ RILEVANTI IN MATERIA DI TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO"

1.A) LE ATTIVITA' SENSIBILI

Con riguardo all'inosservanza delle norme poste a tutela della salute e sicurezza dei lavoratori, da cui possa derivare l'evento dannoso nelle aree a rischio, si ritengono particolarmente sensibili le seguenti attività:

a) Determinazione delle politiche di salute e sicurezza sul lavoro volte a definire gli impegni generali assunti dalla Società per la prevenzione dei rischi ed il miglioramento progressivo della salute e della sicurezza[13].

[13] La politica per la salute e la sicurezza sul lavoro ("SSL") dovrebbe essere definita e documentata dal vertice aziendale nell'ambito della politica generale dell'azienda. La politica indica la visione, i valori essenziali e le convinzioni dell'azienda sul tema della SSL e serve a definire la direzione, i principi d'azione e i risultati a cui tendere ed esprime l'impegno del vertice aziendale nel promuovere nel personale la conoscenza degli obiettivi, la consapevolezza dei risultati a cui tendere, l'accettazione delle responsabilità e le motivazioni. La politica aiuta a dimostrare verso l'interno:

- l'impegno dell'azienda alla tutela della salute e sicurezza dei lavoratori;

e, verso l'esterno, che:

- esiste un impegno concreto dell'azienda in tema di salute e sicurezza sul lavoro;
  - si privilegiano le azioni preventive;
  - l'organizzazione aziendale tende all'obiettivo del miglioramento continuo.

[15] Ai sensi dell'art. 29 del TU Sicurezza il documento di valutazione dei rischi, redatto in collaborazione con il responsabile del servizio di prevenzione e protezione ed il medico competente, può essere tenuto, nel rispetto delle previsioni di cui all' articolo 53, su supporto informatico e deve essere munito anche tramite le procedure applicabili ai supporti informatici di cui all' articolo 53, di data certa o attestata dalla sottoscrizione del documento medesimo da parte del datore di lavoro nonché, ai soli fini della prova della data, dalla sottoscrizione del responsabile del servizio di prevenzione e protezione, del rappresentante dei lavoratori per la sicurezza o del rappresentante dei lavoratori per la sicurezza territoriale e del medico competente, ove nominato. – Si evidenzia inoltre che la valutazione dei rischi, anche nella scelta delle attrezzature di lavoro e delle sostanze o dei preparati chimici impiegati, nonché nella sistemazione dei luoghi di lavoro, deve riguardare tutti i rischi per la sicurezza e la salute dei lavoratori, ivi compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari, tra cui anche quelli collegati allo stress lavoro-correlato, secondo i contenuti dell'accordo europeo dell'8 ottobre 2004, e quelli riguardanti le lavoratrici in stato di gravidanza, secondo quanto previsto dal decreto legislativo 26 marzo 2001, n. 151, nonché quelli connessi alle differenze di genere, all'età, alla provenienza da altri Paesi e quelli connessi alla specifica tipologia contrattuale attraverso cui viene resa la prestazione di lavoro. La valutazione dello stress lavoro-correlato di cui sopra è effettuata nel rispetto delle indicazioni fornite dalla Commissione consultiva permanente per la salute

Eliminato: ¶

b) Identificazione e corretta applicazione delle prescrizioni delle leggi e dei regolamenti applicabili in tema di sicurezza sul lavoro.

c) Identificazione e valutazione dei rischi per tutte le categorie di lavoratori, con particolare riferimento a:

- stesura del Documento di Valutazione dei Rischi[14];
- contratti di prestazione d'opera o affidamento di servizi a lavoratori autonomi all'interno dell'azienda[15];

---

e sicurezza sul lavoro, ed il relativo obbligo decorre dalla elaborazione delle predette indicazioni e comunque, anche in difetto di tale elaborazione, a far data dal **1° agosto 2010**.

[15] E' utile richiamare l'art. 26 del TU Sicurezza rubricato "Obblighi connessi ai contratti d'appalto o d'opera o di somministrazione"il quale sancisce che:

"*1. Il datore di lavoro, in caso di affidamento di lavori, servizi e forniture all'impresa appaltatrice o a lavoratori autonomi all'interno della propria azienda, o di una singola unità produttiva della stessa, nonché nell'ambito dell'intero ciclo produttivo dell'azienda medesima, sempre che abbia la disponibilità giuridica dei luoghi in cui si svolge l'appalto o la prestazione di lavoro autonomo:*

a) verifica, con le modalità previste dal decreto di cui all'articolo 6, comma 8, lettera g), l'idoneità tecnico-professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori, ai servizi e alle forniture da affidare in appalto o mediante contratto d'opera o di somministrazione. Fino alla data di entrata in vigore del decreto di cui al periodo che precede, la verifica è eseguita attraverso le seguenti modalità:

1. acquisizione del certificato di iscrizione alla camera di commercio, industria e artigianato;

2. acquisizione dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei requisiti di idoneità tecnico-professionale, ai sensi dell'articolo 47 del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445;

3. fornisce agli stessi soggetti dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla propria attività.

2. Nell'ipotesi di cui al comma 1, i datori di lavoro, ivi compresi i subappaltatori:

a) cooperano all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;

b) coordinano gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, informandosi reciprocamente anche al fine di eliminare rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva.

3. Il datore di lavoro committente promuove la cooperazione ed il coordinamento di cui al comma 2, elaborando un unico documento di valutazione dei rischi che indichi le misure adottate per eliminare o, ove ciò non è possibile, ridurre al minimo i rischi da interferenze. Tale documento è allegato al contratto di appalto o di opera e va adeguato in funzione dell'evoluzione dei lavori, servizi e forniture. Ai contratti stipulati anteriormente al 25 agosto 2007 ed ancora in corso alla data del 31 dicembre 2008, il documento di cui al precedente periodo deve essere allegato entro tale ultima data. Le disposizioni del presente comma non si applicano ai rischi specifici propri dell'attività delle imprese appaltatrici o dei singoli lavoratori autonomi. Nel campo di applicazione del decreto legislativo 12 aprile 2006, n. 163, e successive modificazioni, tale documento è redatto, ai fini dell'affidamento del contratto, dal soggetto titolare del potere decisionale e di spesa relativo alla gestione dello specifico appalto.

3-bis. Ferme restando le disposizioni di cui ai commi 1 e 2, l'obbligo di cui al comma 3 non si applica ai servizi di natura intellettuale, alle mere forniture di materiali o attrezzature nonché ai lavori o servizi la cui durata non sia superiore ai due giorni, sempre che essi non comportino rischi derivanti dalla presenza di agenti cancerogeni, biologici, atmosfere esplosive o dalla presenza dei rischi particolari di cui all'allegato XI.

3-ter. Nei casi in cui il contratto sia affidato dai soggetti di cui all' articolo 3, comma 34, del decreto legislativo 12 aprile 2006, n. 163, o in tutti i casi in cui il datore di lavoro non coincide con il committente, il soggetto che affida il contratto redige il documento di valutazione dei rischi da interferenze recante una valutazione ricognitiva dei rischi standard relativi alla tipologia della prestazione che potrebbero potenzialmente derivare dall'esecuzione del contratto. Il soggetto presso il quale deve essere eseguito il contratto, prima dell'inizio dell'esecuzione, integra il predetto documento riferendolo ai rischi specifici da interferenza presenti nei luoghi in cui verrà espletato l'appalto; l'integrazione, sottoscritta per accettazione dall'esecutore, integra gli atti contrattuali.

4. Ferme restando le disposizioni di legge vigenti in materia di responsabilità solidale per il mancato pagamento delle retribuzioni e dei contributi previdenziali e assicurativi, l'imprenditore committente risponde in solido con l'appaltatore, nonché con ciascuno degli eventuali subappaltatori, per tutti i danni per i quali il lavoratore, dipendente dall'appaltatore o dal subappaltatore, non risulti indennizzato ad opera dell'Istituto nazionale per l'assicurazione contro gli infortuni sul lavoro (INAIL) o dell'Istituto di previdenza per il settore marittimo (IPSEMA). Le disposizioni del presente comma non si applicano ai danni conseguenza dei rischi specifici propri dell'attività delle imprese appaltatrici o subappaltatrici.

5. Nei singoli contratti di subappalto, di appalto e di somministrazione, anche qualora in essere al momento della data di entrata in vigore del presente decreto, di cui agli articoli 1559, ad esclusione dei contratti di somministrazione di beni e servizi essenziali, 1655, 1656 e 1677 del codice civile, devono essere specificamente indicati a pena di nullità ai sensi dell'articolo 1418 del codice civile i costi delle misure adottate per eliminare o, ove ciò non sia possibile, ridurre al minimo i rischi in materia di salute e sicurezza sul lavoro derivanti dalle interferenze delle lavorazioni. I costi di cui al primo periodo non sono soggetti a ribasso..A tali dati possono accedere, su richiesta, il rappresentante dei lavoratori per la sicurezza e gli organismi locali delle organizzazioni sindacali dei lavoratori comparativamente più rappresentative a livello nazionale.

6. Nella predisposizione delle gare di appalto e nella valutazione dell'anomalia delle offerte nelle procedure di affidamento di appalti di lavori pubblici, di servizi e di forniture, gli enti aggiudicatori sono tenuti a valutare che il valore economico sia adeguato e sufficiente rispetto al costo del lavoro e al costo relativo alla sicurezza, il quale deve essere specificamente indicato e risultare congruo rispetto all'entità e alle caratteristiche dei lavori, dei servizi o delle forniture. Ai fini del presente comma il costo del lavoro è determinato periodicamente, in apposite tabelle, dal Ministro del lavoro, della salute e delle politiche sociali, sulla base dei valori economici previsti dalla contrattazione collettiva stipulata dai sindacati comparativamente più rappresentativi, delle norme in materia previdenziale ed assistenziale, dei diversi settori merceologici e delle differenti aree territoriali. In mancanza di contratto collettivo applicabile, il costo del lavoro è determinato in relazione al contratto collettivo del settore merceologico più vicino a quello preso in considerazione.

7. Per quanto non diversamente disposto dal decreto legislativo 12 aprile 2006, n. 163, come da ultimo modificate dall'articolo 8, comma 1, della legge 3 agosto 2007, n. 123, trovano applicazione in materia di appalti pubblici le disposizioni del presente decreto.

8. Nell'ambito dello svolgimento di attività in regime di appalto o subappalto, il personale occupato dall'impresa appaltatrice o subappaltatrice deve essere munito di apposita tessera di riconoscimento corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro".

- valutazione dei rischi interferenziali;
- Piani di Sicurezza e Coordinamento e Piani Operativi di Sicurezza.

d) Fissazione di obiettivi allineati con gli impegni generali definiti nelle politiche di cui alla lettera a) che precede ed elaborazione di programmi per il raggiungimento di tali obiettivi con relativa definizione di priorità, tempi ed attribuzioni delle rispettive responsabilità – con assegnazione delle relative risorse – in materia di salute e sicurezza sul lavoro, con particolare riferimento a:

- Attribuzione di compiti e doveri[16];
- Attività del Servizio Prevenzione e Protezione, del Medico Competente e del Medico Referente;
- Attività di tutti gli altri soggetti su cui ricade la responsabilità dell'attuazione delle misure per la salute e sicurezza dei lavoratori.

e) Sensibilizzazione dell'intera struttura aziendale al fine di garantire il raggiungimento degli obiettivi prefissati anche attraverso la programmazione di cicli di formazione con particolare attenzione a:

- Coinvolgimento dei lavoratori e/o dei loro rappresentanti ed in particolare per attuare[17]:

---

[16] Si richiama l'art. 16 del TU Sicurezza "Delega di Funzioni":
"*1. La delega di funzioni da parte del datore di lavoro, ove non espressamente esclusa, è ammessa con i seguenti limiti e condizioni:*
a) che essa risulti da atto scritto recante data certa;
b) che il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;
c) che essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;
d) che essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate;
e) che la delega sia accettata dal delegato per iscritto.
2. Alla delega di cui al comma 1 deve essere data adeguata e tempestiva pubblicità.
3. La delega di funzioni non esclude l'obbligo di vigilanza in capo al datore di lavoro in ordine al corretto espletamento da parte del delegato delle funzioni trasferite. L'obbligo di cui al primo periodo si intende assolto in caso di adozione ed efficace attuazione del modello di verifica e controllo di cui all' articolo 30, comma 4.
3-bis. Il soggetto delegato può, a sua volta, previa intesa con il datore di lavoro delegare specifiche funzioni in materia di salute e sicurezza sul lavoro alle medesime condizioni di cui ai commi 1 e 2. La delega di funzioni di cui al primo periodo non esclude l'obbligo di vigilanza in capo al delegante in ordine al corretto espletamento delle funzioni trasferite. Il soggetto al quale sia stata conferita la delega di cui al presente comma non può, a sua volta, delegare le funzioni delegate".

* * *

Da notarsi che <u>non sono delegabili</u> da parte del datore di lavoro:
a) la valutazione di tutti i rischi con la conseguente elaborazione del documento di valutazione dei rischi;
b) la designazione del responsabile del servizio di prevenzione e protezione dai rischi.

[17] La circolazione delle informazioni all'interno dell'azienda è un elemento fondamentale per garantire livelli adeguati di consapevolezza ed impegno riguardo alla politica adottata in tema di SSL. Il principio che dovrebbe ispirare la realizzazione del flusso informativo è quello della cooperazione tra tutti i soggetti interessati, interni e/o esterni all'impresa. La cooperazione si dovrebbe realizzare in una cultura aziendale che dia risonanza al flusso informativo tramite la partecipazione attiva di tutto il personale aziendale ed in particolare di tutti i lavoratori. Maggiore è la condivisione delle informazioni e la partecipazione attiva alla gestione del sistema, maggiore sarà la probabilità di prevenire gli infortuni e le malattie correlate al lavoro.
Pertanto il personale dovrebbe essere:
- consultato, anche attraverso i suoi rappresentanti, sulle questioni afferenti la SSL e soprattutto quando sono previsti cambiamenti che influenzano la SSL, oltre che nella successiva fase di attuazione;
- informato su chi ed in quale misura detiene responsabilità per la SSL e chi sono i soggetti che hanno incarichi specifici inerenti la SSL in azienda.

A questo scopo si dovrebbe realizzare:
1. una adeguata comunicazione interna per sviluppare la cooperazione fra tutti i livelli aziendali, finalizzata alla raccolta e diffusione delle informazioni, realizzando una corretta raccolta e diffusione (dall'alto verso il basso e dal basso verso l'alto) di informazioni pertinenti, attraverso l'utilizzo di strumenti adeguati in funzione delle specifiche esigenze e dimensioni dell'impresa;
2. un'opportuna comunicazione esterna rivolta:
   - al personale esterno (committenti, fornitori, collaboratori esterni),
   - al pubblico (clienti, visitatori, soggetti interessati),
   - alle autorità;
3. la diffusione della politica della salute e sicurezza aziendale.

Esempi di possibili strumenti da utilizzare allo scopo di fornire corrette informazioni ai lavoratori.
<u>1. STRUMENTI</u>
- Assemblea
- Riunioni
- Comunicazioni faccia a faccia
- Opuscoli
- Comunicazioni in busta paga
- Comunicazioni in bacheca

- la consultazione preventiva in merito alla individuazione e valutazione dei rischi ed alla definizione delle misure preventive;
- riunioni periodiche da effettuarsi con frequenza e modalità che tengano conto almeno delle richieste fissate dalla legislazione vigente.

- Monitoraggio[18], periodicità, fruizione e apprendimento;
- Formazione differenziata per soggetti esposti a rischi specifici.

Tenuto conto che costituiscono in ogni caso aree sensibili ai fini della salvaguardia della sicurezza e salubrità nel luogo di lavoro tutte le politiche aziendali che definiscono gli impegni della Società in questo settore, con particolare riferimento agli obiettivi prefissati in tale ambito, le scelte organizzative aziendali devono essere tali da assicurare la miglior competenza e professionalità dei soggetti incaricati a vario titolo di garantire la sicurezza e la salubrità sul luogo di lavoro, nonché piena certezza circa i compiti e le deleghe conferite.

Le attività aziendali finalizzate a garantire la sicurezza sul luogo di lavoro sono formalizzate attraverso apposite procedure.

In materia di salubrità nel luogo di lavoro la Società adotta tutte le misure preventive appropriate per assicurare un livello elevato di protezione dell’ambiente nel suo complesso, al fine di prevenire, ridurre e, per quanto possibile, eliminare l’inquinamento, intervenendo alla fonte delle attività inquinanti e garantendo una corretta gestione delle risorse naturali.

- Manifesti
- Depliants illustrativi
- Segnaletica di sicurezza.

2. CONTENUTI

- Organizzazione aziendale della sicurezza
- Nominativi degli incaricati alla gestione dell’emergenza (addetti alla prevenzione incendi e addetti al primo soccorso), del RSPP, del RLS, del medico competente
- Rischi generali dell’azienda
- Rischi specifici dei reparti/mansioni.

[18] La documentazione è uno strumento organizzativo importante che consente ad una azienda la gestione nel tempo delle conoscenze pertinenti alla specifica realtà produttiva anche con l’obiettivo di contribuire alla implementazione ed al monitoraggio del sistema gestionale per la salute e la sicurezza aziendale. La documentazione dovrebbe essere tenuta ed aggiornata al livello necessario richiesto per mantenere il sistema efficiente ed efficace, in modo che la documentazione sia funzionale al sistema ma non lo condizioni. Le attività di consultazione, coinvolgimento, informazione e formazione del personale dovrebbero essere documentate e registrate. Un buon sistema di gestione della documentazione raggiunge un giusto equilibrio tra la necessità di raccolta, fruibilità ed archiviazione del maggior numero di dati e quella del loro aggiornamento. La documentazione aziendale risponde alle esigenze di conoscenza per sviluppare e mantenere un sistema di gestione efficiente, in modo semplice e snello.
Per documentazione si intende almeno:

- leggi, regolamenti, norme antinfortunistiche attinenti l’attività dell’azienda;
- regolamenti e accordi aziendali;
- quella richiesta dalla normativa vigente in materia di SSL;
- manuali, istruzioni per l’uso di macchine, attrezzature, dispositivi di protezione individuale
- (DPI) forniti dai costruttori;
- informazioni sui processi produttivi;
- schemi organizzativi;
- norme interne e procedure operative;
- piani di emergenza.

Dovrebbero essere stabilite, in funzione delle caratteristiche aziendali, modalità riguardanti la gestione della documentazione, modalità che contengano, tra l’altro, le seguenti indicazioni:

- l’eventuale figura incaricata della gestione del sistema documentale;
- i tempi di conservazione (rinnovo) della documentazione;
- il collegamento tra la gestione della documentazione e i flussi informativi interno ed esterno all’azienda;
- contenuti e la forma (supporti elettronici, cartacei, audiovisivi).

In ogni caso l’azienda stabilisce e mantiene le informazioni necessarie per descrivere gli elementi centrali del sistema di gestione e la loro interazione e per dare direttive per la predisposizione della documentazione correlata.
Tale documentazione può essere raccolta unitariamente oppure facilmente recuperabile al bisogno, anche mediante soluzioni informatiche adeguate.

E' il caso di ricordare, in proposito, la Direttiva del Parlamento Europeo e del Consiglio UE 2010/75/UE relativa alle emissioni industriali, sulla prevenzione e riduzione integrate dell'inquinamento, comunemente denominata "Direttiva IPPC" (*Integrated Pollution Prevention and Control*), la quale ha abrogato la precedente Direttiva adottata nel 1996 dal Consiglio dei Ministri dell'Unione Europea ed inizialmente trasposta nella legislazione nazionale con il Decreto Legislativo del 4 agosto 1999, n. 372, (anch'esso abrogato dal successivo D.Lgs n. 59 del 2005 che ha riordinato la materia). La Direttiva stabilisce i principi generali che governano gli obblighi base dei responsabili delle installazioni industriali, sia nuove sia esistenti. Le misure per prevenire l'inquinamento prevedono l'utilizzo delle "migliori tecniche disponibili" (*Best Available Techniques*, "BAT"), ossia lo sviluppo e la diffusione di produzioni più pulite[19]. La BAT comprende procedure, tecniche, tecnologie ed altri aspetti quali manutenzione, standard operativi e verifiche di consumi energetici e di efficienza e riguarda tutti gli aspetti del funzionamento di un impianto o di un'industria che influenzano l'ambiente. In quest'ottica, l'inquinamento comprende le sostanze tradizionali e il calore, il rumore e le vibrazioni, nonché il consumo delle risorse: acqua, materie prime ed energia.

E' inoltre il caso di richiamare il D.Lgs. 7 luglio 2011, n. 121 ("*Attuazione della direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della direttiva 2009/123/CE - che modifica la direttiva 2005/35/CE - relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni*"), entrato in vigore il 16 agosto 2011, che introduce nel nostro ordinamento il regime di responsabilità degli enti collettivi in relazione alla commissione di reati ambientali di cui al nuovo **art. 25-undecies** del D.lgs. 231/2001. I reati ambientali saranno oggetto di specifica trattazione nella successiva PARTE QUINDICESIMA, tuttavia, si segnala sin d'ora che nel recepire le direttive 2008/99/CE e 2009/123/CE, il legislatore delegato ha inteso estendere l'ambito di applicazione del D.lgs. 231/2001 ad alcune figure di reato già previste dall'ordinamento penale (vedi *sub* PARTE GENERALE Parte Prima – Paragrafo 1.5.2.15) oltre che a due nuove fattispecie introdotte dalla indicata novella (segnatamente i nuovi articoli 727-*bis* e 733-*bis* c.p.).

Con particolare attenzione ai reati di cui al Testo Unico dell'Ambiente (D. Lgs. n. 152/06), l'art. 25 *undecies* richiama espressamente l'attività di gestione rifiuti non autorizzata, nonché la mancata ottemperanza agli obblighi previsti dal sistema di controllo della tracciabilità dei rifiuti (SISTRI).

1.B) DESCRIZIONE DEL PROCESSO

Il processo si riferisce al complesso di attività riguardanti il corretto adempimento degli obblighi legislativi circa la prevenzione dei reati in materia di sicurezza e salute nei luoghi di lavoro e l'elaborazione dei sistemi di controllo e delle misure preventive e protettive dei lavoratori della Società, in coerenza con le *policy* interne e verificando l'attuazione degli adempimenti previsti. Esso si articola nelle seguenti fasi:

- definizione dell'organizzazione, delle responsabilità, delle autorità, delle risorse e competenze professionali necessarie per la gestione delle attività che hanno un impatto significativo sulla salute e sulla sicurezza dei lavoratori;

- comunicazione dei ruoli, delle responsabilità e delle autorità a tutti i livelli aziendali mediante l'attuazione di una procedura che preveda: (i)un programma di formazione ed informazione progettato dall'azienda; (ii) una informazione mirata mediante una "scheda di informazione mansione"; (iii) la distribuzione della modulistica che riporta appunto la suddivisione di ruoli, responsabilità ed obiettivi specificati per ogni figura.

[19] Realizzare produzioni più pulite significa realizzare processi produttivi con il minimo impatto ambientale, ed eliminando nel contempo le inefficienze energetiche e ottimizzando l'impiego delle risorse. Realizzare produzioni più pulite significa, quindi, attuare strategie preventive integrate che ottimizzino prodotti, processi e servizi allo scopo di minimizzare l'impatto ambientale attraverso l'impiego efficiente delle risorse energetiche e materie prime e la riduzione degli inquinanti prodotti, anzi, le produzioni pulite devono tendere al limite teorico delle "emissioni zero".

- gestione degli adempimenti in materia di antinfortunistica e tutela dell'igiene e della salute sul lavoro;

- individuazione dei criteri generali per la definizione degli obiettivi e dei traguardi, dei criteri di conduzione dei sopralluoghi e delle modalità per la corretta gestione della documentazione, nonché per il riesame del sistema.

In tutte le fasi del processo è fatto obbligo di attenersi:

- alla normativa *pro-tempore* vigente in materia di antinfortunistica e tutela dell'igiene e della salute sul lavoro;

- agli strumenti per la gestione e il controllo delle tematiche di antinfortunistica e tutela dell'igiene e della salute sul lavoro – e relative normative interne – adottati dalla Società (con particolare riferimento ai contenuti dei documenti di valutazione dei rischi, al monitoraggio degli infortuni sul lavoro ed ai sistemi di gestione riguardanti contratti di appalto, d'opera e cantieri temporanei o mobili).

Ciò al fine di garantire:

- l'effettuazione di una mappatura del rischio approfondita e orientata secondo le specificità dell'attività;

- un'attenta verifica ed eventuale integrazione delle procedure interne di prevenzione ai sensi dei principi contenuti nel Decreto in coerenza con la specificità dei rischi di violazione delle norme richiamate dall'art. 25 septies del Decreto medesimo;

- la valutazione ed individuazione dei raccordi tra i vari soggetti coinvolti nel sistema di controllo, con particolare riferimento alle persone incaricate dalla Società (qualificabile come controllo tecnico-operativo o di primo grado) e l'Organismo di Vigilanza incaricato del controllo sulla efficienza ed efficacia delle procedure rilevanti ai sensi del Decreto (controllo di secondo grado).

1.c) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

1) Il reato di **omicidio colposo** commesso con violazione dell'articolo 55, comma 2, del D. Lgs. n. 81/2008, attuativo dell'articolo 1, della Legge delega n. 123/2007, ovverosia, con violazione delle prescrizioni aventi ad oggetto la designazione del Responsabile Prevenzione e Protezione Rischi, le attività di valutazione dei rischi medesimi e di predisposizione ed adozione della relativa documentazione (c.d. attività "*non delegabili*" dal Datore di Lavoro) (art. 589 c.p.).

2) Il reato di **omicidio colposo** commesso con violazione delle prescrizioni del D. Lgs. n. 81/2008, attuativo dell'articolo 1, della Legge delega n. 123/2007, diverse da quelle di cui all'articolo 55, comma 2, del decreto medesimo (art. 589 c.p.).

3) Il reato di **lesioni colpose gravi o gravissime** commesse con violazione delle prescrizioni del D. Lgs. n. 81/2008, attuativo della Legge delega n. 123/2007 (art. 590, terzo comma, c.p.).

Gli elementi costitutivi delle fattispecie criminose di cui ai precedenti punti 1), 2) e 3) sono i seguenti.

(i) Una condotta di natura colposa consistente nella violazione delle sopra richiamate previsioni in materia di salute e sicurezza sul lavoro, avuto riguardo al complesso delle misure di sicurezza e prevenzione

tecnicamente possibili, concretamente attuabili e generalmente praticate alla luce dell'esperienza e delle più avanzate conoscenze tecnico-scientifiche.

(ii) Il verificarsi di uno dei seguenti eventi-reato:

a. la morte del lavoratore, nei casi di cui ai precedenti punti 1) e 2);

b. lesioni "*gravi*" o "*gravissime*" alla persona fisica del lavoratore, nei casi di cui al precedente punto 3).

Per "*lesioni*" si intende un danno alla incolumità della persona fisica stessa.

La lesione è considerata "*grave*" (art. 583, c. 1, c.p.) nei seguenti casi: (a) se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni; (b) se il fatto produce l'indebolimento permanente di un senso o di un organo.

La lesione è considerata invece "*gravissima"* se dal fatto deriva (art. 583, c. 2, c.p.): a) una malattia certamente o probabilmente insanabile; (b) la perdita di un senso; (c) la perdita di un arto o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare ovvero una permanente e grave difficoltà della favella; (d) la deformazione ovvero lo sfregio permanente del viso.

(iii) il nesso di causalità tra la condotta di cui al precedente punto (i) e l'evento-reato di cui al conseguente punto (ii). E' necessario, dunque, che l'evento-reato sia conseguenza, immediata e diretta, della violazione delle prescrizioni in materia di salute e sicurezza sul lavoro, così come sopra individuate; pertanto: (a) dovrà sussistere un nesso di derivazione effettiva tra la violazione colposa delle predette prescrizioni sulla salute e la sicurezza e lo svolgimento dell'attività lavorativa; (b) si avrà una interruzione del nesso di causalità laddove l'evento lesivo si verifichi per comportamenti del lavoratore abnormi ed esorbitanti rispetto al procedimento lavorativo e, perciò, imprevedibili ed inevitabili.

L'applicabilità di tali reati a Venis è stabilita direttamente dalla legge come specificato negli articoli 3 e 30 del D. Lgs. 81/2008 (Testo Unico sulla Sicurezza sul Lavoro).

E' il caso di precisare, inoltre, che l'obbligo di sicurezza in capo alla Società non può intendersi in maniera esclusivamente statica quale obbligo di adottare tutte le misure di prevenzione e sicurezza possibili nei termini esposti al precedente punto (i) (forme di protezione oggettiva), ma deve intendersi anche in maniera dinamica implicando l'obbligo di informare e formare i lavoratori sui rischi propri dell'attività lavorativa e sulle misure idonee per evitare i rischi o ridurli al minimo (forme di protezione soggettiva).

Trattandosi di reati a forma libera, le modalità attuative per il perfezionamento degli stessi potrebbero essere molteplici.

In particolare, trattandosi di reati di natura colposa, caratterizzati dallo svolgimento di attività pericolose per l'altrui incolumità, per il loro perfezionamento non è richiesta la rappresentazione e la volontà, da parte dell'agente, dell'evento morte o dell'evento lesioni, né tanto meno, l'intenzione di arrecare un pregiudizio a terzi soggetti.

Le modalità attuative dei reati in questione consistono, generalmente, in condotte di tipo omissivo (ad es. mancata adozione delle cautele prescritte); non è, però, da escludersi la rilevanza di condotte di tipo commissivo

(ordine di eseguire una determinata attività, in spregio della richiamata normativa anti-infortunistica): anche in tali casi, non è richiesto che la finalizzazione volontaristica dell'ordine di violare le predette prescrizioni abbia ad oggetto la morte o le lesioni del lavoratore.

Si precisa, comunque, che, perché possa ipotizzarsi una responsabilità della Società ai sensi del Decreto, è necessario che dalla condotta colposa penalmente rilevante, come sopra descritta – pur caratterizzandosi per l'assenza di rappresentazione e volontà, da parte del soggetto agente, dell'evento morte o lesioni del terzo quale conseguenza della propria condotta – **sia disceso un *vantaggio* per la Società stessa** (ad es. in termini di risparmio di costi e/o tempi nelle attività aziendali). Stante la natura colposa del reato, è da escludersi, ragionevolmente, che la descritta condotta penalmente rilevante possa essere realizzata nell'*interesse* della Società.

Ne consegue che la condotta del soggetto agente, integratrice dei reati sopra richiamati e rilevante ai fini del Decreto, dovrà essere caratterizzata quantomeno dalla c.d. "*colpa cosciente o specifica*", ovverosia, consistere nella volontaria violazione delle anzidette prescrizioni sulla salute e la sicurezza pur mancando la rappresentazione e volontà dell'evento morte o lesioni (ad esempio, un soggetto apicale, consapevole dell'aggravio di costi che deriverebbe dall'ammodernamento, peraltro necessario, dei macchinari in uso presso la società, onde porre in medesimi nelle condizioni di sicurezza prescritte dalla legge, allo scopo di evitare che la persona giuridica sia costretta ad effettuare tali spese, omette di provvedere all'ammodernamento dei macchinari stessi).

Come si è visto, secondo il corrente orientamento giurisprudenziale e le Linee Guida di Confindustria, è da ritenersi non configurabile uno dei reati di cui ai precedenti punti 1), 2) e 3) e, comunque, la responsabilità amministrativa della Società – per mancanza del nesso di causalità – laddove l'evento lesivo si verifichi per comportamenti del lavoratore abnormi ed esorbitanti rispetto al procedimento lavorativo e perciò, imprevedibili e inevitabili; in particolare, potrà trattarsi di condotte personali del lavoratore, avulse dall'esercizio della prestazione lavorativa o ad essa non riconducibili, esercitate ed intraprese volontariamente in base a ragioni e a motivazioni arbitrarie, tali, dunque, da interrompere il nesso eziologico tra prestazione ed attività lavorativa (ad esempio: la scelta autonoma del lavoratore di utilizzare per prova un macchinario per il cui utilizzo il lavoratore medesimo non abbia le competenze tecniche, ovvero, pur in presenza di queste ultime, con modalità operative difformi dalle disposizioni di legge e dalle indicazioni contenute nel libretto d'uso e manutenzione fornito dalla ditta costruttrice).

Soggetti attivi delle condotte in questione possono essere, ciascuno in relazione al proprio ambito di competenze e responsabilità e con riferimento, pertanto, alle regole ed alle prescrizioni in materia di salute e sicurezza nei luoghi di lavoro che sono a ciascuno specificamente indirizzate:

- i soggetti tenuti a far osservare le norme di prevenzione e protezione, ovverosia, tutti coloro che, nell'ambito dell'organizzazione aziendale, in forza di quanto previsto dall'organigramma e dal sistema di deleghe in essere, risultino titolari dei poteri decisionali e di spesa idonei a garantire l'attuazione ed il rispetto delle norme in materia di salute e sicurezza sui luoghi di lavoro;

- coloro che rivestono gli specifici ruoli di controllo tecnico-operativo nell'ambito della Società, in ottemperanza con quanto previsto dalla normativa in materia di tutela della salute e della sicurezza;

- i soggetti tenuti ad osservare le richiamate norme, ovverosia, tutti gli altri dirigenti, dipendenti e collaboratori della Società (limitatamente al mancato rispetto delle *policy* e/o procedure aziendali elaborate ad *hoc*).

Coerentemente, potrebbe allo stesso modo sorgere la responsabilità amministrativa di quest'ultima laddove:

- la violazione delle norme sulla salute e la sicurezza (che abbia causato l'evento morte o lesioni) sia stata

posta in essere, quale “ingerenza” nell’esecuzione dei lavori, da parte di persone prive di un collegamento diretto con la Società (si pensi ad un dipendente della committente nel caso in cui la Società operi come appaltatore, o ad un Responsabile dei lavori e/o un Direttore lavori nominato all’esterno e quindi estraneo all’organizzazione aziendale della Società) le quali abbiano, in concreto, impartito ordini alle maestranze di quest’ultima in violazione delle norme di prevenzione e

- il soggetto individuato dalla società come Datore di Lavoro abbia prestato acquiescenza a tale ingerenza; ciò in applicazione del principio della cooperazione colposa di cui all’art. 113 c.p..

1.D) FUNZIONI INTERESSATE

Dal punto di vista della localizzazione fisica sono interessate:

- la sede principale di Venis e gli Uffici periferici, anche di decentramento di funzioni IT;
- i singoli cantieri di esecuzione opere e lavori (individuati anch’essi come Unità produttive ai sensi della normativa vigente).

Dal punto di vista funzionale, gli ambiti aziendali potenzialmente interessati dalle attività a rischio di commissione dei reati in parola sono stati individuati sulla base dell’Organigramma Venis allegato alla Parte Generale del Presente Modello.

Essi sono:

- l’Organo Amministrativo;
- tutte le funzioni aziendali, sia quelle di linea che quelle di supporto e di staff, ed i relativi dirigenti, dipendenti e collaboratori, con particolare riferimento alla Funzione che esercita gli adempimenti in materia di Sicurezza del Lavoro e Ambiente;
- coloro che ricoprono la carica di Datore di Lavoro per la sede centrale e, laddove siano soggetti diversi, per le sedi periferiche e per i singoli cantieri;
- con riferimento all’Unità produttiva cantiere, anche il Responsabile del Procedimento relativo alla singola opera o lavoro, in quanto ad esso, con l’ausilio del Direttore dei Lavori incaricato, competono i compiti in materia di sicurezza sui luoghi di lavoro e misure generali di tutela previste dalle leggi vigenti; particolare riferimento deve essere fatto alla Funzione Sistemi e Servizi Tecnologici Sicurezza Informatica in quanto direttamente coinvolta nei procedimenti e contratti pubblici di sviluppo in materia IT, vocazione precipua di Venis;
- il Responsabile della Sicurezza incaricato per cantiere.

Sono altresì interessati tutti i dirigenti, dipendenti e collaboratori, pur non ricompresi nelle Funzioni sopra elencate, operanti nelle diverse attività e/o fasi dei processi precedentemente individuate ed in ogni caso tenuti al rispetto delle *policy* e/o procedure aziendali elaborate ad *hoc*.

1.E) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sull’elemento qualificante della **tracciabilità degli atti** del processo e il **sistema di deleghe** in materia definite a livello organizzativo.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- Attività di valutazione dei rischi e predisposizione delle misure di prevenzione e protezione conseguenti;
- Attività di natura organizzativa (quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza);
- Attività di sorveglianza sanitaria;
- Attività di informazione e formazione dei lavoratori;
- Attività di vigilanza con riferimento al rispetto delle procedure in materia di sicurezza;
- Acquisizione di documentazioni e certificazioni obbligatorie di legge;
- Definizione di periodiche verifiche dell’applicazione e dell’efficacia delle procedure adottate;
- Definizione e aggiornamento di un sistema di deleghe *ad hoc*;
- Definizione di idonei sistemi di registrazione dell’avvenuta effettuazione delle attività di cui alla presente elencazione;
- Definizione di un sistema di incentivazione legato alla corretta gestione della normativa in materia di antinfortunistica e tutela dell’igiene e della salute sul lavoro;
- Tracciabilità delle singole attività (documentazione a supporto, verbalizzazione delle decisioni, intestazione/formalizzazione dei documenti e modalità/tempistiche di archiviazione);
- Verifica della corrispondenza delle dichiarazioni/certificazioni presentate con la documentazione tecnica di supporto;
- Archiviazione dei flussi documentali fra le funzioni della Società interessate e gli organi della Pubblica Amministrazione deputati al rilascio di autorizzazioni e/o deputati all’effettuazione di ispezioni e verifiche.

1.F) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato o comunque contrari al Presente Modello, al Codice Etico ed al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione.

Inoltre, considerato che tutte la aree aziendali sono potenzialmente a rischio di inadempimento ai dettami richiesti dalla normativa relativa alla sicurezza sul lavoro e che Venis è tenuta a rispettare le norme sopra richiamate anche nella gestione e nell'affidamento di appalti di lavori, servizi e forniture, di seguito sono riportate le ulteriori indicazioni comportamentali applicabili:

- deve esistere segregazione dei compiti tra chi autorizza, chi esegue, chi contabilizza e chi controlla una determinata opera o lavoro nell'interesse della Società, in modo tale che nessuno possa gestire in autonomia un intero processo;

- le cariche e le responsabilità di Datore di Lavoro in relazione ai dipendenti della Società devono essere razionalmente distribuite fra le figure apicali e dirigenziali in ragione delle specifiche competenze funzionali, nonché debitamente a queste delegate dall'Organo Amministrativo della Società, anche al fine di massimizzare l'efficacia dei sistemi di controllo sull'operato del personale dipendente e la prossimità funzionale fra responsabili e dipendenti.

- deve essere effettuata la formalizzazione delle attività, evidenziando gli opportuni punti di controllo. Le operazioni aziendali devono essere regolate da una procedura definita e le attività estemporanee devono ottemperare almeno al principio della verificabilità;

- il sistema delle deleghe interne e delle procure ad agire verso l'esterno deve essere coerente con le responsabilità organizzative e gestionali assegnate e prevedere una puntuale indicazione delle soglie di approvazione delle spese;

- deve essere garantita la tracciabilità: ogni operazione, transazione e azione deve essere verificabile, documentata, coerente e congrua in modo tale che sia possibile in ogni momento l'effettuazione di controlli che attestino le caratteristiche e le motivazioni delle stesse;

- deve esistere un sistema di controllo di gestione in grado di segnalare l'insorgere di situazioni di criticità e anomalie;

- le funzioni di Responsabile Unico di Procedimento e di Direttore della Sicurezza devono essere affidate a personale qualificato allo scopo e debitamente coadiuvato nell'esercizio delle funzioni di controllo e tutela;

- deve essere prevista la pianificazione periodica delle attività di formazione del personale e diffusione in azienda della normativa riguardante salute e sicurezza, lasciando adeguata traccia delle suddette attività di pianificazione e dell'attività di diffusione.

1.G) INFORMATIVA VERSO L'ORGANISMO DI VIGILANZA

Il Responsabile della Funzione Finanza, Bilancio e Amministrazione del Personale, anche avvalendosi della collaborazione delle altre Funzioni aziendali, deve informare l'OdV in merito:

a. alle attività annualmente svolte in materia di sicurezza sul lavoro, comprese le eventuali attività di formazione del personale, ed alle risultanze emerse;

b. agli infortuni eventualmente verificatisi e all'indice di gravità degli stessi, con analitica descrizione di eventuali infortuni mortali e gravi o gravissimi (da comunicarsi comunque al verificarsi dell'evento)

ed agli eventuali casi di denuncia di malattia professionale.

c. agli esiti di eventuali ispezioni di Autorità Amministrative o Giudiziarie.

d. agli appalti affidati dalla Società con indicazione dei RUP e Responsabili della Sicurezza nominati

Gli organigrammi, le deleghe e procure inerenti l’antinfortunistica e la tutela dell’igiene e della salute sul lavoro non costituiranno oggetto di informazione specifica ma l’accesso alla relativa documentazione dovrà essere sempre consentito all’OdV, il quale dovrà essere edotto, altresì, dei luoghi presso i quali sono disponibili, per loro verifica.

1.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Principi di Comportamento Generali e nei Rapporti con la Pubblica Amministrazione;
- Procure generali e speciali di attribuzione della qualifica di Datore di Lavoro;
- Documento di valutazione dei rischi d’azienda come approvato dall’SPP;
- Documentazione specifica di sicurezza (PSC, POS, DUVRI) relativa ad attività esterne alle sedi o anche interne ma complementari e secondarie rispetto all’ attività principale;
- Documento Programmatico per la Sicurezza (DPS).

PARTE DODICESIMA – REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI E UTILITÀ DI PROVENIENZA ILLECITA

(art. 25 octies del Decreto)

Con il Decreto Legislativo 21 novembre 2007, n. 231 (in vigore dal 29 dicembre 2007) il legislatore ha dato attuazione alla Direttiva 2005/60/CE del Parlamento e del Consiglio del 26 ottobre 2005, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (c.d. III Direttiva Antiriciclaggio), e alla Direttiva 2006/70/CE della Commissione che ne reca misure di esecuzione. L'intervento normativo ha comportato un riordino della complessa normativa antiriciclaggio presente nel nostro ordinamento giuridico. L'art. 63, comma 3, D. Lgs. n. 231/2007 ha introdotto nel Decreto un nuovo art. 25 octies, che estende la responsabilità amministrativa degli enti ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

Nella materia era recentemente intervenuto il D.L. n. 78/2010, recante "*Misure urgenti in materia di stabilizzazione finanziaria e di competitività economica",* convertito con modificazioni dalla L. n. 122/2010, il quale prevedeva che, ai fini di adeguamento alle disposizioni adottate in ambito comunitario in tema di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, le limitazioni all'uso del contante e dei titoli al portatore, di cui all'art. 49, commi 1, 5, 8, 12 e 13, del Decreto Legislativo 21 novembre 2007 n. 231,fossero adeguate all'importo di Euro 5.000,00 (cinquemila). Con il D.L. 201/2011 (pubblicato in G.U. n. 284 del 06/12/2011 e convertito in legge, dall'art. 1, comma 1, L. 22 dicembre 2011, n. 214 - "Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici") è stato ulteriormente ridotto il limite per la tracciabilità dei trasferimenti di denaro contante e dei titoli al portatore che attualmente è di Euro 1000 (*mille/00*).

Le operazioni di ammontare pari o superiore non possono quindi essere regolarizzate in contanti e il trasferimento di denaro contante tra soggetti diversi è possibile solo fino all'importo di Euro 999,99 (*novecentonovantanove*/99). E' inoltre vietato detenere libretti di deposito bancari o postali al portatore con saldo pari o superiore ad Euro 1.000 (*mille/00*), i quali hanno dovuto pertanto essere estinti o il loro saldo ridotto al di sotto del limite di Euro 1000 (*mille/00*) entro il 31 dicembre 2011.

Aree a rischio

Le attività aziendali interessate dal rischio di commissione dei reati in esame possono essere individuate nelle seguenti:

- attività approvvigionamento di beni e servizi;
- gestione pagamenti (attività relative agli esborsi finanziari a fronte di approvvigionamenti di beni e servizi);
- gestione incassi;
- gestione del personale;
- attività con soggetti terzi (intendendosi per tali le attività relative ai rapporti instaurati tra società e soggetti terzi).

1) "ATTIVITÀ RILEVANTI IN MATERIA DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI E UTILITÀ DI PROVENIENZA ILLECITA"

1.A) DESCRIZIONE DEL PROCESSO

I processi sopra considerati comprendono le attività di approvvigionamento di beni e servizi ed i relativi esborsi finanziari, la gestione degli incassi e del personale.

Con particolare riferimento alle attività con soggetti terzi, il processo attiene essenzialmente:

- alla gestione di flussi e transazioni finanziarie;
- alla gestione dei rapporti con banche ed altri intermediari finanziari (operazioni di apertura, utilizzo, controllo e chiusura dei conti correnti; richiesta e rilascio di fideiussioni; richiesta di finanziamenti, etc.);
- ai contratti di acquisto, vendita, fornitura, approvvigionamento, subappalto, etc., stipulati con soggetti terzi ed alle connesse attività degli Uffici della Società competenti, con particolare riferimento ai pagamenti ed alle garanzie;
- agli investimenti con terzi soggetti, con particolare riferimento ad accordi/*joint ventures* o alla creazione di consorzi;
- al sostenimento di spese a favore di soggetti terzi, al fine di pubblicizzare il marchio e l'immagine della Società.

1.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

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

L'art. 648 c.p. (**Ricettazione**) punisce chi, fuori dei casi di concorso nel reato, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi altro delitto, o comunque, si intromette nel farle acquistare, ricevere od occultare.

Per "*acquisto*" deve intendersi l'effetto di un'attività negoziale, sia a titolo gratuito che oneroso, mediante la quale l'agente consegue il possesso del bene. Il possesso, anche se solo temporaneo o per mera compiacenza, del bene proveniente dal delitto deve conseguire, in qualsiasi forma, anche nell'ipotesi in cui l'agente *riceva* il bene medesimo. Da ultimo, per "*occultamento*" deve intendersi il nascondimento, successivo all'impossessamento, del bene proveniente dal delitto.

La ricettazione può realizzarsi anche mediante l'"*intromissione*" nell'acquisto, nella ricezione o nell'occultamento della cosa. Tale condotta si esteriorizza in ogni attività di mediazione, da intendersi tecnicamente, in senso lato, tra l'autore del reato principale e il terzo acquirente.

L'ultimo comma dell'art. 648 c.p. estende la punibilità anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto.

Gli obiettivi dell'incriminazione della descritta condotta sono i seguenti: *i*) impedire il perpetrarsi della lesione di interessi patrimoniali iniziata con la consumazione del reato principale; *ii*) evitare la commissione dei reati principali, come conseguenza dei limiti posti alla circolazione dei beni provenienti dai reati medesimi.

Anche con riferimento al reato di **riciclaggio** (art. 648 bis c.p.) gli obiettivi dell'incriminazione sono due: *i)* impedire che gli autori dei reati possano far fruttare i capitali illegalmente acquisiti, rimettendoli in circolazione come capitali ormai "depurati" e perciò investibili anche in attività economiche produttive lecite; *ii)* scoraggiare la stessa commissione dei reati principali, mediante le barriere frapposte alla possibilità di sfruttarne i proventi.

Segnatamente, l'art. 648 bis c.p. punisce chiunque fuori dei casi di concorso nel reato, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Per *sostituzione* si intende la condotta consistente nel rimpiazzare il denaro, i beni o le altre utilità di provenienza illecita con valori diversi. Il *trasferimento* consiste nella condotta tendente a ripulire il denaro, i beni o le altre utilità mediante il compimento di atti negoziali. Le *operazioni* idonee ad ostacolare l'identificazione dell'illecita provenienza potrebbero essere considerate quelle in grado di intralciare l'accertamento da parte della autorità giudiziaria della provenienza delittuosa dei valori provenienti dal reato.

Il richiamo del terzo comma dell'articolo in esame all'ultimo comma dell'art. 648 c.p. comporta, anche per tale reato, la punibilità pur quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto.

La configurazione del delitto di **impiego di denaro, beni o utilità di provenienza illecita** (art. 648 ter c.p.) risponde ad una duplice finalità: (i) impedire che il c.d. "denaro sporco", frutto dell'illecita accumulazione, venga trasformato in denaro pulito; (ii) in una seconda fase, fare in modo che il capitale, pur così emendato dal vizio di origine, non possa trovare un legittimo impiego.

La clausola di riserva contenuta nel comma 1 della anzidetta disposizione prevede la punibilità solamente di chi non sia già compartecipe del reato principale ovvero non sia imputabile a titolo di ricettazione o riciclaggio. Da ciò deriva che per la realizzazione della fattispecie *de qua* occorre la presenza, quale elemento qualificante rispetto alle altre figure criminose sopra esaminate *sub* nn. 1) e 2), di una condotta di impiego dei capitali di provenienza illecita in attività economiche o finanziarie.

Il termine *impiegare* deve essere inteso nel senso di "*utilizzare per qualsiasi scopo*". Tuttavia, considerato che il fine ultimo perseguito dal legislatore consiste nell'impedire il turbamento del sistema economico e dell'equilibrio concorrenziale attraverso l'utilizzo di capitali illeciti reperibili a costi inferiori rispetto a quelli leciti, si ritiene che il termine impiegare debba essere inteso come "*investire*" e, dunque, ritenersi rilevante, ai fini della configurazione del reato in esame, un utilizzo a fini di profitto.

Anche nell'art. 648 ter c.p. si rinvia all'ultimo comma dell'art. 648 c.p.

1.c) FUNZIONI INTERESSATE

Gli ambiti aziendali potenzialmente interessati dalle attività a rischio di commissione dei reati in parola sono stati individuati sulla base dell'Organigramma Venis allegato alla Parte Generale del Presente Modello.

In dettaglio, gli ambiti aziendali interessati ricomprendono:

- l’Organo Amministrativo
- la Direzione Coordinamento Generale
- la Funzione Finanza, Bilancio e Amministrazione del Personale
- la Funzione Acquisti, Gare e Contratti
- la Funzione Tecnologie, Servizi e Sviluppo
- il Responsabile del Procedimento
- la Funzione Comunicazione, Sviluppo Personale e Qualità

Sono altresì interessati tutti i dirigenti e dipendenti nonché collaboratori e partner, pur non ricompresi nelle Funzioni sopra elencate, operanti nelle diverse attività e/o fasi del processo precedentemente individuate.

1.D) SISTEMA DI CONTROLLO

Il sistema di controllo applicabile si basa essenzialmente sugli elementi qualificanti della **separazione di ruolo** nelle fasi chiave del processo e della **tracciabilità delle fasi del processo**.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati:

- la segregazione delle responsabilità tra le aree/soggetti che svolgono le attività di:
    - autorizzazione,
    - esecuzione,
    - contabilizzazione e
    - controllo

  di una determinata operazione, in modo tale che nessuno possa gestire in autonomia un intero processo;
- deve essere effettuata la formalizzazione delle attività, evidenziando gli opportuni punti di controllo. Le operazioni aziendali devono essere regolate da una procedura definita e le attività estemporanee devono ottemperare almeno al principio della verificabilità;
- il sistema delle deleghe interne e delle procure ad agire verso l’esterno deve essere coerente con le responsabilità organizzative e gestionali assegnate e prevedere una puntuale indicazione delle soglie di approvazione delle spese;
- è escluso effettuare prestazioni in favore dei consulenti, dei partner e dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere;

- garantire la tracciabilità: ogni operazione, transazione, pagamento e azione deve essere verificabile, documentata, coerente e congrua in modo tale che sia possibile in ogni momento l'effettuazione di controlli che attestino le caratteristiche e le motivazioni alla base delle scelte. Tutta la documentazione riguardante ogni singola attività dei processi sopra considerati deve esser periodicamente aggiornata ed adeguatamente archiviata e conservata;

- deve esistere un sistema di controllo di gestione in grado di segnalare l'insorgere di situazioni di criticità ed anomalie.

1.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo.

In particolare i principi procedurali che devono essere implementati per prevenire la fattispecie di reato considerate sono i seguenti:

- nell'ambito dei rapporti con i consulenti, i fornitori, i partner commerciali e, in genere, con le controparti contrattuali deve essere garantito il rispetto dei principi di correttezza, trasparenza e buona fede;

- con riferimento alla correttezza commerciale/professionale dei fornitori e dei partner, devono essere richieste tutte le informazioni necessarie, utilizzando ogni strumento idoneo a tal fine;

- gli incarichi conferiti ad eventuali aziende di servizi e/o persone fisiche che curino gli interessi economico/finanziari della società devono essere anch'essi redatti per iscritto, con l'indicazione dei contenuti e delle condizioni economiche pattuite;

- è necessario che le funzioni competenti assicurino il controllo della avvenuta regolarità dei pagamenti nei confronti di tutte le controparti e dovrà essere precisamente verificato che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme;

- il controllo sia formale che sostanziale (verifica della sede legale della società controparte, verifica degli istituti di credito utilizzati, verifica relativamente all'utilizzo di società fiduciarie) deve essere garantito con riferimento ai flussi finanziari aziendali e ai pagamenti verso terzi:

- è necessario che siano previste limitazioni sull'uso del contante, titoli al portatore, assegni e libretti al portatore, di cui all'articolo 49, commi 1, 5, 8, 12 e 13, del decreto legislativo 21 novembre 2007, n. 231, e che in ogni caso le transazioni finanziarie in contanti non superino mai l'importo massimo di Euro 999,99 (*novecentonovantanove*/99) così come previsto dal D.L. 201/2011 (convertito in legge, dall'art. 1, comma 1, L. 22 dicembre 2011, n. 214 - "Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici, la promozione e la tutela della concorrenza e per lo sviluppo industriale e infrastrutturale del Paese").

1.F) FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

In generale non sono previsti flussi informativi specifici, ma l'accesso ai documenti deve essere sempre consentito all'Organismo di Vigilanza senza alcun obbligo di preavviso.

Atteso che l’Organismo di Vigilanza deve provvedere altresì ad effettuare il controllo di merito anche con riferimento al rispetto della normativa antiriciclaggio di cui al Dlgs 231/07, verificando altresì l’adozione di procedure di prevenzione al coinvolgimento di episodi di riciclaggio e finanziamento al terrorismo da parte di Venis, sono previsti flussi informativi specifici con gli altri organi di controllo di cui all’art. 52 del Dlgs 231/07, come il Collegio Sindacale, al fine di garantire la funzionalità del Modello.

1.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Principi di Comportamento Generali e nei rapporti con la Pubblica Amministrazione
- Procedura organizzativa VAQ-AC-MP-01 “Albo dei fornitori in Venis”
- Procedura organizzativa VAQ-AC-MP-02 “Gli approvvigionamenti in Venis”
- Procedura organizzativa VAQ-AC-MP-04 “Gestione Gare”

PARTE TREDICESIMA – DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

(art. 25 nonies D.Lgs 231/01)

Mediante l'introduzione nel Decreto dell'articolo 25 nonies, ad opera della Legge 23 luglio 2009, n. 99, la responsabilità amministrativa dell'Ente è stata estesa ad alcuni delitti in materia di violazione del diritto d'autore attraverso il richiamo, del medesimo articolo 25 nonies, degli articoli 171, comma 1, lettera a bis, 171 comma 3, 171 bis, 171 ter, 171 septies e octies della Legge 22 aprile 1941 n. 633 (c.d. legge sul diritto d'autore).

Aree a rischio

Ferma restando la non esaustività dell'elenco che segue, in ragione della continua evoluzione dell'attività svolta da Venis, sono da considerarsi in ogni caso aree a rischio le seguenti attività:

1) Gestione del sito www.venis.it;
2) Gestione di portali informativi o diffusivi;
3) Gestione di altri siti Internet in generale;
4) Gestione dei servizi di rete accessibili al pubblico (anche nel caso di sviluppo *ad hoc*);
5) Sviluppo, produzione o distribuzione di materiale informativo, didascalico, illustrativo o promozionale, su qualsiasi supporto, anche digitale o *on line*, che possa riportare opere protette dalla legge sul diritto d'autore;
6) Sistema automatizzato di *streaming* audio/video delle sedute degli organi collegiali dell'ente locale di riferimento.

1) "ATTIVITÀ RILEVANTE IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE"

1.A) DESCRIZIONE DEI PROCESSI

I processi attengono a tutte le attività di gestione degli spazi su siti o portali Internet, così come alla produzione, sviluppo o distribuzione di materiale su supporto digitale, magnetico o fisico, in via continuativa o nel caso di organizzazione temporanea di eventi, con particolare attenzione all'immissione di contenuti in rete da parte della Società (distribuzione di pacchetti software, applicativi, audiovisivi).

1.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Il rischio di commissione di delitti in materia di violazione del diritto d'autore nell'ambito dello svolgimento delle attività aziendali di Venis è piuttosto ridotto, sia in ragione della tipologia e delle modalità con cui l'attività aziendale viene svolta, sia in ragione della natura stessa dei reati in esame, trattandosi di fattispecie criminose

relativamente alle quali è difficile ipotizzare che possano essere commessi nell'interesse o nel vantaggio dell'Ente.

Tuttavia, è il caso di focalizzare l'attenzione sui i reati di cui all'**art. 171, comma 1, lett. a bis)**, e **comma 3**, **art. 171 bis**, **art. 171 ter**, **art. 171 septies** e **art. 171 octies** della legge sul diritto d'autore, per i quali il rischio che vengano commessi è, in linea di principio, maggiormente sussistente.

Il primo delitto (**art. 171, comma 1, lett. a bis**), introdotto dalla Legge 31 marzo 2005, n. 43, punisce 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.

In questa norma ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere frustrate le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete. L'inserimento del delitto nel Decreto risponde quindi ad una volontà di responsabilizzazione di tutte quelle aziende che gestiscono server attraverso cui si mettono a disposizione del pubblico opere protette da diritto d'autore.

Le aziende che operano nel settore dovranno predisporre controlli più accurati sui contenuti che transitano sui propri server. Ciò, a stretto rigore, anche qualora siano gli utenti stessi a rendere pubblici i contenuti direttamente e senza filtro preventivo del gestore (si pensi al sistema di funzionamento di "*youtube.com*"). Anche in questi casi, invero, si potrebbe configurare un responsabilità per la società che non si è organizzata per prevenire tale rischio di reato.

Il delitto di cui all'**art. 171, comma 3** punisce le condotte sopra menzionate ove commesse su una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

In quest'ultima fattispecie di danno, il bene giuridico protetto non è, evidentemente, l'aspettativa di guadagno del titolare dell'opera, ma il suo onore e la sua reputazione.

L'**art. 171 bis**, introdotto dal Decreto legislativo 29 dicembre 1992 n. 518, di attuazione della Direttiva 91/250/CEE, ha segnato l'ingresso nel panorama normativo italiano della tutela penale del software.

La disposizione tuttavia non contiene alcuna definizione del proprio oggetto di tutela. Per ricostruirne l'esatta portata è allora necessario far riferimento alle disposizioni civilistiche contenute nella medesima legge.

In particolare, l'art. 2 della legge sul diritto d'autore tutela i programmi per elaboratore, in qualsiasi forma espressi, purché originali, quale risultato della creazione intellettuale dell'autore mentre esclude dalla tutela le idee ed i principi che stanno alla base di un programma, compresi quelli alla base delle sue interfacce.

L'articolo 171 bis si divide in due commi: il primo volto alla tutela dei software in generale, il secondo, inserito dal Decreto Legislativo 6 maggio 1999, n. 169, tutela invece le banche dati.

Quanto al primo comma, la disposizione colpisce anzitutto la condotta di abusiva duplicazione: il legislatore si è mostrato più rigoroso di quello europeo, che invece riteneva necessaria la punibilità solo di condotte più propriamente finalizzate al commercio. Ad oggi, quindi, è prevista la rilevanza penale di ogni condotta di duplicazione di software che avvenga ai fini di lucro, accezione ben più ampia della preesistente, che prevedeva il necessario dolo specifico di profitto.

A restringere l'ambito di applicabilità della norma vi è però il riferimento all'abusività della riproduzione che, sul piano soggettivo implica che il dolo dell'agente debba ricomprendere anche la conoscenza delle norme

extrapenali che regolano la materia.

La seconda parte del comma elenca le condotte di importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale e locazione di programmi “pirata”; sono tutte condotte caratterizzate dall’intermediazione tra il produttore della copia abusiva e l’utilizzatore finale.

Infine, nell’ultima parte del comma il legislatore ha inteso inserire una norma volta all’anticipazione della tutela penale, punendo condotte aventi 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.

Sul piano soggettivo, tutte le condotte ora esaminate sono caratterizzate dal dolo specifico del profitto. Nel sostituire il fine di profitto a quello di lucro, nel corso dell’evoluzione normativa della fattispecie *de qua*, il legislatore ha inteso ampliare l’ambito di applicazione della norma, per ricomprendervi anche quei comportamenti che non sono sorretti dallo specifico scopo di conseguire un guadagno di tipo prettamente economico.

La riforma dell’elemento soggettivo non è di poco conto ed ha forti ripercussioni sull’eventuale punibilità degli Enti. In effetti, si può configurare il reato anche qualora, all’interno della Società, vengano usati, a scopi lavorativi, programmi non originali, al solo fine di risparmiare il costo dei software originali.

Nel secondo comma dell’art. 171 bis ad essere tutelate sono invece le banche dati: stando all’art. 2 della stessa legge, tali debbono intendersi le raccolte di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo.

Questo secondo comma deve essere prudentemente considerato da Venis, in considerazione dell’attività svolta, ai sensi della Convenzione del 4 aprile 2006, di gestione delle banche dati del Comune di Venezia, oltre che dei propri *data base* informativi funzionali all’erogazione dei servizi IT sul territorio municipale.

In questi casi si dovrà porre particolare attenzione qualora si voglia offrire a soggetti interessati il servizio di consultazione. Dovrà essere predisposta un procedura ad hoc per questo tipo di attività, procedura che da un lato permetta il trasferimento del materiale ai soggetti interessati, ma che d’altro canto predisponga cautele idonee ad evitare che il materiale, una volta uscito dalla disponibilità esclusiva dell’azienda, circoli senza controllo.

L’**art. 171 ter** tende alla tutela di una serie numerosa di opere dell’ingegno: opere destinate al circuito radiotelevisivo e cinematografico, incorporate in supporti di qualsiasi tipo contenenti fonogrammi e videogrammi di opere musicali, ma anche opere letterarie, scientifiche o didattiche.

Le numerose condotte sanzionate, singolarmente analizzate nella Parte Generale del presente Modello, si inseriscono nell’ottica di ampliamento della tutela del software che il legislatore sembra perseguire negli ultimi anni.

A restringere l’ambito di applicabilità della disposizione, però, vi sono due requisiti. Il primo è che le condotte siano poste in essere per fare un uso non personale dell’opera dell’ingegno, e il secondo è il dolo specifico di lucro, necessario per integrare il fatto tipico.

Ne consegue, che in considerazione dell’attività e dell’oggetto sociale di Venis, il rischio che tale reato possa essere concretamente perpetrato è piuttosto remoto. Ciò nonostante, una successiva evoluzione della vocazione IT della Società ovvero un ampliamento della attività attualmente svolte, quali ad esempio quella di *streaming* audio/video delle sedute collegiali dell’amministrazione del Comune di Venezia, potrebbe portare ad esistenza più concreti rischi di integrazione della fattispecie *de qua*.

Appare inoltre pressoché nullo il rischio che in Venis possano perfezionarsi i reati contemplati dagli artt. 171 septies ed octies, che si analizzano brevemente di seguito soltanto per completezza.

L'**art. 171 septies** è diretto alla tutela delle funzioni di controllo della SIAE, in un'ottica di tutela anticipata del diritto d'autore. Si tratta di un reato di ostacolo che si consuma con la mera violazione dell'obbligo.

Le disposizione estende la pena prevista dal primo comma dell'art. 173 bis ai produttori e agli importatori dei supporti non soggetti al contrassegno SIAE che non comunichino alla SIAE stessa entro trenta giorni dall'importazione o dalla commercializzazione i dati necessari all'univoca identificazione dei supporti medesimi. Il secondo comma punisce invece la falsa comunicazione di tali dati alla SIAE. E' evidente l'intento di accordare una tutela penale alle funzioni di vigilanza delle Autorità preposte al controllo del settore.

La disposizione di cui all'**art. 171 octies** punisce chi, a fini fraudolenti, produce, pone in vendita, promuove, installa, modifica, utilizza per uso pubblico o privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato.

L'articolo, poi, continua definendo ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio. Vale a restringere l'ambito di applicabilità della norma l'elemento soggettivo di perseguimento di fini fraudolenti.

Si può solo notare come in genere tali servizi, soprattutto di istallazione, vengano forniti da artigiani che lavorano in modo autonomo, qualificati come piccoli imprenditori, il che rende pertanto difficile immaginare un reale impatto per Venis in relazione al Decreto.

1.C) FUNZIONI INTERESSATE

Gli ambiti aziendali potenzialmente interessati dalle attività a rischio di commissione dei reati in parola sono stati individuati sulla base dell'Organigramma Venis allegato alla Parte Generale del Presente Modello.

In dettaglio, gli ambiti aziendali interessati ricomprendono:

- la Funzione Tecnologie, Servizi e Sviluppo
- la Funzione Comunicazione

Sono altresì interessati tutti i dirigenti, dipendenti e collaboratori, pur non ricompresi nelle Funzioni sopra elencate, operanti nelle diverse attività e/o fasi del processo precedentemente individuate.

1.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa essenzialmente sugli elementi della **separazione delle funzioni/attività** nelle fasi salienti dei processi e della **tracciabilità**.

- Prevedere che siano fra loro distinti i soggetti che:

  - autorizzano l’immissione in rete di contenuti,
  - eseguono materialmente l’immissione,
  - controllano che il processo sia avvenuto correttamente/controllino l’eventuale presenza di *user-generated contents* immessi da terzi in violazione.

- Prevedere un sistema di deleghe accurato coerente con le responsabilità organizzative e gestionali assegnate.
- Ogni operazione relativa all’immissione in rete di contenuti deve essere adeguatamente registrata per garantirne la tracciabilità.
- Deve esistere un sistema di controllo in grado di segnalare tempestivamente l’insorgere di situazioni di criticità ed anomalie.
- Deve esistere una funzione incaricata della gestione di eventuali segnalazione di terzi o soggetti interessati i cui diritti risultino asseritamente violati.

1.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo.

In particolare, i principi procedurali che devono essere implementati per prevenire la fattispecie di reato considerate sono i seguenti:

- Nell’immissione in rete di contenuti assicurare che ogni tipo di immissione sia inibita elettronicamente, e comunque non operabile in assenza di preventiva o parallela autorizzazione con sistemi di *strong authentication* dai responsabili delle Funzioni Sistemi e Servizi Tecnologici o Funzione Tecnologie, Servizi e Sviluppo;
- Controllo periodico dei contenuti eventualmente immessi negli spazi in gestione da parte di soggetti terzi attraverso sistemi *web 2.0*, nei limiti fisicamente imposti dal decentramento ed eterogeneità dei contenuti;
- Prevedere procedure rapide di eventuali contenuti immessi in violazione delle normative richiamate, sempre previo vaglio del Responsabile di Funzione;
- Prevedere procedure operative ad hoc per la gestione delle banche dati in particolare qualora si voglia offrire a soggetti interessati il sevizio di consultazione;
- Prevedere piani di formazione specifici del personale sui contenuti della legge sul diritto d’autore e sulle modalità corrette di gestione degli spazi sul portale.

1.F) INFORMATIVA VERSO L’ORGANISMO DI VIGILANZA

Le Funzioni aziendali coinvolte dovranno provvedere a comunicare:

a. l’elenco di eventuali controlli/segnalazioni ricevute in merito a violazione di diritti d’autore detenuti da terzi e le relative azioni intraprese.

1.G) DOCUMENTI DI RIFERIMENTO

- Codice etico;
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione.

PARTE QUATTORDICESIMA – INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA

(art. 25 nonies del Decreto)

La Legge 3 agosto 2009, n. 116 (pubblicata sulla G.U. n. 188 del 14 agosto 2009), recante "*Ratifica ed esecuzione della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione, adottata dalla Assemblea generale dell'ONU il 31 ottobre 2003 con risoluzione n. 58/4, firmata dallo Stato italiano il 9 dicembre 2003, nonché norme di adeguamento interno e modifiche al codice penale e al codice di procedura penale*", all'art. 4 introduce nel Decreto l'art. 25 nonies, rubricato "***Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria***".

Il **reato (art. 377 bis c.p.)** si perfeziona laddove chiunque, con violenza o minaccia o offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando la stessa possa avvalersi della facoltà di non rispondere.

La trattazione di tale reato si configura in maniera diversa rispetto allo schema seguito per i reati precedentemente considerati. Invero, per la natura stessa del reato e la peculiarità della condotta, non è possibile procedere né all'individuazione di specifici meccanismi di controllo né alla previsione di indicazioni comportamentali in modalità preventiva. Allo stesso modo non è possibile e non avrebbe senso in relazione alla *ratio* del Decreto prevedere flussi informativi nei confronti dell'Organismo di Vigilanza.

Le funzioni interessate, invece, se non altro con riferimento al soggetto attivo del reato, possono essere tutte le funzioni aziendali.

Con attenzione alla tipologia di reato in esame, pertanto, appare opportuno procedere soltanto alla formulazione delle seguenti brevi osservazioni.

Preliminarmente va precisato che soggetto attivo può essere chiunque, mentre il destinatario della condotta può essere soltanto chi ha la facoltà di non rispondere in un processo penale, ossia l'indagato o l'imputato, nell'unico processo oppure in un procedimento connesso.

La differenza tra tale reato e la c.d. subornazione consiste nella circostanza che in quella condotta il *subornato* non ha realizzato il reato cui tendeva il "*subornatore*" e, inoltre, nel reato di subornazione non è prevista né la violenza né la minaccia come modalità della condotta.

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

A titolo di mero esempio, nella ipotesi che vengano indagati l'Amministratore Delegato ed in concorso il Responsabile Amministrativo per reati societari o altri reati commessi nell'ambito della propria attività o ruolo all'interno dell'azienda, il reato potrebbe configurarsi qualora il primo, con violenza o minaccia, o con promessa

di denaro o altre utilità, induca il secondo a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria.

PARTE QUINDICESIMA – I REATI AMBIENTALI

(art. 25-undecies del Decreto)

Con l'introduzione nel D. Lgs. 231/2001 del nuovo art. 25-*undecies*, la responsabilità amministrativa degli Enti è stata estesa ad alcuni reati ambientali, dettagliatamente descritti nella PARTE GENERALE del presente Modello. Il regime di responsabilità degli Enti collettivi in relazione alla commissione dei reati ambientali di cui al nuovo **art. 25 *undecies*** riguarda sia alcune figure di reato già previste dall'ordinamento penale, che due nuove fattispecie introdotte dalla indicata novella (nuovi articoli 727 *bis* e 733 *bis* c.p.).

Con gli ultimi provvedimenti normativi, recepiti nel nostro ordinamento con il D. Lgs. 7 luglio 2011, n. 121, il legislatore comunitario ha ritenuto opportuno introdurre un ulteriore strumento per garantire una maggiore protezione dell'ambiente, colpendo quelle organizzazioni che, con dolo o per grave negligenza, con comportamenti illeciti posti in essere nel loro interesse o vantaggio, possono creare danni anche irreversibili alle persone ed alle risorse naturali.

Gli eco-reati previsti dal D. Lgs. 231/2001 implicano la responsabilità delle persone giuridiche laddove siano commessi a vantaggio dell'Ente da chi detenga una posizione preminente in seno alla propria organizzazione:

- sia in forza di formale potere di rappresentanza,
- sia in presenza della sostanziale capacità decisionale e di controllo,
- ovvero ancora, in quanto la carenza di sorveglianza o controllo da parte di tali soggetti sui propri sottoposti abbia reso possibile la commissione del reato da parte di questi ultimi.

L'omissione delle previste doverose cautele organizzative e gestionali idonee a prevenire tali tipologie criminose, si configura pertanto come una colpa organizzativa che vede coinvolta la struttura interna dell'impresa, i rapporti di gestione ed i vincoli di dipendenza gerarchica.

In tale contesto, si discute della possibilità per le aziende in possesso di sistemi di gestione ambientale conformi agli standard internazionali, di veder riconosciuta (analogamente a quanto già previsto in tema di sicurezza dall'art. 30 del T.U.[20]) la conformità del modello organizzativo, per le parti corrispondenti, alla prevenzione dei reati ambientali. Ci si riferisce, in particolare, alle organizzazioni dotate di un Sistema di gestione Ambientale certificato ISO 14001 da un verificatore accreditato Accredia o registrate secondo il Regolamento EMAS.

Tali imprese, potrebbero trovare minori difficoltà e criticità nella prevenzione dei reati e nell'adozione del Modello, avendo già predisposto l'organizzazione aziendale interna secondo i principi contenuti nella norma EMAS o nello standard ISO 14001, che prevedono l'individuazione degli aspetti ambientali e delle leggi applicabili, la chiara definizione di ruoli e responsabilità, il miglioramento della competenza del personale, la documentazione dell'attività svolta ed il controllo e rispetto delle procedure aziendali

La conformità dei modelli di organizzazione ai codici di comportamento delle associazioni di categoria di cui all'art. 6 del Decreto e l'adozione di sistemi di gestione ambientali interni, potranno essere, pertanto, sicuramente viste con favore.

[20] In base al comma 5 dell'art. 30 del D. Lgs. 81/2008 "*in sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee Guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti. Agli stessi fini ulteriori modelli di organizzazione e gestione aziendale possono essere indicati dalla commissione di cui all'art. 6*"

Tuttavia, occorre segnalare che tale conformità non potrà essere considerata equivalente né sostitutiva della progettazione e successiva esecuzione di un modello organizzativo conforme ai principi del Decreto, in quanto il sistema di gestione ambientale dovrà essere integrato con quanto richiesto dal Decreto agli art.li 6 e 7. Questo significa prevedere un coordinamento tra la politica ambientale aziendale ed il codice etico aziendale, l’introduzione ed integrazione con il sistema dell’OdV e l’attribuzione dei relativi poteri di controllo[21] - la presenza dell’Organismo avrà certo un peso nella programmazione delle verifiche interne ed in sede di riesame del sistema stesso - nonché la progettazione di specifici flussi informativi in entrata ed in uscita dello stesso Organismo e l’introduzione nel sistema disciplinare di riferimenti specifici alla violazione delle norme di carattere ambientale adottate dall’organizzazione.

Nel D. Lgs. 231/2001 sono stati inseriti ben diciassette reati ambientali, provenienti da fonti normative assai eterogenee: il codice penale (art. 727-bis e 733-bis), la Convenzione di Washington, il D. Lgs. 152/2006 (Norme in materia ambientale), la L. 549/1993 (misure a tutela dell’ozono stratosferico e dell’ambiente) e il D. Lgs. 202/2007 (Attuazione della direttiva 2005/35/CE relativa all’inquinamento provocato dalle navi e conseguenti sanzioni), tutti già individuati e descritti nella Parte Generale del presente Modello. In questa sede ci limitiamo quindi a richiamarne brevemente il contenuto, per poi passare ad evidenziare le aree a maggior rischio per Venis ed i reati eventualmente al suo interno ipotizzabili:

- l’uccisione, la distruzione, il prelievo o possesso, di esemplari di specie animali o vegetali selvatiche protette o il danneggiamento di un habitat all’interno di un sito protetto;
- l’esercizio di una attività industriale ad alto impatto ambientale senza Autorizzazione Integrata Ambientale;
- lo scarico di acque reflue industriali, senza autorizzazione e/o lo scarico di acque reflue industriali inquinanti;
- gli illeciti nella gestione dei servizi idrici integrati, commessi dai gestori di tali servizi in materia di trattamento delle acque reflue;
- lo scarico nelle acque del mare da parte di navi od aeromobili di sostanze o materiali per i quali è imposto il divieto assoluto di sversamento ai sensi delle disposizioni contenute nelle convenzioni internazionali vigenti in materia e ratificate dall’Italia;
- l’utilizzazione agronomica di effluenti di allevamento, di acque di vegetazione dei frantoi oleari, nonché di acque reflue provenienti da aziende agricole e piccole aziende agroalimentari senza preventiva autorizzazione;
- l’importazione, l’esportazione, la riesportazione, la vendita e il trasporto, anche per conto terzi, di specie animali e vegetali in via di estinzione o l’importazione di oggetti ad uso personale o domestico relativi a tali specie;
- la falsificazione o alterazione di certificati, licenze, notifiche di importazione, dichiarazioni, comunicazioni, finalizzati all’importazione o alla vendita di specie animali e vegetali in via di estinzione;

[21] Come previsto dall’art. 6 del Decreto, per godere dell’esimente è necessario definire adeguati poteri e risorse anche in capo all’Organismo di Vigilanza, prevedendo ad esempio l’inserimento nell’organico di una persona dotata di particolari competenze in cambio ambientale, oltre che adeguati e specifici flussi informativi nei confronti dello stesso e la possibilità, per l’OdV medesimo, di eseguire verifiche sull’efficienza del modello nella prevenzione dei reati ambientali, coordinandole con eventuali altre verifiche periodiche pianificate dalla direzione aziendale per la valutazione dell’efficacia del modello.

- la detenzione di esemplari vivi di mammiferi e rettili di specie selvatica ed esemplari vivi di mammiferi e rettili provenienti da riproduzioni in cattività che costituiscano pericolo per la salute e per l'incolumità pubblica;
- la violazione delle norme relative alla produzione, il consumo, l'importazione, l'esportazione, la detenzione, la raccolta, il riciclo e la commercializzazione delle sostanze lesive dell'ozono stratosferico e dannose per l'ambiente;
- l'inquinamento doloso e colposo dei mari;
- attività per il traffico illecito di rifiuti.

Soggetti attivi delle condotte in questione possono essere, ciascuno in relazione al proprio ambito di competenza e responsabilità e con riferimento, pertanto, alle regole ed alle prescrizioni in materia di tutela dell'ambiente e prevenzione dell'inquinamento che sono a ciascuno specificamente indirizzate:

a) i soggetti tenuti a far osservare le norme di natura ambientale, ovverosia, tutti coloro che, nell'ambito dell'organizzazione aziendale, in forza di quanto previsto dall'organigramma e dal sistema di deleghe in essere, risultino titolari dei poteri decisionali e di spesa idonei a garantire l'attuazione ed il rispetto delle norme in materia di prevenzione di reati ambientali;

b) coloro che rivestono gli specifici ruoli di controllo tecnico-operativo nell'ambito della Società, in ottemperanza con quanto previsto dal Protocollo di comportamento;

c) gli ulteriori i soggetti coinvolti nei processi operativi segnalati tenuti ad osservare le richiamate norme.

Considerato l'oggetto sociale di Venis e l'attività anche cantieristica che la stessa svolge, il rischio che al suo interno possano essere perpetrati tali reati non è affatto escludibile

Di seguito, sono elencate le aree di attività maggiormente "a rischio" per Venis e le eventuali modalità attuative dei reati.

AREE A RISCHIO

Con riferimento all'analisi delle specifiche attività aziendali a rischio si segnalano fondamentalmente i processi operativi relativi alla gestione e al trattamento dei rifiuti, con attenzione anche a sostanze/scarti pericolosi e/o radioattivi, tenendo conto che in alcuni casi il produttore dei rifiuti può essere ritenuto corresponsabile di una illecita gestione dei rifiuti posta in essere da parte di aziende terze.

1) "GESTIONE E TRATTAMENTO DEI RIFIUTI, ANCHE SOSTANZE/SCARTI PERICOLOSI E/O RADIOATTIVI"

1.A) DESCRIZIONE DEL PROCESSO

Il processo si riferisce a tutte le attività svolte dalle Funzioni aziendali preposte alla gestione e trattamento dei rifiuti/scarti aziendali, ivi comprese sostanze pericolose e/o radioattive.

1.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Attività di **gestione rifiuti non autorizzata**, bonifica dei siti traffico illecito di rifiuti, sistema informatico di controllo della tracciabilità dei rifiuti (art. 256, 257, 259, 260 *bis* T.U. dell'ambiente – D.Lgs. 152/2006).

Meritano un particolare approfondimento due categorie di reati, con riferimento ai quali, la possibilità che essi vengano perpetrati all'interno dell'azienda non può essere esclusa.

Il reato di **gestione di rifiuti non autorizzata** si configura qualora venga perpetrata un'attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della autorizzazione, iscrizione o comunicazione prescritta dagli articoli 208 e seguenti del decreto.

Il problema nasce dal fatto che, in alcuni casi il produttore dei rifiuti può essere ritenuto corresponsabile di una illecita gestione dei rifiuti posta in essere da parte di aziende terze.

In tema di gestione dei rifiuti, la recente giurisprudenza (Cass. Penale Sez. III, 15 giugno 2011 Sent. N. 23971) ha infatti stabilito che le responsabilità per la sua corretta effettuazione, in relazione alle disposizioni nazionali e comunitarie gravano su tutti i soggetti coinvolti nella produzione, distribuzione, utilizzo e consumo dei beni dai quali originano i rifiuti stessi, e le stesse si configurano anche a livello di semplice istigazione, determinazione, rafforzamento o facilitazione nella realizzazione degli illeciti. La responsabilità dei detentori e/o produttori di rifiuti si configura quindi anche quando costoro si siano resi responsabili di comportamenti materiali o psicologici tali da determinare una compartecipazione, anche a livello di semplice facilitazione, negli illeciti commessi dai soggetti dediti alla gestione dei rifiuti.

L'articolo 256 del T.U. sanziona altresì, al comma terzo, la condotta di chi realizza o gestisce una discarica non autorizzata, prevedendo un aggravamento della pena nel caso in cui la discarica sia destinata, anche in parte, allo smaltimento di rifiuti pericolosi.

In tal senso, il reato potrebbe essere integrato anche qualora lo smaltimento dei rifiuti aziendali, anche non pericolosi, venisse effettuato in maniera difforme alle prescrizioni legislative e regolamentari applicabili.

L'art. 256 sanziona espressamente anche la condotta di chiunque, in violazione del divieto di cui all'articolo 187 del decreto medesimo, effettua attività non consentite di miscelazione di rifiuti.

La giurisprudenza ha inoltre precisato, che il reato di gestione non autorizzata di rifiuti è configurabile anche laddove il detentore di un rifiuto se ne disfi sottoponendolo ad operazioni di recupero, non sussistendo, nel caso specifico, le condizioni per l'applicazione della disciplina derogatoria prevista per le materie prime secondarie e per i sottoprodotti.

Occorre inoltre segnalare che la recente reintroduzione del SISTRI (Sistema di Tracciabilità dei Rifiuti pericolosi e speciali) in via obbligatoria per particolari tipologie di aziende, tra cui Venis, rende certamente ipotizzabile, se non altro in linea di principio, un ulteriore reato, quale il mancato rispetto degli adempimenti relativi al sistema informatico di controllo della tracciabilità dei rifiuti (Art. 260 bis T.U.).

L'effettiva operatività del Sistema di tracciabilità dei rifiuti è stata oggetto di diverse proroghe che si sono susseguite, ultima quella prevista dall'art. 52 del D.L. 83/2012, convertito il 7 agosto senza modifiche in L. 134/20012, il quale ha sospeso il termine di operatività del SISTRI fino al compimento delle verifiche di funzionalità del sistema stesso e comunque non oltre il 30 giugno 2013, insieme ad ogni adempimento informatico connesso.

Nel merito, al fine di comprendere meglio la nuova disciplina, occorre necessariamente chiarire alcuni principi sanciti dall'art. 184 del D. Lgs. 152/06, il quale distingue preliminarmente i rifiuti, secondo la loro origine, in due macro-categorie: (i) rifiuti urbani e (ii) rifiuti speciali.

Secondo le caratteristiche di pericolosità gli stessi rifiuti sono poi distinti in: (i) rifiuti pericolosi e (ii) rifiuti non pericolosi.

I rifiuti urbani e speciali, pericolosi e non, a loro volta sono classificati secondo la loro destinazione finale: (i) non riutilizzabili, da avviare necessariamente a smaltimento, e (ii) riutilizzabili, da avviare a smaltimento o a recupero nei cicli produttivi, secondo i casi.

L’articolo 182 del D.lgs 152/06 chiarisce inoltre che lo smaltimento dei rifiuti è da considerarsi come soluzione residuale, nel caso non esistano alternative tecnicamente valide o economicamente sostenibili che ne consentano il recupero. Tutti i rifiuti sono identificati da un codice a 6 cifre.

L’elenco dei codici identificativi (denominato C.E.R. 2002 e allegato alla parte quarta del D. Lgs. 152/06) è articolato in 20 classi, a seconda del ciclo produttivo che ha dato origine al rifiuto.

All’interno dell’elenco, alcune tipologie di rifiuti sono classificate come pericolose o non pericolose fin dall’origine, mentre per altre la pericolosità dipende dalla concentrazione di sostanze pericolose contenute. I rifiuti pericolosi sono contrassegnati nell’elenco da un asterisco.

All’interno di tale elenco sono ovviamente ricompresi anche i rifiuti prodotti nell’ambito delle attività di ufficio, le cui principali tipologie sono:

- toner, cartucce per stampanti laser, cartucce per stampanti a getto d’inchiostro, nastri per stampanti ad impatto esausti etc., classificati come rifiuti speciali, non pericolosi e pericolosi, a seconda delle loro caratteristiche;
- tubi catodici (lampade al neon) guasti, lampade a risparmio energetico, classificati sempre come rifiuti speciali pericolosi;
- rifiuti di apparecchiature elettriche ed elettroniche obsolete o RAEE (computer, stampanti, fotocopiatrici, centralini telefonici, monitor, video etc.), sono rifiuti speciali, non pericolosi e pericolosi;
- filtri provenienti da impianti di condizionamento e fancoil, classificati sempre come rifiuti speciali pericolosi;
- pile ed accumulatori (batterie alcaline, batterie da cellulari, etc.), sono rifiuti speciali, non pericolosi e pericolosi;
- carta e archivi cartacei, sono rifiuti speciali non pericolosi.

I **codici C.E.R.** coi quali vengono classificati tali rifiuti (parte quarta del D. Lgs. 152/06) sono i seguenti.

- Toner, cartucce e nastri:
  - 08 03 18 rifiuto speciale non pericoloso;
  - 08 03 17 rifiuto speciale pericoloso, se destinato allo smaltimento; 16 02 16 se destinato al recupero.

  (Si segnala che in precedenza era possibile classificare tali rifiuti con i codici C.E.R. 15 01 02, 15 01 04, 15 01 06 relativi agli imballaggi, tuttavia il D.M. n. 186 del 5 Aprile 2006 ha sancito (andando a modificare il punto 13.20 del D.M. 05/05/98) che i codici C.E.R. corretti per classificare e destinare tali materiale alle operazioni di recupero, sono appunto i C.E.R. 08 03 18 e 16 02 16).

- Tubi catodici e lampade a risparmio energetico:
    - 20.01.21 rifiuti speciali pericolosi.
- Rifiuti da apparecchiature elettriche ed elettroniche obsolete:
    - 16 02 14 rifiuto speciale non pericoloso;
    - 16 02 13 rifiuto speciale pericoloso.
- Filtri da impianti di aerazione:
    - 15 02 02 rifiuti speciali pericolosi.
- Pile ed accumulatori:
    - 16 06 04 rifiuto speciale non pericoloso;
    - 16 06 01/02/03 rifiuti speciali pericolosi.
- Carta:
    - 15 01 01 rifiuto speciale non pericoloso;
    - 20 01 01 rifiuto urbano.

Ai sensi della normativa vigente, le tipologie di rifiuti sopra indicate non sono assimilabili ai rifiuti urbani e pertanto non possono essere destinati alle comuni discariche, ma devono essere gestiti in modo separato tramite operatori espressamente autorizzati dalle autorità competenti, siano essi società di trasporto oppure di smaltimento.

Occorre inoltre ricordare sempre che la legge, e più specificamente l’art. 183 del D. Lgs. 152/06, obbliga i produttori a smaltire i rifiuti prodotti entro il termine massimo di un anno, a prescindere dal quantitativo e dalla loro pericolosità.

Sulla base della classificazione che precede e considerato che ai sensi dell’art. 188 ter D. Lgs. 152/2006 sono tenuti ad aderire al sistema di controllo della tracciabilità dei rifiuti (SISTRI) sia gli enti e le imprese produttori di rifiuti speciali pericolosi, sia le imprese e gli enti produttori di rifiuti speciali non pericolosi derivanti da lavorazioni industriali qualora abbiano più di dieci dipendenti, Venis è da ritenersi compresa tra le aziende che devono aderire al sistema di tracciabilità dei rifiuti.

Pertanto Venis ha provveduto all’iscrizione al SISTRI (in data 1 marzo 2010, pratica n. WEB_VE 32486) non potendosi oltretutto escludere che essa possa incorrere in responsabilità amministrativa ai sensi del D. Lgs. 231/2001 per omissione di ulteriori attività previste a corollario dell’iscrizione medesima.

La condotta tipica del reato è infatti estesa a chi fornisca al suddetto sistema informazioni incomplete o inesatte, alterando fraudolentemente uno qualunque dei dispositivi tecnologici accessori al predetto sistema informatico di controllo, o comunque impedendone in qualsiasi modo il corretto funzionamento.
Se le indicazioni riportate, pur incomplete o inesatte, non pregiudicano la tracciabilità dei rifiuti è prevista una riduzione delle sanzioni.

Il quarto comma dell'art. 260 *bis* prevede inoltre la sanzione amministrativa accessoria della sospensione da un mese a un anno dalla carica rivestita dal soggetto cui l'infrazione è imputabile, ivi compresa la sospensione dalla carica di amministratore.

Il comma cinque contiene infine una norma di chiusura, sanzionando la condotta di coloro che, al di fuori di quanto previsto nei commi precedenti, si rendono inadempienti agli ulteriori obblighi su di loro incombenti ai sensi del predetto sistema di controllo della tracciabilità dei rifiuti (SISTRI).

Per i reati in esame, non è necessariamente richiesto l'elemento psicologico del dolo, essendo sufficiente, per la loro realizzazione, la colpa organizzativa dell'azienda, che può essere intesa anche come grave negligenza, da parte dei soggetti dotati di poteri formali o sostanziali (cd. soggetti apicali), nel pianificare procedure e forme specifiche di controllo del rispetto degli obblighi di legge sui propri sottoposti che abbiano eventualmente commesso il reato.

1.C) FUNZIONI INTERESSATE

Da un punto di vista funzionale, gli ambiti aziendali potenzialmente interessati dalle attività a rischio di commissione del reato in esame sono stati individuati sulla base dell'Organigramma Funzionale di Venis allegato alla Parte Generale del Presente Modello.

Essi ricomprendono:

- Organo Amministrativo (anche in generale per l'obbligo giuridico di controllo della gestione della società, del cui operato sono direttamente responsabili ex lege ai sensi dell'art. 2392 c.c.);
- Direzione Coordinamento Generale;
- Tecnologie, Servizi e Sviluppo.

Sono altresì interessati tutti i dirigenti, dipendenti e collaboratori, pur non ricompresi nelle Funzioni sopra elencate, operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

1.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa sugli elementi della **tracciabilità delle fasi del processo** e del **sistema di deleghe** in materia definite a livello organizzativo.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati:

- definizione e aggiornamento di un sistema di deleghe ad *hoc* e specifici criteri autorizzativi;
- definizione e aggiornamento di un sistema di procedure aziendali specifiche e previsione di periodiche verifiche dell'effettiva applicazione e dell'efficacia delle procedure adottate;
- verifica delle autorizzazioni dei soggetti a cui si decide di affidare i propri rifiuti;
- corretta gestione dei formulari e delle comunicazioni obbligatorie agli enti nei tempi previsti dalla legge;

- previsione di sistemi di verifica del rispetto dei canoni di integrità, trasparenza e correttezza del processo con particolare riguardo alla tracciabilità delle varie fasi di gestione e smaltimento dei rifiuti, nonché ai tempi e alle risorse impiegate;

- periodiche verifiche dell'acquisizione di documentazioni e certificazioni obbligatorie per legge e definizione di specifici criteri di conservazione e archiviazione delle stesse;

- definizione di idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui alla presente elencazione;

- previsione di adeguati meccanismi di gestione delle deroghe a quanto sopra esposto

1.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo.
In particolare:

- è necessario prevedere specifiche modalità di gestione delle comunicazioni con l'esterno, soprattutto con le Autorità di Vigilanza in materia ambientale.

- è necessario che siano conosciuti e scadenzati gli obblighi di comunicazione previsti per legge e prevedere specifiche modalità di archiviazione dei flussi documentali fra le aree della Società interessate e gli organi della Pubblica Amministrazione deputati al rilascio di autorizzazioni e/o all'effettuazione di ispezioni e verifiche in materia di regolare smaltimento dei rifiuti;

- è necessario prevedere periodiche revisioni interne dei metodi di raccolta, stoccaggio e separazione dei rifiuti;

- è fondamentale il coinvolgimento delle varie aree aziendali nell'implementazione del modello con particolare riferimento alle cautele da adottare per la raccolta, stoccaggio e separazione dei rifiuti, mediante attività di informazione e formazione dei lavoratori;

- è necessaria la previsione di strumenti per valutare l'efficacia della formazione erogata ed il trasferimento sul lavoro delle competenze trasmesse ai dipendenti, in maniera da poter intervenire in caso di eventuali mancanze;

- definizione di un sistema di incentivazione del personale legato alla corretta esecuzione degli adempimenti richiesti in materia di raccolta, separazione e stoccaggio dei rifiuti;

- previsione di reporting, preferibilmente procedimentalizzati, che consentano di ricostruire il percorso delle sostanze di scarto/rifiuti fino al completo smaltimento.

1.F) INFORMATIVA VERSO L'ORGANISMO DI VIGILANZA

Il Responsabile della Funzione Generali Finanza, Bilancio e Amministrazione del Personale deve inviare all'Organismo di Vigilanza, per quanto di competenza, anche avvalendosi di personale sottoposto e della collaborazione dei dirigenti e/o dipendenti di altre Funzioni aziendali, quanto segue:

a. elenco delle comunicazioni effettuate agli enti a norma di legge

b. elenco delle documentazioni e certificazioni obbligatorie richieste ed ottenute per legge

c. esito di eventuali controlli da parte di Autorità di Vigilanza.

In ogni caso, all’OdV è riservata la possibilità di eseguire liberamente verifiche sull’efficienza del modello nella prevenzione dei reati ambientali, accedendo alla documentazione all’uopo necessaria, coordinandole con eventuali altre verifiche periodiche pianificate dalla direzione aziendale per la valutazione dell’efficacia del Modello.

1.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico;
- Principi di Comportamento Generali e nei Rapporti con la Pubblica Amministrazione.

PARTE SEDICESIMA – IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE

(art. 25-duodecies del Decreto)

Con il Decreto Legislativo del 16 luglio 2012 n. 109, in vigore dal 9 agosto 2012 (cd. decreto immigrazione), il legislatore ha dato attuazione alla direttiva 2009/52/CE ampliando il novero dei reati-presupposto di cui al D. Lgs. 231/2001. In base all'art. 2 del D. Lgs. 109 del 2012, la responsabilità ex D.Lgs 231/2001 è stata estesa anche alle fattispecie penali disciplinate dall'art. 22, comma 12 bis del D. Lgs. 286/2008 (cd. testo Unico sull'immigrazione), per il tramite dell'introduzione nel D. Lgs. 231/2001 dell'art. 25-duodecies. L'art. 25-duodecies prevede, segnatamente, in relazione alla commissione del delitto di cui all'art. 22, comma 12 bis, la sanzione pecuniaria da 100 a 200 quote, entro il limite di 150.000 Euro. La fattispecie riguarda i datori di lavoro che impiegano lavoratori stranieri privi del permesso di soggiorno o lavoratori il cui permesso sia scaduto (e di cui non sia stato chiesto il rinnovo nei termini di legge), o ancora revocato o annullato. In tal caso, ai sensi del suddetto art. 22, il datore di lavoro è punito con la reclusione da 6 mesi a 3 anni e con la sanzione pecuniaria di Euro 5000 per ogni lavoratore impiegato. Il richiamo esplicito dell'art. 25-duodecies all'art. 12 bis, peraltro modificato dallo stesso D. Lgs. 109/2012, il quale ha aumentato le pene per il datore di lavoro sopra indicate da un terzo alla metà, limita la responsabilità dell'Ente alle sole ipotesi aggravate in cui:

- i lavoratori occupati siano superiori a tre;
- i lavoratori occupati siano minori in età non lavorativa;
- i lavoratori occupati siano sottoposti alle condizioni lavorative di particolare sfruttamento e pericolo di cui al terzo comma dell'art. 603-bis del Codice Penale (Intermediazione illecita e sfruttamento del lavoro).

Al datore di lavoro (e di conseguenza all'Ente) è stata concessa, tuttavia, la possibilità di avvalersi di una procedura transitoria prevista dall'art. 5 del D.Lgs. 109/2012, in vigore dal 15 settembre al 15 ottobre 2012. I datori di lavoro che, alla data di entrata in vigore del Decreto, abbiano in tal senso occupato irregolarmente da almeno tre mesi lavoratori stranieri, hanno potuto usufruire della possibilità di dichiarare la sussistenza del rapporto di lavoro allo sportello unico per l'immigrazione, ed in siffatte ipotesi, i procedimenti penali ed amministrativi nei confronti del datore di lavoro e dell'Ente interessato sono risultati sospesi sino alla conclusione del procedimento di rilascio del contratto di soggiorno.

Con particolare riferimento alle modalità d'impiego e d'assunzione del personale adottate in Venis ed in considerazione del tipo di attività svolta nonché delle cautele assunte nelle procedure di selezione ed assunzione del personale, oltre evidentemente ai principi condivisi e fatti propri dal personale di ruolo, espressi e cristallizzati nel Codice Etico, il rischio che tali reati possano realizzarsi appare assai remoto anche se non escludibile.

AREE A RISCHIO

Con riferimento all'analisi delle specifiche attività aziendali a rischio occorre sicuramente segnalare i soggetti apicali dell'Ente, preposti alla formale assunzione di personale, ma anche coloro che procedono direttamente all'assunzione dei lavoratori privi di permesso di soggiorno, quali la Funzione Finaza, Bilanzio e Amministrazione del Personale, oltre a colui il quale si avvalga delle loro prestazioni tenendoli alle proprie dipendenze (ovvero colui che ricopre la funzione di "datore di lavoro").

1) "IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE"

1.A) DESCRIZIONE DEL PROCESSO

I processi sopra considerati comprendono le attività di selezione, nonché tutte le attività accessorie necessarie alla costituzione del rapporto di lavoro con cittadini membri di Paesi terzi.

1.B) REATI IPOTIZZABILI E MODALITÀ ATTUATIVE

Delitto di cui all'articolo 22 (**Lavoro subordinato a tempo determinato e indeterminato**), comma 12-*bis*, del decreto legislativo 25 luglio 1998, n. 286 (**Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero**)

La condotta tipica del reato è quella del datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal medesimo articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto il rinnovo, o ancora il cui permesso sia stato revocato o annullato, soltanto nelle ipotesi aggravate in cui le pene sono aumentate da un terzo alla metà, ovvero:

a) se i lavoratori occupati sono in numero superiore a tre;

b) se i lavoratori occupati sono minori in età non lavorativa;

c) se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-*bis* del codice penale.

Trattasi di un reato di natura permanente, in quanto la norma incriminatrice attribuisce rilievo all'effettivo svolgimento della prestazione lavorativa piuttosto che al momento della costituzione del rapporto. Anche ai fini della individuazione del luogo di consumazione del reato, deve aversi riguardo all'effettivo svolgimento della prestazione lavorativa piuttosto che al momento di costituzione del rapporto, tenuto conto che la condizione di illegalità dei lavoratori non consente la formalizzazione di un regolare rapporto di lavoro.

Coerentemente ai canoni ermeneutici tipici del sistema di responsabilità ex D.Lgs. 231/2001, anche il reato in esame deve essere commesso nell'interesse o a vantaggio dell'ente.

La giurisprudenza ha avuto modo di segnalare, inoltre, che la responsabilità del datore di lavoro per il reato di occupazione alle proprie dipendenze di lavoratori stranieri privi del permesso di soggiorno, non è esclusa a fronte di una situazione di irregolare presenza sul territorio dello Stato, dal fatto che questo adduca circostanze diverse, che è comunque onere del datore di lavoro verificare (Cass. Pen Sez. I, sent. n. 25990 del 17-06-2010).

Da ultimo, occorre evidenziare, che è soggetto attivo del reato non soltanto colui che procede all'assunzione di detti lavoratori, ma anche colui che, pur non avendo provveduto direttamente all'assunzione, se ne avvalga tenendoli alle sue dipendenze (Cass. Pen. Sez. I, sent. n. 25615 del 18-05-2011).

1.C) FUNZIONI INTERESSATE

Gli ambiti aziendali potenzialmente interessati dalle attività a rischio di commissione dei reati in parola sono stati individuati sulla base dell'Organigramma Funzionale di Venis allegato alla Parte Generale del Presente Modello.

Esse ricomprendono:

- l'Organo Amministrativo

- la Direzione Coordinamento Generale
- la Funzione Comunicazione, Sviluppo Personale e Qualità
- la Funzione Tecnologie, Servizi e Sviluppo

Sono altresì interessati tutti i dirigenti e dipendenti, pur non ricompresi nelle Funzioni sopra elencate operanti nelle diverse attività e/o fasi dei processi precedentemente individuate.

1.D) SISTEMA DI CONTROLLO

Il sistema di controllo si basa, sia nelle fasi di selezione che di assunzione, sugli elementi qualificanti della **tracciabilità** e della puntuale **registrazione della documentazione**.

Le modalità di accesso all’impiego e di svolgimento effettivo dell’attività lavorativa in Venis, sono improntate, in generale, a criteri di trasparenza delle procedure, idonei a garantire ed a consentire la verifica, in ogni fase applicativa, del pieno rispetto delle leggi vigenti e dei principi e delle regole generali del presente Modello.

La documentazione raccolta nelle fasi prodromiche all’assunzione deve essere idonea a dare evidenza dei criteri e delle modalità adottate nella selezione delle risorse umane da acquisire; criteri e modalità in ogni caso resi noti prima del processo di selezione.

In questa cornice, in cui si inquadra la politica generale delle assunzioni di Venis, l’unico elemento specifico di controllo aggiuntivo, nel caso di assunzione di lavoratori provenienti da Paesi terzi, deve essere rappresentato, in sede di sottoscrizione della lettera di assunzione e/o lettera impegnativa di assunzione, dalla verifica dell’esistenza, tra la documentazione raccolta, di regolare permesso di soggiorno.

1.E) PROTOCOLLO COMPORTAMENTALE

Non adottare comportamenti a rischio di reato e/o contrari al Presente Modello, al Codice Etico e al Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione, in tutte le fasi del processo. Inoltre:

- integrare le policy aziendali dirette alla selezione ed assunzione del personale mediante l’esplicita previsione:
  - del divieto di occupare lavoratori stranieri privi del permesso di soggiorno;
  - di flussi informativi continui e costanti verso il “datore di lavoro”.
- Inserire nei contratti con i terzi apposite clausole che garantiscano il rispetto di tali principi anche da parte dei fornitori, soprattutto nel caso in cui l’Azienda stessa faccia ricorso al lavoro interinale mediante le agenzie specializzate.

1.F) INFORMATIVA VERSO L’ORGANISMO DI VIGILANZA

Il Responsabile della Funzione Gestione Risorse Umane deve inviare all’Organismo di Vigilanza, per quanto di competenza, quanto segue:

a. elenco delle assunzioni di lavoratori provenienti da Paesi terzi effettuate.

1.G) DOCUMENTI DI RIFERIMENTO

- Codice Etico
- Protocollo di Comportamento Generale e nei Rapporti con la Pubblica Amministrazione
- Regolamento in materia di Reclutamento e Selezione del Personale
- Flusso Assunzione del Personale (VAQ-AQ-FG-10)

PARTE DICIASSETTESIMA – I REATI TRANSNAZIONALI

(Legge 16 marzo 2006, n. 146)

La Legge 16 marzo 2006, n. 146 di Ratifica ed Esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea Generale il 15 novembre 2000 e il 31 maggio 2001, come modificata dal Decreto Legislativo 21 novembre 2007, n. 231 in materia di riciclaggio, ha esteso la responsabilità amministrativa delle società anche alla criminalità internazionale nel caso di commissione di determinati reati. Si tratta segnatamente dei reati di:

- **Associazione per delinquere**
- **Associazione di tipo mafioso**
- **Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri**
- **Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope**
- **Favoreggiamento dell'immigrazione clandestina**
- **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria**
- **Favoreggiamento personale**.

E' il caso di segnalare che il D. Lgs. n. 231/2007 in materia di riciclaggio è intervenuto sulla disciplina della Legge 146/2006 abrogando i commi 5 e 6 dell'art. 10 della stessa legge che limitava l'ambito della responsabilità amministrativa degli Enti per i reati di riciclaggio ed impiego di denaro beni e utilità di provenienza illecita alle sole ipotesi in cui i reati medesimi presentassero il carattere della transnazionalità. A seguito di tale abrogazione, oggi, i reati suddetti rientrano nella disciplina della responsabilità amministrativa a prescindere dal carattere di transnazionalità del reato.

La valenza transnazionale dei reati in questione limita molto il loro ambito di concreta configurazione. In effetti, perché presentino il carattere della transnazionalità i reati in esame debbono essere puniti con la pena della reclusione non inferiore nel massimo a quattro anni, aver comportato il coinvolgimento di un gruppo criminale organizzato, essere commessi in più di uno Stato oppure in un solo Stato se una parte sostanziale della preparazione, pianificazione, direzione o controllo del crimine sia però avvenuta in un altro Stato, ovvero essere commessi in uno Stato se in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato, o essere commessi in uno Stato, ma con effetti sostanziali in un altro Stato.

In considerazione dell'attività svolta da Venis e del suo oggetto sociale, tenuto conto del fatto che la stessa Venis non svolge attività con controparti estere (da intendersi come cittadini o residenti in altri Stati e soggetti con sede all'estero, né peraltro ciò appare consentito per la Società dal disposto dell'art. 13 del Decreto Legge 4 luglio 2006, n. 223, s.m.i., c.d. "Decreto Bersani"), nonché del fatto che, affinché le descritte fattispecie criminose siano rilevanti, oltre ad avere una valenza transnazionale debbono anche essere poste in essere nell'interesse o a vantaggio della Società stessa (interesse o vantaggio che sarebbe difficile immaginare con riferimento alla vocazione di Venis), il rischio che in Venis tali reati vengano concretamente perpetrati è da ritenersi improbabile.

PARTE DICIOTTESIMA – OPERAZIONI PROMANATE DIRETTAMENTE DAI SOGGETTI IN POSIZIONE APICALE

Un cenno a parte meritano le operazioni promanate dai soggetti c.d. apicali direttamente e al di fuori di quanto previsto da eventuali procedure organizzative aziendali.

Ai sensi dell'art. 5 del Decreto, i soggetti apicali sono coloro "*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 coloro che esercitano anche di fatto la gestione ed il controllo dello stesso*".

Il Decreto non ha modificato il sistema normativo che disciplina l'amministrazione ed il governo delle società, sicché l'autonomia decisionale dei soggetti in posizioni apicali è sostanziale ed indefettibile espressione della libertà di gestione dell'impresa in forma societaria.

I soggetti in posizione apicale, in via ordinaria, decidono operazioni che seguono i normali criteri previsti dal Modello Organizzativo, che gli stessi conoscono e condividono. Pur tuttavia tali soggetti sono talvolta necessitati – nell'interesse della Società – ad avviare operazioni che seguono un *iter* procedimentale diverso da quello dettagliato nel Modello Organizzativo, a causa di situazioni di eccezionalità dovute ad esigenze di straordinaria urgenza o di particolare riservatezza od anche di singola peculiarità dell'operazione.

Proprio con riferimento a quest'ultima tipologia di operazione è tuttavia oltremodo necessario garantire la sussistenza di elementi di controllo idonei a consentire la verificabilità delle ragioni che hanno generato decisioni e/o comportamenti alla base delle operazioni stesse.

Ne consegue che il **sistema di controllo** deve necessariamente basarsi sui due elementi qualificanti della **tracciabilità degli atti** e del **flusso informativo** verso l'Organismo di Vigilanza.

In particolare, gli elementi specifici di controllo sono:

- Tracciabilità dell'operazione in termini di documentazione e supporti informativi atti a consentire la ricostruibilità a posteriori delle motivazioni e delle situazioni contingenti in cui si è sviluppata l'operazione stessa.
  Speciale riguardo deve assumere l'esplicazione, ancorché in forma sintetica (ma non generica), delle ragioni e dei motivi che hanno determinato la scelta operativa. Non necessariamente devono essere esplicitate le ragioni della decisione, ma le caratteristiche (ad es., riservatezza ed urgenza) che hanno reso impossibile l'attuazione della decisione secondo lo schema operativo prefissato;

- Specifica informativa, da parte dello stesso soggetto apicale che ha attivato l'operazione "in deroga", verso l'Organismo di Vigilanza affinché possa attuare i dovuti riscontri con sistematicità e tempestività.

Concludendo, si osserva che un ulteriore elemento di rafforzo del sistema deriva dagli specifici flussi informativi in deroga previsti, nella presente Parte Speciale, con riferimento ai sistemi di controllo dei singoli reati. Tali flussi informativi prevedono, infatti, l'invio degli estremi delle operazioni "in deroga" (a prescindere dalle origini delle stesse) all'Organismo di Vigilanza a cura dei Responsabili delle Funzioni materialmente esecutrici.