

ISTITUTO SANTA CECILIA SRL

**MODELLO DI ORGANIZZAZIONE
GESTIONE E CONTROLLO
(D.LGS. 231/2001)**

Rev. 1.2 – marzo 2025

con la consulenza di



TITOLO DOCUMENTO: Modello di organizzazione gestione e controllo

STRUTTURA: ISTITUTO SANTA CECILIA SRL
via Maratona 11, Civitavecchia

REVISIONE: Rev. 1.2 (marzo 2025)

STORIA DELLE MODIFICHE:

Versione:	Data:	Modifiche effettuate:
1.0	luglio 2014	Prima emissione
1.1	novembre 2018	Introduzione nuovi reati presupposto e procedure di segnalazione (whistleblowing)
1.2	marzo 2025	Modifica ragione sociale

Sommario

PARTE GENERALE	5
1. Definizioni	6
2. ISTITUTO SANTA CECILIA SRL	7
3. Il D.lgs. 231/2001 e la normativa rilevante	8
4. Le Linee Guida	9
5. Il Modello	10
5.1. La costruzione del Modello.....	10
5.2. La funzione del Modello	11
5.3. Principi ed elementi ispiratori del Modello	11
5.4. L'adozione del Modello e successive modifiche	12
6. I Processi Sensibili dell'ISTITUTO SANTA CECILIA SRL	13
7. L'organismo interno di vigilanza.....	14
7.1. Identificazione dell'organismo interno di vigilanza e requisiti. Nomina e revoca.....	14
7.2. Funzioni e poteri dell'organismo interno di vigilanza	14
8. La formazione delle risorse e la diffusione del Modello	16
8.1. Formazione ed informazione dei Dipendenti	16
8.2. Informazione ai Consulenti ed ai Partner	16
9. Sistema disciplinare	17
9.1. Funzione del sistema disciplinare	17
9.2. Violazioni del Modello	17
9.3. Le sanzioni	18
9.4. Misure nei confronti dei Consulenti e dei Partner.....	18
10. Procedure di segnalazione (whistleblowing).....	20
10.1. Procedure di segnalazione.....	20
11. Verifiche sull'adeguatezza del Modello	21
ORGANIGRAMMA.....	22
PARTE SPECIALE	24
12. Reati contro la pubblica amministrazione	25
12.1. Attività Sensibili	26
12.2. Principi generali di comportamento nei rapporti con la PA.....	26

12.3. Divieti.....	27
13. Reati societari e abusi di mercato	28
13.1. Attività Sensibili	29
13.2. Principi generali di comportamento.....	30
14. Reati in materia di violazione delle norme antfortunistiche e sulla tutela della sicurezza e salute sul lavoro	31
14.1. Attività sensibili.....	32
14.2. Valutazione dei rischi e misure preventive	33
14.3. Principi generali di condotta in materia di tutela della sicurezza e della salute sul lavoro.....	34
15. Reati ambientali (art. 25-undecies, D.lgs. 231/2001)	35
15.1. Attività sensibili.....	37
15.2. Principi generali di comportamento	38
15.3. Divieti.....	38
16. Reati in materia di delitti informatici e di illecito trattamento di dati personali (art. 24-bis D.lgs. 231/2001)	39
16.1. Attività sensibili.....	41
16.2. Principi generali di comportamento	42
16.3. Divieti.....	43

PARTE GENERALE

1. DEFINIZIONI

- “CCNL”: contratto applicato da ISTITUTO SANTA CECILIA SRL con riferimento al contratto collettivo nazionale di lavoro
- “Organismo di Vigilanza” o “OdV”: l’organismo interno di controllo, preposto alla vigilanza sul funzionamento e sull’osservanza del Modello nonché al relativo aggiornamento.
- “Consulenti”: coloro che agiscono in nome e/o per conto di ISTITUTO SANTA CECILIA SRL sulla base di un mandato o di altro rapporto di collaborazione professionale;
- “Dipendenti”: tutti i dipendenti (compresi i dirigenti) di ISTITUTO SANTA CECILIA SRL;
- “D.lgs. 231/2001”: il Decreto Legislativo dell’8 giugno 2001 n. 231 e successive modifiche e integrazioni.
- “Modello”: Modello di Organizzazione, Gestione e Controllo della Società che raccoglie l’insieme di processi e regole comportamentali che indirizzano lo svolgimento delle attività dell’Azienda in conformità alla legge che ha istituito la Responsabilità Amministrativa delle Persone Giuridiche (D.lgs. 231/2001).
- “P.A.”: la pubblica amministrazione e, con riferimento ai reati nei confronti della pubblica amministrazione, i pubblici ufficiali e gli incaricati di un pubblico servizio (es. i concessionari di un pubblico servizio).
- “Reati”: le fattispecie di reati ai quali si applica la disciplina prevista dal D.lgs. 231/2001, anche a seguito di sue successive modificazioni ed integrazioni.
- “Codice etico”: documento contenente i principi generali di comportamento a cui i destinatari devono attenersi anche con riferimento alle attività di cui al Modello di Organizzazione, Gestione e Controllo adottato dalla Società.
- “Destinatari”: Amministratori, Dipendenti, Outsourcer ed altri soggetti con cui la Società entri in contatto nello svolgimento di relazioni d’affari.
- “Sistema Disciplinare”: insieme delle misure sanzionatorie applicabili in caso di violazione del Modello.
- “Processi Sensibili”: attività di ISTITUTO SANTA CECILIA SRL nel cui ambito ricorre il rischio di commissione dei Reati;
- “Reati”: i reati ai quali si applica la disciplina prevista dal D.lgs. 231/2001;

2. ISTITUTO SANTA CECILIA SRL

Questo documento si riferisce alla società ISTITUTO SANTA CECILIA SRL, con sede in Civitavecchia, via Maratona, 11.

ISTITUTO SANTA CECILIA SRL gestisce un centro di recupero rieducativo e riabilitativo per soggetti invalidi civili, affetti da discinesie motorie, da minorazione fisiche, psichiche e sensoriali dipendenti da qualunque causa. La società ha sempre svolto e svolge tuttora la propria attività esclusivamente nella Regione Lazio. Per le erogazioni delle prestazioni di assistenza sanitaria, l'Istituto è inserito nella programmazione sanitaria della Regione Lazio, con la quale opera in regime di c.d. accreditamento. Le capacità operative e ricettive dell'Istituto dipendono dalla tipologia di trattamento sanitario prestato, distinguendo in:

a) trattamenti con degenza "a tempo pieno", sono riservati, principalmente, a soggetti portatori di gravi handicap;

b) trattamenti di tipo "ambulatoriale" possono essere erogati a favore di:

- soggetti che, a seguito di patologie congenite e/o acquisite o di incidenti traumatici, necessitano di riabilitazione fisioterapica.

- bambini in età evolutiva, che necessitino giornalmente, di trattamenti di neuropsicomotricità infantile;

c) trattamenti con degenza diurna (c.d. "semi-residenziale"), a favore di soggetti affetti da minorazioni fisiche o psichiche i quali, durante il corso della giornata, vengono assistiti nello svolgimento di attività ludiche e ricreative oltre che riabilitative.

Questo documento si riferisce all'ISTITUTO SANTA CECILIA SRL e a tutte le società da essa partecipate. Nel documento si indicherà sempre il nome "ISTITUTO SANTA CECILIA SRL", quale sinonimo della società madre e delle società partecipate.

3. IL D.LGS. 231/2001 E LA NORMATIVA RILEVANTE

In data 8 giugno 2001 è stato emanato - in esecuzione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 - il D.lgs. 231/2001, entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali cui l'Italia ha già da tempo aderito.

Il D.lgs. 231/2001, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" ha introdotto per la prima volta in Italia la responsabilità in sede penale degli enti per alcuni reati commessi nell'interesse o a vantaggio degli stessi, da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso e, infine, da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati. Tale responsabilità si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto.

La nuova responsabilità introdotta dal D.lgs. 231/2001 mira a coinvolgere nella punizione di taluni illeciti penali il patrimonio degli enti che abbiano tratto un vantaggio dalla commissione dell'illecito. Per tutti gli illeciti commessi è sempre prevista l'applicazione di una sanzione pecuniaria; per i casi più gravi sono previste anche misure interdittive quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la P.A., l'interdizione dall'esercizio dell'attività, l'esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi.

Quanto ai reati cui si applica la disciplina in esame, si tratta attualmente delle seguenti tipologie:

- (a) reati commessi nei rapporti con la P.A.,
- (b) reati in tema di falsità in monete, carte di pubblico credito e valori di bollo,
- (c) alcune fattispecie di reati in materia societaria,
- (d) reati con finalità di terrorismo o di eversione dell'ordine democratico e reati contro la personalità individuale.
- (e) reati informatici
- (f) reati in materia di trattamento dei dati personali
- (g) reati colposi commessi con violazione di norme antinfortunistiche
- (h) reati transnazionali
- (i) reati ambientali

4. LE LINEE GUIDA

L'ISTITUTO SANTA CECILIA SRL nella predisposizione del presente Modello si è ispirata alle Linee Guida di Confindustria.

Tuttavia, la scelta eventuale di non adeguare il Modello ad alcune indicazioni contenute nelle Linee Guida non inficia la validità dello stesso - come peraltro precisano espressamente le Linee Guida -. Il singolo Modello, infatti, dovendo essere redatto con riferimento alla realtà concreta della società, ben può discostarsi dai codici citati che, per loro natura, hanno carattere generale.

5. IL MODELLO

5.1. La costruzione del Modello

Successivamente all'emanazione del D.lgs. 231/2001, l'ISTITUTO SANTA CECILIA SRL ha avviato un progetto interno finalizzato a garantire la predisposizione del Modello di cui all'art. 6 del citato decreto. L'ISTITUTO SANTA CECILIA SRL, al fine di sempre più assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, ha ritenuto opportuno adottare un modello di organizzazione e di gestione in linea con le prescrizioni del Decreto (di seguito "Modello"). L'ISTITUTO SANTA CECILIA SRL ritiene che l'adozione di tale Modello, unitamente alla emanazione del Codice Etico, costituiscano, al di là delle prescrizioni di legge, un ulteriore valido strumento di sensibilizzazione di tutti i dipendenti di Istituto e di tutti gli altri soggetti allo stesso cointeressati (Fornitori, Partner, Investitori, ecc.). Tutto ciò affinché i suddetti soggetti seguano, nell'espletamento delle proprie attività, comportamenti corretti e trasparenti in linea con i valori etico-sociali cui si ispira IRSS nel perseguimento del proprio oggetto sociale, e tali comunque da prevenire il rischio di commissione dei reati contemplati dal Decreto.

La predisposizione del presente Modello è stata preceduta da una serie di attività preparatorie suddivise in differenti fasi e dirette tutte alla costruzione di un sistema di prevenzione e gestione dei rischi, in linea con le disposizioni del D.lgs. 231/2001 ed ispirate, oltre che alle norme in esso contenute, anche alle Linee Guida.

Sebbene l'adozione del presente Modello costituisca una "facoltà" dell'ente e non un obbligo, l'ISTITUTO SANTA CECILIA SRL ha deciso di procedere con la sua predisposizione ed adozione in quanto consapevole che tale sistema rappresenti un'opportunità per migliorare la sua corporate governance, conformemente a quanto fatto anche da altre società appartenenti al medesimo gruppo societario di cui anche l'ISTITUTO SANTA CECILIA SRL fa parte.

Si descrivono qui di seguito brevemente le fasi in cui si è articolato il lavoro di individuazione delle aree a rischio, sulle cui basi si è poi dato luogo alla predisposizione del presente Modello.

1) "As-is analysis". L'identificazione dei Processi Sensibili è stata attuata attraverso il previo esame della documentazione aziendale (principali procedure in essere, organigrammi, ecc.) e una serie di interviste con i soggetti chiave nell'ambito della struttura aziendale (Consigliere Delegato, responsabile Amministrazione e Finanza, Direttore sanitario, responsabile Risorse Umane, ecc.) mirate all'individuazione e comprensione dei Processi Sensibili e dei sistemi e procedure di controllo già adottati in relazione ai medesimi.

Obiettivo di questa fase è stata l'analisi del contesto aziendale, al fine di identificare in quale area/settore di attività e secondo quale modalità vi sia la potenziale possibilità di commettere i Reati.

L'analisi è stata condotta principalmente su tutte le attività che prevedono un contatto/un'interazione tra risorse aziendali e soggetti qualificabili come Pubblici Ufficiali o incaricati di Pubblico Servizio, nonché sulle attività sociali capaci di influire sulla commissione dei reati societari considerati assoggettabili alle sanzioni di cui al D.lgs. 231/2001.

Se ne è ricavata una rappresentazione dei Processi Sensibili, dei controlli già esistenti e delle relative criticità, con particolare "focus" agli elementi di "compliance" e controllo specifici per

soddisfare i requisiti del Modello. I Processi Sensibili dell'ISTITUTO SANTA CECILIA SRL sono quelli descritti al capitolo successivo.

2) Effettuazione della "gap analysis". Sulla base dei Processi Sensibili individuati, delle procedure e controlli già adottati, nonché delle previsioni e finalità del D.lgs. 231/2001, si sono individuate le azioni di miglioramento delle attuali procedure interne e dei requisiti organizzativi essenziali per la definizione di un modello "specifico" di organizzazione, gestione e monitoraggio ai sensi del D.lgs. 231/2001.

3) Predisposizione del Modello. Il presente Modello è costituito da una "Parte Generale" e da una "Parte Speciale" predisposta per le diverse categorie di reato contemplate nel D.lgs. 231/2001.

5.2. La funzione del Modello

L'adozione e l'efficace attuazione del Modello non solo consente all'ISTITUTO SANTA CECILIA SRL di beneficiare dell'esimente prevista dal D.lgs. 231/2001, ma migliora, nei limiti previsti dallo stesso, la sua corporate governance, limitando il rischio di commissione dei Reati.

Scopo del Modello è la predisposizione di un sistema strutturato ed organico di procedure ed attività di controllo (preventivo ed ex post) che abbia come obiettivo la riduzione del rischio di commissione dei Reati mediante la individuazione dei Processi Sensibili e la loro conseguente proceduralizzazione.

I principi contenuti nel presente Modello devono condurre, da un lato, a determinare una piena consapevolezza del potenziale autore del Reato di commettere un illecito (la cui commissione è fortemente condannata e contraria agli interessi dell'ISTITUTO SANTA CECILIA SRL, anche quando apparentemente essa potrebbe trarne un vantaggio), dall'altro, grazie ad un monitoraggio costante dell'attività, a consentire all'ISTITUTO SANTA CECILIA SRL di reagire tempestivamente nel prevenire od impedire la commissione del Reato stesso.

Tra le finalità del Modello vi è, quindi, quella di sviluppare la consapevolezza nei Dipendenti, Organi Sociali, Consulenti e Partner, che operino per conto o nell'interesse della società nell'ambito dei Processi Sensibili di poter incorrere - in caso di comportamenti non conformi alle norme e procedure aziendali (oltre che alla legge) - in illeciti passibili di conseguenze penalmente rilevanti non solo per sé stessi, ma anche per la società.

Inoltre, si intende censurare fattivamente ogni comportamento illecito attraverso la costante attività dell'Organismo di Vigilanza sull'operato delle persone rispetto ai Processi Sensibili e la comminazione di sanzioni disciplinari o contrattuali.

5.3. Principi ed elementi ispiratori del Modello

Nella predisposizione del presente Modello si è tenuto conto delle procedure e dei sistemi di controllo (rilevati in fase di "as-is") esistenti e già ampiamente operanti in azienda, ove giudicati idonei a valere anche come misure di prevenzione dei Reati e controllo sui Processi Sensibili.

Conformemente a quanto previsto anche dalle Linee Guida, sono state considerate le policy e le procedure esistenti che, previo eventuale adeguamento, potessero essere qualificabili come generali elementi costitutivi del Modello, ovvero:

- il sistema organizzativo aziendale;

- le policy e le procedure aziendali;
- il sistema di deleghe di poteri e delle procure;
- il sistema di comunicazione al personale;
- il sistema disciplinare.

Il presente Modello, fermo restando la sua finalità peculiare descritta al precedente paragrafo e relativa al D.lgs. 231/2001, si inserisce nel più ampio sistema di controllo costituito principalmente dalle regole di corporate governance e dal sistema di procedure già in essere in azienda e nel gruppo.

Principi cardine a cui il Modello si ispira sono:

- le Linee Guida di Confindustria in base alle quali è stata predisposta la mappatura dei Processi Sensibili dell'ISTITUTO SANTA CECILIA SRL;
- i requisiti indicati dal D.lgs. 231/2001 ed in particolare:
 - l'attribuzione ad un organismo di vigilanza del compito di promuovere l'attuazione efficace e corretta del Modello anche attraverso il monitoraggio dei comportamenti aziendali ed il diritto ad una informazione costante sulle attività rilevanti ai fini del D.lgs. 231/2001;
- l'attività di verifica del funzionamento del Modello con conseguente aggiornamento periodico (controllo ex post);
- l'attività di sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
- i principi generali di un adeguato sistema di controllo interno ed in particolare:
 - la verificabilità e documentabilità di ogni operazione rilevante ai fini del D.lgs. 231/2001;
 - il rispetto del principio della separazione delle funzioni;
 - la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
 - la comunicazione all'organismo di vigilanza delle informazioni rilevanti;

5.4. L'adozione del Modello e successive modifiche

Sebbene l'adozione del Modello sia prevista dalla legge come facoltativa e non obbligatoria, l'ISTITUTO SANTA CECILIA SRL ha ritenuto necessario procedere con l'adozione del presente Modello da parte dell'Assemblea dei Soci.

Essendo il presente Modello un "atto di emanazione dell'organo dirigente" (in conformità alle prescrizioni dell'art. 6, comma I, lettera a del D.lgs. 231/2001) le successive modifiche e integrazioni, fermo restando quanto previsto nel successivo capitolo, sono rimesse alla competenza del Consiglio di Amministrazione dell'ISTITUTO SANTA CECILIA SRL.

6. I PROCESSI SENSIBILI DELL'ISTITUTO SANTA CECILIA SRL

Dall'analisi dei rischi condotta dall'ISTITUTO SANTA CECILIA SRL ai fini del D.lgs. 231/2001 è emerso che i Processi Sensibili allo stato riguardano principalmente:

- le relazioni con la P.A.;
- i reati societari.
- omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro;
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita;
- reati ambientali
- Delitti informatici ed illecito trattamento dei dati

Gli altri reati contemplati dal D.lgs. 231/2001 appaiono solo astrattamente e non concretamente configurabili.

Si rinvia alle rispettive Parti Speciali per una più dettagliata descrizione dei Processi Sensibili sopra elencati.

7. L'ORGANISMO INTERNO DI VIGILANZA

7.1. Identificazione dell'organismo interno di vigilanza e requisiti. Nomina e revoca

In base alle previsioni del D.lgs. 231/2001, l'organismo cui affidare il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento deve essere un organismo della società (art. 6. 1, b) del D.lgs. 231/2001 e dotato di autonomi poteri di iniziativa e controllo.

L'ISTITUTO SANTA CECILIA SRL, in considerazione della specificità dei compiti che fanno capo all'OdV, ha effettuato la nomina dell'OdV.

7.2. Funzioni e poteri dell'organismo interno di vigilanza

All' OdV, una volta individuato, saranno affidati i compiti di vigilare:

- sull'osservanza del Modello da parte dei Dipendenti e collaboratori, degli Organi Sociali, dei Consulenti e dei Partner;
- sull'efficacia ed efficienza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei Reati;
- sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative.

A tal fine, all' OdV saranno altresì affidati i compiti di:

- Verifiche e controlli:
 - attuare le procedure di controllo previste dal Modello anche tramite l'emanazione di disposizioni (regolamentari e/o informative) interne;
 - condurre ricognizioni sull'attività aziendale ai fini dell'aggiornamento della mappatura dei Processi Sensibili;
 - effettuare periodicamente verifiche mirate su determinate operazioni o specifici atti posti in essere da ISTITUTO SANTA CECILIA SRL, soprattutto nell'ambito dei Processi Sensibili, i cui risultati devono essere riassunti in un apposito rapporto da esporsi in sede di reporting agli Organi Sociali deputati;
 - raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere a lui trasmesse o tenute a sua disposizione (vedi in dettaglio il successivo cap. 5.4);
 - coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per il miglior monitoraggio delle attività in relazione alle procedure stabilite nel Modello. A tal fine, l'OdV ha libero accesso a tutta la documentazione aziendale che ritiene rilevante e deve essere costantemente informato dal management: a) sugli aspetti dell'attività aziendale che possono esporre l'ISTITUTO SANTA CECILIA SRL al rischio concreto di commissione di uno dei Reati; b) sui rapporti con i Consulenti e con i Partner che operano per conto della società nell'ambito di Operazioni Sensibili;

- attivare e svolgere le inchieste interne, raccordandosi di volta in volta con le funzioni aziendali interessate per acquisire ulteriori elementi di indagine;
- **Formazione:**
 - coordinarsi con il responsabile Risorse Umane per la definizione dei programmi di formazione per il personale e del contenuto delle comunicazioni periodiche da farsi ai Dipendenti e agli Organi Sociali, finalizzate a fornire agli stessi la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al D. Lgs. 231/2001;
 - predisporre ed aggiornare con continuità, in collaborazione con la funzione Risorse Umane, lo spazio sul sito Internet contenente tutte le informazioni relative al D. Lgs. 231/2001 e al Modello;
 - monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello e predisporre la documentazione interna necessaria al fine della sua efficace attuazione, contenente istruzioni d'uso, chiarimenti o aggiornamenti dello stesso;
- **Sanzioni:**
 - coordinarsi con il management aziendale per valutare l'adozione di eventuali sanzioni disciplinari, fermo restando la competenza di quest'ultimo per l'irrogazione della sanzione e il relativo procedimento disciplinare.
- **Aggiornamenti:**
 - interpretare la normativa rilevante e verificare l'adeguatezza del Modello a tali prescrizioni normative;
 - valutare le esigenze di aggiornamento del Modello;
 - indicare al management le eventuali integrazioni ai sistemi di gestione delle risorse finanziarie (sia in entrata che in uscita), già presenti in ISTITUTO SANTA CECILIA SRL, per introdurre alcuni accorgimenti idonei a rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto.

L'OdV ha libero accesso presso tutte le funzioni della società - senza necessità di alcun consenso preventivo - onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal D.lgs. n. 231/2001.

Al fine di garantire che l'attività dell'OdV sia efficace e penetrante, e fermo restando il suo potere e responsabilità per la vigilanza sul funzionamento, sull'osservanza e sull'aggiornamento del Modello, egli potrà avvalersi non solo dell'ausilio di tutte le strutture della società ma altresì - sotto la sua diretta sorveglianza e responsabilità - di consulenti esterni, con specifiche competenze professionali in materia, per l'esecuzione delle operazioni tecniche necessarie alla funzione di controllo. Tali consulenti dovranno sempre riferire i risultati del proprio operato all'OdV.

8. LA FORMAZIONE DELLE RISORSE E LA DIFFUSIONE DEL MODELLO

8.1. Formazione ed informazione dei Dipendenti

Ai fini dell'efficacia del presente Modello, è obiettivo dell'ISTITUTO SANTA CECILIA SRL garantire una corretta conoscenza, sia alle risorse già presenti in azienda sia a quelle da inserire, delle regole di condotta ivi contenute, con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nei Processi Sensibili.

L'adozione del presente Modello è comunicata a tutti i dipendenti e collaboratori presenti in azienda al momento dell'adozione stessa.

Ai nuovi assunti, invece, viene consegnato il Codice Etico, con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza.

I suddetti soggetti si impegnano nello svolgimento dei propri compiti afferenti alle Processi Sensibili e in ogni altra attività che possa realizzarsi nell'interesse o a vantaggio della società, al rispetto dei principi, regole e procedure in esso contenuti.

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D.lgs. 231/2001 è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della società.

8.2. Informazione ai Consulenti ed ai Partner

I Consulenti ed i Partner devono essere informati del contenuto del Modello e dell'esigenza dell'ISTITUTO SANTA CECILIA SRL che il loro comportamento sia conforme ai disposti del D.lgs. 231/2001. A costoro viene consegnata copia del Codice Etico.

I suddetti soggetti, al momento della consegna del codice Etico, si impegnano, nello svolgimento dei propri compiti afferenti ai Processi Sensibili e in ogni altra attività che possa realizzarsi nell'interesse o a vantaggio della società, al rispetto dei principi, regole e procedure in esso contenuti.

9. SISTEMA DISCIPLINARE

9.1. Funzione del sistema disciplinare

La definizione di un sistema di sanzioni (commisurate alla violazione e dotate di deterrenza) applicabili in caso di violazione delle regole di cui al presente Modello rende efficiente l'azione di vigilanza ed ha lo scopo di garantire l'effettività del Modello stesso. La definizione di tale sistema disciplinare costituisce, infatti, ai sensi dell'art. 6 primo comma lettera e) del D.lgs. 231/2001, un requisito essenziale del Modello medesimo ai fini dell'esimente rispetto alla responsabilità della società.

L'applicazione del sistema disciplinare e delle relative sanzioni è indipendente dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del D.lgs. 231/2001.

9.2. Violazioni del Modello

Fermi restando gli obblighi nascenti dallo Statuto dei Lavoratori, i comportamenti sanzionabili sono i seguenti:

- a) violazione di procedure interne previste o richiamate dal presente Modello (ad esempio non osservanza delle procedure prescritte, omissione di comunicazioni in merito a informazioni prescritte, omissione di controlli, ecc.) o adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti non conformi alle prescrizioni del Modello o alle procedure ivi richiamate;
- b) violazione di procedure interne previste o richiamate dal presente Modello o adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti non conformi alle prescrizioni del Modello o dalle procedure ivi richiamate che esponano la società ad una situazione oggettiva di rischio di commissione di uno dei Reati;
- c) adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti non conformi alle prescrizioni del presente Modello, o alle procedure ivi richiamate, e diretti in modo univoco al compimento di uno o più Reati;
- d) adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti palesemente in violazione delle prescrizioni del presente Modello, o con le procedure ivi richiamate, tale da determinare la concreta applicazione a carico della società di sanzioni previste dal D.lgs. 231/2001.

Le sanzioni verranno commisurate al livello di responsabilità ed autonomia del Dipendente, all'eventuale esistenza di precedenti disciplinari a carico dello stesso, all'intenzionalità del suo comportamento nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui la società può ragionevolmente ritenersi esposta - ai sensi e per gli effetti del D.lgs. 231/2001 - a seguito della condotta censurata.

Il sistema disciplinare è soggetto a costante verifica e valutazione da parte del Consiglio di Amministrazione e del responsabile delle Risorse Umane, rimanendo quest'ultimo responsabile della concreta applicazione delle misure disciplinari qui delineate su eventuale segnalazione, una volta nominato, dell'OdV e sentito il superiore gerarchico dell'autore della condotta censurata.

9.3. Le sanzioni

La violazione da parte dei Dipendenti soggetti al CCNL delle singole regole comportamentali di cui al presente Modello costituisce illecito disciplinare.

I provvedimenti disciplinari irrogabili nei riguardi di detti lavoratori - nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) ed eventuali normative speciali applicabili - sono quelli previsti dall'apparato sanzionatorio del CCNL, e precisamente:

- richiamo verbale;
- richiamo scritto;
- multa non superiore all'importo di quattro ore della retribuzione;
- sospensione dal lavoro e dalla retribuzione fino ad un massimo di dieci giorni;
- licenziamento (anche, se necessaria, previa sospensione cautelare).

Restano ferme - e si intendono qui richiamate - tutte le previsioni di cui al CCNL, tra cui la necessità che:

- la contestazione disciplinare sia inviata al lavoratore non oltre il termine di trenta giorni dal momento in cui gli organi direttivi sanitari ed amministrativi hanno avuto effettiva conoscenza della mancanza commessa;
- il provvedimento disciplinare non sia adottato dal datore di lavoro oltre il termine di trenta giorni dalla presentazione della deduzione da parte del lavoratore;
- il predetto termine di trenta giorni rimanga sospeso nel caso in cui il dipendente richieda di essere ascoltato di persona unitamente al rappresentante sindacale, riprendendo poi a decorrere detto termine ab initio per ulteriori trenta giorni dalla data in cui le parti si saranno incontrate per discutere della contestazione;
- sia rispettato il principio di gradualità e proporzionalità delle sanzioni, in relazione alla gravità della mancanza e, pertanto, che il tipo e l'entità di ciascuna delle sanzioni siano determinati in relazione ai seguenti criteri generali di cui al CCNL.

Per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, al management aziendale.

9.4. Misure nei confronti dei Consulenti e dei Partner

Ogni violazione da parte dei Consulenti o dei Partner delle regole di cui al presente Modello agli stessi applicabili o di commissione dei Reati nello svolgimento della loro attività per l'ISTITUTO SANTA

CECILIA SRL è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti.

Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla società, come nel caso di applicazione alla stessa da parte del giudice delle misure previste dal D.lgs. 231/2001.

10. PROCEDURE DI SEGNALAZIONE (WHISTLEBLOWING)

La ratio sottesa all'adozione della Legge 30 novembre 2017, n. 179 è quella di individuare strumenti di tutela nei confronti dei lavoratori che denunciino reati o irregolarità di cui siano venuti a conoscenza nell'ambito delle proprie attività lavorative. Gli strumenti che previsti sono volti a:

- garantire la riservatezza a chi segnala le violazioni;
- assicurare la protezione del segnalante nei confronti di sanzioni disciplinari da parte dei datori di lavoro;
- prevedere misure deterrenti contro ogni informativa impropria.

Per realizzare tali obiettivi si prevedono:

a) uno o più canali che consentano ai soggetti di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;

b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;

c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;

d) nel sistema disciplinare sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

10.1. Procedure di segnalazione

I soggetti abilitati alla segnalazione sono tutti i dipendenti e collaboratori dell'ISTITUTO, la segnalazione può avvenire in forma libera, attraverso i contatti dell'Organismo di Vigilanza (OdV) il quale garantisce l'anonimato della segnalazione.

Competente a sanzionare chi viola le tutele riservate alla protezione dell'identità dei soggetti segnalanti è l'Organismo di Vigilanza (OdV).

11. VERIFICHE SULL'ADEGUATEZZA DEL MODELLO

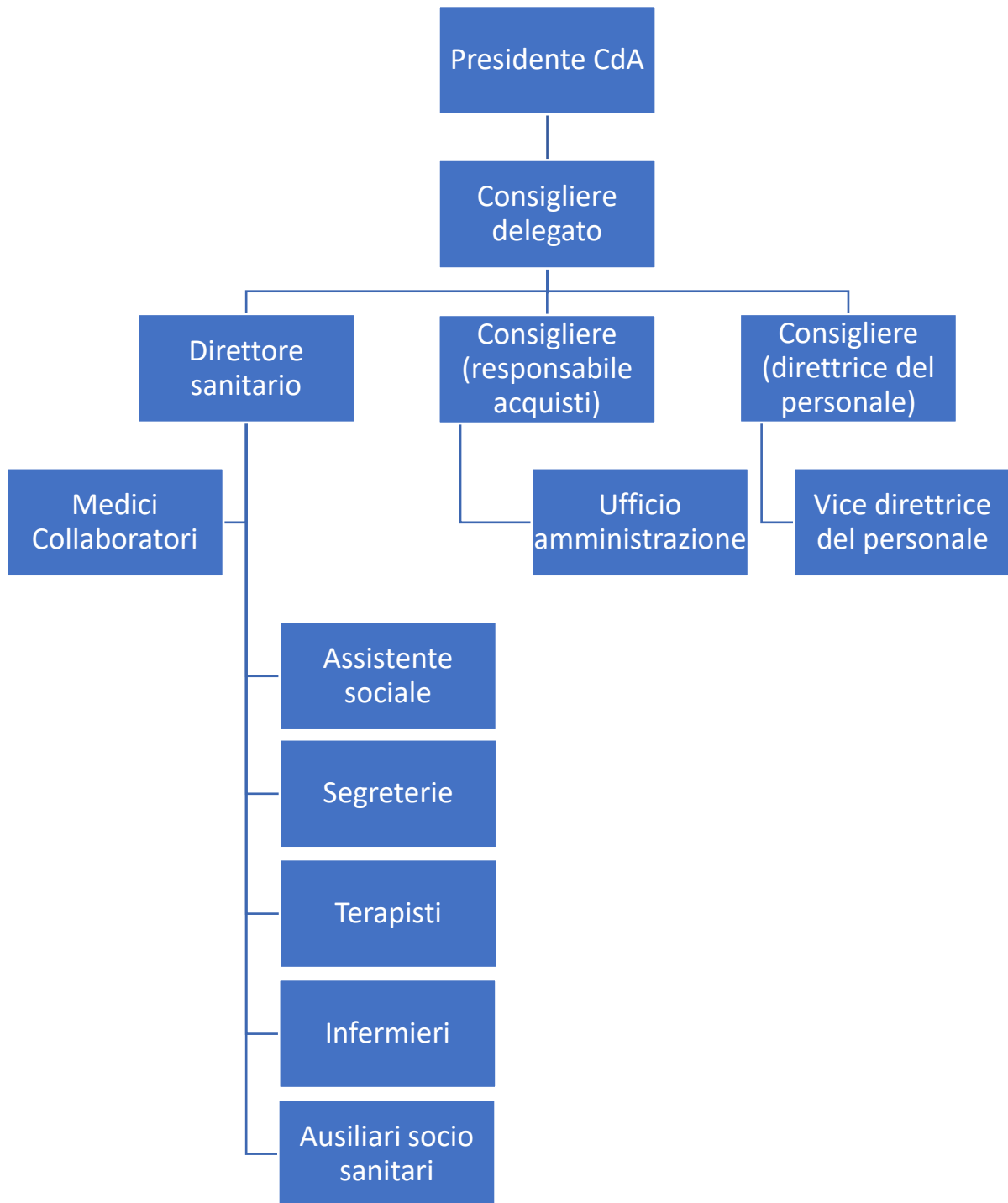
Oltre all'attività di vigilanza che l'OdV svolgerà continuamente sull'effettività del Modello (e che si concreta nella verifica della coerenza tra i comportamenti concreti dei destinatari ed il Modello stesso), egli periodicamente effettua specifiche verifiche sulla reale capacità del Modello alla prevenzione dei Reati, preferibilmente coadiuvandosi con soggetti terzi in grado di assicurare una valutazione obiettiva dell'attività svolta.

Tale attività si concretizza in una verifica a campione dei principali atti societari e dei contratti di maggior rilevanza conclusi dall'ISTITUTO SANTA CECILIA SRL in relazione ai Processi Sensibili e alla conformità degli stessi alle regole di cui al presente Modello.

Inoltre, viene svolta una review di tutte le segnalazioni ricevute nel corso dell'anno, degli eventi considerati rischiosi e della consapevolezza dei Dipendenti e degli Organi Sociali rispetto alla problematica della responsabilità penale dell'impresa con verifiche a campione.

Le verifiche e il loro esito sono oggetto di report annuale al Consiglio di Amministrazione.

ORGANIGRAMMA



PARTE SPECIALE

12. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

Nella presente Parte Speciale si riporta una breve esplicazione dei delitti contro soggetti pubblici interni o internazionali, indicati negli artt. 24 e 25 del Decreto 231/2001.

Concussione (art. 317 c.p.)

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

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

Tali ipotesi di reato si configurano nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio ricevano, per sé o per altri, denaro o altri vantaggi per compiere, omettere o ritardare atti del suo ufficio (determinando un vantaggio in favore del corruttore). Si ricorda che il reato di corruzione è un reato a concorso necessario, in cui sono puniti sia il corrotto sia il corruttore. La corruzione c.d. propria, quella per il compimento di un atto contrario ai doveri d'ufficio (ad esempio, accettazione di denaro per garantire l'aggiudicazione di una gara), può essere commessa da un pubblico ufficiale e da qualsiasi persona incaricata di un pubblico servizio, mentre la corruzione c.d. impropria, quella per il compimento di un atto dovuto (ad esempio, velocizzare una pratica la cui evasione è di propria competenza), può essere commessa da un pubblico ufficiale e da un incaricato di pubblico servizio che rivesta la qualifica di pubblico impiegato.

Possono configurarsi sia corruzioni c.d. attive (il dipendente corrompe un pubblico ufficiale o un incaricato di pubblico servizio per ottenere un vantaggio per la società), sia corruzioni c.d. passive (l'esponente della società riceve denaro o altra utilità per compiere un atto dovuto o contrario ai doveri d'ufficio), nei casi in cui l'attività svolta in concreto debba essere qualificata come pubblica funzione o pubblico servizio. Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

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

Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale o l'incaricato di pubblico servizio rifiuti l'offerta illecitamente avanzatagli (anche in tal caso, ove si tratti di istigazione alla corruzione impropria, l'incaricato di pubblico servizio deve rivestire, nel contempo, anche la qualifica di pubblico impiegato, non necessaria, invece, nel caso di istigazione alla corruzione propria).

Corruzione in atti giudiziari (art. 319-ter)

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

Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea (art. 640, comma 2 n. 1, c.p.)

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

12.1. Attività Sensibili

I reati considerati nel paragrafo che precede, possono essere commessi nella gestione dei rapporti con la Pubblica Amministrazione (intesa in senso lato e incluse, ove compatibili, le società a partecipazione pubblica) e nello svolgimento di attività che interagiscano con una pubblica funzione.

Al fine della individuazione delle Attività Sensibili, si è posta l'attenzione sui terreni in cui l'ISTITUTO SANTA CECILIA SRL, estrinsecando la propria attività, potrebbe, in astratto, incorrere nella realizzazione dei reati sopra elencati.

Così, in concreto, sono emerse le seguenti Attività Sensibili:

- rapporti con gli Enti Pubblici competenti (ad esempio, Ministero della Salute, Regioni) in relazione agli adempimenti periodici da eseguire in base alla normativa vigente ed alle autorizzazioni ottenute;

In relazione a ciascuna delle aree di attività elencate, è stato vagliato in concreto il modello di comportamento usualmente adottato dall'ISTITUTO SANTA CECILIA SRL nella partecipazione alle singole procedure, di cui sono stati evidenziate le aree in cui l'attività (interna ed esterna) della stessa non appariva sufficientemente tracciabile.

Inoltre, sono state considerate, in astratto, talune variabili di impresa suscettibili di ingenerare o accrescere i rischi in esame:

- realizzazione di attività illecite da parte di gruppi di persone; tale variabile può assumere rilevanza, in quanto i risultati da questi acquisiti possono porsi come il prodotto di indefinite e sfuggenti interazioni personali e di business, per loro stessa natura di difficile tracciabilità;

12.2. Principi generali di comportamento nei rapporti con la PA

La presente Parte Speciale prevede l'espresso obbligo, a carico degli esponenti aziendali, di:

- stretta osservanza di tutte le leggi e regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con la Pubblica Amministrazione ed alle attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio;
- instaurazione e mantenimento di qualsiasi rapporto con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza.

- In particolare, nell'espletamento delle attività considerate a rischio, i Destinatari dovranno attenersi ai seguenti principi generali di condotta:
- astenersi dal tenere comportamenti tali da integrare le fattispecie di reato previste in questa parte speciale del Modello;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Inoltre, è necessario che venga osservato quanto segue:

- l'ISTITUTO SANTA CECILIA SRL non inizierà o proseguirà nessun rapporto con esponenti aziendali, collaboratori esterni o partner che non intendano allinearsi al principio della stretta osservanza delle leggi;
- deve essere conservato un adeguato supporto documentale di ciascuna operazione a rischio, che consenta in ogni momento il controllo delle caratteristiche dell'operazione, del relativo processo decisionale, delle autorizzazioni rilasciate per la stessa e delle verifiche su di essa effettuate;
- gli incarichi conferiti ai collaboratori esterni devono essere redatti per iscritto, con l'indicazione del compenso pattuito;
- la fornitura di materiale in conto visione, conto deposito e comodato d'uso, avvengono secondo quanto stabilito dalle procedure interne le quali, tenendo conto delle normative in vigore in materia, regolamentano in modo corretto e trasparente questo tipo di operazioni.

12.3. Divieti

È fatto divieto agli esponenti aziendali di:

- effettuare elargizioni in denaro di qualsiasi entità a pubblici funzionari italiani ed esteri;
- distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale di cui al paragrafo che segue;
- accordare o promettere altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione, che possano essere interpretati come azioni arrecanti un vantaggio fuori da quanto concesso e descritto nel D.lgs. 231/2001;
- effettuare prestazioni in favore dei Partner aziendali che abbiano relazioni con soggetti della Pubblica Amministrazione in nome e conto dell'ISTITUTO SANTA CECILIA SRL, che non trovino adeguata giustificazione nel contesto del rapporto di business costituito con i Partner stessi;
- riconoscere compensi in favore dei Partner esterni che non trovino adeguata giustificazione in relazione sia al tipo di incarico da svolgere, sia in merito all'ammontare della ricompensa in relazione alle prassi di mercato accettate;

13. REATI SOCIETARI E ABUSI DI MERCATO

False comunicazioni sociali (artt. 2621 e 2622 c.c.)

Si tratta di due ipotesi criminose la cui condotta tipica coincide quasi totalmente e che si differenziano per il verificarsi o meno di un danno patrimoniale ai destinatari delle comunicazioni. La prima (art. 2621 c.c.) è una fattispecie di pericolo ed è costruita come una contravvenzione dolosa; la seconda (art. 2622 c.c.) di natura delittuosa, è costruita come un reato di danno.

Le due fattispecie criminose si realizzano tramite l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, idonei ad indurre in errore i destinatari della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, con l'intenzione di ingannare i soci, i creditori o il pubblico; ovvero l'omissione, con la stessa intenzione, di informazioni sulla situazione medesima la cui comunicazione è imposta dalla legge. Si precisa che:

- a) la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
- b) le informazioni false od omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene;
- c) la punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio al lordo delle imposte non superiore al 5% o una variazione del patrimonio netto non superiore all'1%; in ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate differiscono in misura non superiore al 10% di quella corretta;
- d) la responsabilità si estende anche all'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.
- e) soggetti attivi del reato sono gli amministratori, i direttori generali, i sindaci ed i liquidatori (reato proprio).

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

La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altre società o scissioni, che cagionino danno ai creditori (reato di evento). Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Soggetti attivi del reato sono, anche in questo caso, gli amministratori.

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

Il reato è integrato dalle seguenti condotte:

- a) fittizia formazione o aumento del capitale sociale mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale;
- b) sottoscrizione reciproca di azioni o quote;

c) sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono gli amministratori ed i soci conferenti.

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

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

Tale condotta criminosa consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.

Corruzione tra privati (art. 2635 c.c.)

Tale ipotesi di reato si realizza quando 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 nocimento alla società, sono puniti con la reclusione da uno a tre anni. Commette tale reato anche chi dà o promette denaro o altra utilità alle persone sopra indicate. La ratio incriminatrice della norma sia da ravvisarsi nell'esigenza di reprimere le forme di mala gestio connesse ad un fenomeno di deviazione dal buon andamento societario.

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

La "condotta tipica" prevede che si determini, con atti simulati o con frode, la maggioranza in assemblea allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

13.1. Attività Sensibili

In relazione ai reati ed alle condotte criminose descritte nel paragrafo che precede, ai fini della presente Parte Speciale del Modello, le aree ritenute più specificatamente a rischio risultano essere quelle relative alle seguenti attività:

- la predisposizione di comunicazioni dirette ai soci in generale riguardo alla situazione economica, patrimoniale e finanziaria della Società (bilancio d'esercizio, bilancio consolidato, relazione trimestrale e semestrale, etc);
- la predisposizione e divulgazione verso l'esterno di dati o notizie relative all'associazione stessa;
- predisposizione delle comunicazioni a soci e/o a terzi relative alla situazione economica, patrimoniale e finanziaria della Società;
- gestione rapporti con Soci, Società di revisione e Collegio Sindacale;
- adempimenti richiesti dal Collegio Sindacale, dai Soci o dalla Società di Revisione;
- operazioni su quote sociali, conferimenti, capitale e destinazione dell'utile - operazioni straordinarie (fusioni, scissioni, ecc.), ripartizioni dei beni;

- comunicazioni esterne, svolgimento e verbalizzazione assemblee

13.2. Principi generali di comportamento.

Obiettivo delle presente Parte Speciale è che tutti i Destinatari, nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle aree a rischio, si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi dei Reati Societari.

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

- fornire un elenco dei principi generali e delle procedure specifiche cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;

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

A. astenersi dal tenere comportamenti tali da integrare le fattispecie di reato previste in questa parte speciale del Modello;

B. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire, di per sé, fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

C. tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e delle altre comunicazioni sociali, al fine di fornire ai soci ed al pubblico in generale una informazione veritiera e appropriata sulla situazione economica, patrimoniale e finanziaria della Società.

In ordine a tale punto, è fatto divieto di:

- predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Società;
- omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società.

D. Tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nell'acquisizione, elaborazione e comunicazione dei dati e delle informazioni necessarie per pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria.

E. Osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale ed agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere al riguardo.

14. REATI IN MATERIA DI VIOLAZIONE DELLE NORME ANTIFORTUNISTICHE E SULLA TUTELA DELLA SICUREZZA E SALUTE SUL LAVORO

A seguito dell'entrata in vigore dell'art. 25-septies, tra i reati presupposto per l'applicazione del D.lgs. 231/01 figurano anche l'omicidio colposo (articolo 589 codice penale) e le lesioni colpose gravi o gravissime (articolo 590 codice penale), commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Per lesioni gravi s'intendono quelle che determinano:

- 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 40 giorni;
- l'indebolimento permanente di un senso o di un organo.
- Per lesioni gravissime s'intendono quelle che determinano:
 - una malattia certamente o probabilmente insanabile;
 - la perdita di un senso;
 - la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella;
 - la deformazione, ovvero lo sfregio permanente del viso.

I reati colposi in oggetto acquistano rilevanza dal punto di vista della responsabilità amministrativa della persona giuridica qualora siano conseguenza di violazioni della normativa di riferimento in materia di tutela dell'igiene e della salute sul lavoro e, in particolare, in via puramente esemplificativa ma non esaustiva, nelle seguenti ipotesi:

- mancata o inadeguata effettuazione della valutazione dei rischi;
- mancata o inadeguata elaborazione del relativo documento e del suo periodico aggiornamento;
- mancata designazione del Responsabile Servizio Prevenzione e Protezione (RSPP) ovvero designazione di un soggetto non in possesso di adeguata esperienza, formazione e preparazione professionale;
- omissione di predisposizione ovvero rimozione o danneggiamento di impianti, apparecchi e / o strumenti di segnalazione destinati alla prevenzione di disastri e / o infortuni sul lavoro (omissione o rimozione delle cautele antinfortunistiche);
- omissione nella collocazione ovvero rimozione o danneggiamento tale da renderli inservibili all'uso di apparecchi o altri strumenti destinati alla estinzione di un incendio ovvero al salvataggio o soccorso in caso di disastro o infortunio sul lavoro (omissione o rimozione dei dispositivi di sicurezza);
- mancata erogazione della formazione / informazione ai dipendenti prevista dalla normativa vigente;

- mancata designazione del medico competente alla sorveglianza sanitaria delle condizioni di lavoro e dei dipendenti ovvero designazione di un soggetto non in possesso di adeguata esperienza, formazione e preparazione professionale.

I soggetti tradizionalmente destinatari degli obblighi di sicurezza, di igiene e di salute del lavoro sono il datore di lavoro, i dirigenti e i preposti. A tali soggetti si aggiungono quelli istituzionalmente tenuti all'osservanza delle norme di sicurezza, di igiene e di salute del lavoro da disposizioni normative che regolino il caso concreto.

Tra gli obblighi di sicurezza, di igiene e di salute del lavoro cui l'ente deve adempiere si ricordano – per la loro ampiezza e grande significatività - quelli che seguono (senza esclusione, ovviamente, di ogni altro dovere imposto dalla normativa tempo per tempo vigente):

A. obbligo di valutare, in relazione alla natura della attività dell'azienda ovvero dell'unità produttiva, tutti i rischi per la sicurezza e per la salute dei lavoratori, ivi compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari, anche nella scelta delle attrezzature di lavoro e delle sostanze e dei preparati chimici impiegati, nonché nella sistemazione dei luoghi di lavoro, e conseguente obbligo di redazione del c.d. "Documento di Valutazione dei Rischi" ex artt. 17 e 28 e ss. del D.lgs. 81/2008;

B. obbligo di porre in essere ogni attività di prevenzione richiesta dalle situazioni concrete, realizzando il complesso delle disposizioni o misure da adottare o prevedere in tutte le fasi della attività lavorativa per evitare ogni infortunio e, comunque, diminuire i rischi professionali, nel rispetto della salute della popolazione e dell'integrità dell'ambiente esterno. Agli scopi suddetti, si debbono aggiornare le misure di prevenzione in relazione agli eventuali mutamenti organizzativi e produttivi suscettibili di assumere rilevanza ai fini della salute e della sicurezza del lavoro, ovvero in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;

C. obblighi di vigilanza e controllo dei lavoratori in ordine alla corretta attuazione delle misure di prevenzione;

D. obbligo di provvedere affinché ciascun lavoratore riceva un'adeguata informazione sui rischi per la sicurezza e la salute connessi all'attività dell'impresa;

E. obbligo di provvedere affinché ciascun lavoratore riceva una formazione sufficiente ed adeguata in materia di sicurezza e di salute, con preciso riferimento al proprio posto di lavoro e alle proprie mansioni.

14.1. Attività sensibili

In relazione ai reati ed alle condotte criminose descritte nel paragrafo che precede, le aree ritenute più specificatamente a rischio risultano essere le seguenti:

- la nomina del Responsabile Sicurezza Prevenzione e Protezione e del Medico competente;
- l'effettuazione della valutazione dei rischi;
- l'elaborazione del documento di valutazione dei rischi e del suo periodico aggiornamento;
- la predisposizione degli impianti, apparecchi e / o strumenti di segnalazione destinati alla prevenzione di disastri e / o infortuni sul lavoro;

- la collocazione degli apparecchi o degli altri strumenti destinati alla estinzione di un incendio ovvero al salvataggio o soccorso in caso di disastro o infortunio sul lavoro;
- l'erogazione e svolgimento di servizi di formazione / informazione ai dipendenti prevista dalla normativa vigente;
- la designazione del medico competente alla sorveglianza sanitaria delle condizioni di lavoro e dei dipendenti.

14.2. Valutazione dei rischi e misure preventive

Sono stati effettuati gli accertamenti necessari per la valutazione dei rischi per la sicurezza e salute dei lavoratori ai sensi della normativa vigente (D. Lgs. n. 81/2008).

Ad esito del processo di mappatura dei rischi rilevanti ai fini della legge in materia di prevenzione degli infortuni e di tutela della salute e dell'igiene sul lavoro, è stato elaborato il Documento di Valutazione dei Rischi, redatto a norma degli artt. 17 e 28 e ss. del D. Lgs. 81/2008.

Il Documento di Valutazione dei Rischi adottato dall'ISTITUTO SANTA CECILIA SRL e le successive modifiche ed integrazioni costituiscono parte integrante del presente Modello.

Il processo di mappatura dei rischi ha avuto ad oggetto ogni ambiente lavorativo o posto di lavoro della Società ed è stata effettuato applicando il seguente schema operativo:

- identificazione dei fattori di rischio;
- esposti descrizione dei fattori di rischio e delle condizioni operative legate ai fattori di rischio;
- Stima esposizioni del rischio.

Il processo di mappatura dei rischi è stato condotto attraverso una dettagliata analisi del ciclo lavorativo inserito nell'ambiente di lavoro, operando una distinzione tra rischi per la sicurezza dei lavoratori, rischi per la salute dei lavoratori e rischi derivanti da fattori organizzativi e gestionali.

In conformità alle disposizioni di legge in materia di tutela della salute e sicurezza sul lavoro, il datore di lavoro, tramite il Responsabile del Servizio di Prevenzione e Protezione, è tenuto ad indire almeno una volta all'anno una riunione cui partecipano:

- Il Presidente e il Consigliere Delegato, in qualità di datore di lavoro e legale rappresentante della Società;
- il Responsabile del Servizio di Prevenzione e Protezione dai rischi;
- il Medico competente (ove prevista la sua nomina);
- il Rappresentante dei lavoratori per la sicurezza.

Nel corso di tale riunione, di cui viene redatto verbale, viene esaminato il Documento di Valutazione dei Rischi, le misure di prevenzione e protezione e i programmi d'informazione e formazione del personale.

Il Documento di Valutazione dei Rischi dovrà essere costantemente aggiornato e conforme alle norme tempo per tempo vigenti in materia antinfortunistica e di tutela della sicurezza, della salute e dell'igiene sul lavoro.

In particolare, l'ISTITUTO SANTA CECILIA SRL si impegna a verificare l'adeguatezza di tutte le misure antinfortunistiche adottate, se del caso avvalendosi di consulenti dotati di competenze specifiche in materia di salute e sicurezza sul lavoro.

Fermo restando quanto precede, ogni qualvolta vengono posti in essere dei cambiamenti o delle variazioni alle postazioni di lavoro, alle mansioni lavorative o interventi strutturali significativi, l'ISTITUTO SANTA CECILIA SRL si adopererà affinché sia tempestivamente effettuata una specifica mappatura dei rischi concernente i cambiamenti, le variazioni e / o gli interventi strutturali intercorsi, con conseguente rielaborazione ed adeguamento del Documento di Valutazione dei Rischi e del Sistema di Gestione della Salute e Sicurezza sul Lavoro.

14.3. Principi generali di condotta in materia di tutela della sicurezza e della salute sul lavoro

In materia di norme antinfortunistiche e tutela dell'igiene e della salute sul lavoro, tutti i Destinatari del Modello ed, in particolare, tutti i Soggetti Apicali saranno tenuti a:

- astenersi dal tenere comportamenti tali da integrare le fattispecie di reato previste nella presente "Parte Speciale" del Modello;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle qui considerate, possano potenzialmente dare origine alle fattispecie criminose di cui alla presente "Parte Speciale";
- astenersi dal tenere comportamenti che possano in qualche modo o per qualsiasi ragione diminuire l'efficacia dei presidi adottati dalla Società e / o richiesti dalla legge ovvero da regolamenti aziendali interni ai fini della tutela della sicurezza ed igiene sul lavoro;
- tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività finalizzate alla attuazione di tutte le misure previste in tema di adeguamento della sicurezza ed igiene in azienda;
- osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità e della salute sul luogo di lavoro;
- assicurare il regolare funzionamento delle procedure e di tutte le misure previste nel Documento di Valutazione dei Rischi e dall'SGSL, garantendo ed agevolando ogni forma di monitoraggio interno sulla relativa gestione.

15. REATI AMBIENTALI (ART. 25-UNDECIES, D.LGS. 231/2001)

L'articolo 25-undecies del D.lgs. n. 231/2001 introdotto dal D.lgs. n. 121 del 7 luglio 2011 ha inserito, tra i reati presupposto per la punibilità dell'ente, i reati contro l'ambiente.

La Legge 22 maggio 2015 n.68, recante Disposizioni in materia di delitti contro l'ambiente, ha modificato in maniera significativa il D.Lgs.152/2006 e ha introdotto all'interno del codice penale un lungo elenco di reati ambientali (collocati nel nuovo Titolo VI-bis intitolato "Dei delitti contro l'ambiente"), una buona parte dei quali è configurato dalla Legge stessa come reato-presupposto atto a far scattare la responsabilità amministrativa dell'impresa, con conseguente modificazione e integrazione dell'articolo 25-undecies del decreto legislativo 8 giugno 2001 n.231.

In relazione al campo di operatività di ISTITUTO SANTA CECILIA SRL, risulta astrattamente configurabile il rischio di commissione dei seguenti reati:

- attività di gestione di rifiuti non autorizzata (D.lgs. 152/06, art. 256);
- inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (D.lgs. 152/06, art. 257);
- violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D.lgs. 152/06, art. 258);
- false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; Omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI - area movimentazione nel trasporto di rifiuti (D.lgs. 152/06, art. 260-bis);
- Inquinamento colposo (D.lgs. 202/07, art. 9);
- Inquinamento ambientale (articolo 452-bis c.p. introdotto dalla L. 68/2015)
- Disastro ambientale (articolo 452-ter c.p. introdotto dalla L. 68/2015)
- Delitti colposi contro l'ambiente (articolo 452-quinquies c.p. introdotto dalla L. 68/2015)

Inquinamento ambientale (art. 452-bis cod. pen.)

Commette tale reato (delitto) chiunque abusivamente cagiona una compromissione o un deterioramento significativi e misurabili:

- 1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo;
- 2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna.

Il reato prevede un'aggravante per la persona fisica nel caso in cui l'inquinamento sia prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette.

Disastro ambientale (art. 452-quater cod. pen.)

Commette tale reato (delitto) chiunque, fuori dai casi previsti dall'articolo 434 c.p, abusivamente cagiona un disastro ambientale. Costituiscono disastro ambientale alternativamente:

- 1) l'alterazione irreversibile dell'equilibrio di un ecosistema;
- 2) l'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali;
- 3) l'offesa alla pubblica incolumità in ragione della rilevanza del fatto per l'estensione della compromissione o dei suoi effetti lesivi ovvero per il numero delle persone offese o esposte a pericolo.

Delitti colposi contro l'ambiente (art. 452-quinquies cod. pen.)

La fattispecie dei delitti colposi contro l'ambiente, che sono reati-presupposto (al pari dei precedenti) per la responsabilità amministrativa dell'ente, prevede che se taluno dei fatti di cui ai reati di "inquinamento ambientale" e "disastro ambientale" (rispettivamente artt.452-bis e 452-quater c.p.) è commesso per colpa, le pene per le persone fisiche sono diminuite.

Se dalla commissione dei fatti indicati sopra deriva il pericolo di inquinamento ambientale o di disastro ambientale, le pene sono ulteriormente diminuite.

Violazione del divieto di scarico sul suolo, nel suolo e nelle acque sotterranee

All' art. 137 comma 11, primo periodo è sanzionata la condotta di chiunque, nel caso di scarico sul suolo, di cui alla tabella 4 dell'allegato 5 alla Parte terza del Codice dell'Ambiente, non osservi i divieti di scarico previsti dagli artt. 103 e 104 Cod. Amb.

L'art. 256 Cod. Amb. sanziona penalmente una pluralità di condotte che, configurandosi prevalentemente come violazione di disposizioni normative relative alla gestione di rifiuti, sono potenzialmente lesive dell'ambiente.

Le attività illecite previste dall'art. 256 Cod. Amb. sono riconducibili alla categoria dei "reati di pericolo astratto", per i quali la messa in pericolo del bene giuridico protetto (i.e. l'ambiente) è presunta dal legislatore, senza necessità di verificare concretamente la sussistenza del pericolo. La semplice violazione delle norme relative alle attività di Gestione dei Rifiuti o l'impedimento dei controlli predisposti in via amministrativa costituiscono, quindi, di per sé fattispecie di reato punibili.

Assumono rilevanza ai fini del Decreto:

Gestione non autorizzata di Rifiuti ai sensi dell'art. 256 comma 1 Cod. Amb.

Il primo comma dell'art. 256 Cod. Amb. punisce una pluralità di condotte connesse alla Gestione non autorizzata dei Rifiuti, ossia le attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di Rifiuti di qualsiasi genere – pericolosi e non pericolosi – poste in essere in mancanza della specifica autorizzazione, iscrizione o comunicazione prevista dagli artt. da 208 a 216 Cod. Amb.

Si precisa che, ai sensi dell'art. 193 comma 9 Cod. Amb., per le "attività di trasporto" non rilevano gli spostamenti di Rifiuti all'interno di un'area privata.

Una responsabilità del Produttore potrebbe, tuttavia, configurarsi a titolo di concorso nel reato. Ciò, non solo in casi di conoscenza della natura illecita dell'attività di Gestione dei Rifiuti concessa in appalto, ma anche in caso di violazione di specifici obblighi di controllo sul soggetto incaricato alla raccolta e smaltimento dei Rifiuti prodotti.

Si tenga, infatti, presente che tutti i soggetti coinvolti nel complesso delle attività di Gestione dei Rifiuti – tra cui anche il Produttore – sono tenuti, non solo al rispetto delle disposizioni normative relative al proprio ambito di attività, ma anche ad un controllo sulla corretta esecuzione delle attività precedenti o successive alla propria. Di conseguenza, il Produttore è tenuto a controllare che il soggetto a cui venga affidata la raccolta, il trasporto o lo smaltimento dei Rifiuti prodotti svolga tali attività in modo lecito. In caso contrario, l'inosservanza di obblighi precauzionali potrebbe determinare un "concorso colposo nel reato doloso".

Gestione di discarica non autorizzata ai sensi dell'art. 256 terzo comma Cod. Amb.

Il comma terzo della stessa disposizione punisce chiunque realizzi o gestisca una Discarica non autorizzata, con specifico aggravamento di pena nel caso in cui la stessa sia destinata allo smaltimento di Rifiuti Pericolosi.

In particolare, si precisa che nella definizione di Discarica non rientrano "gli impianti in cui i rifiuti sono scaricati al fine di essere preparati per il successivo trasporto in un impianto di recupero, trattamento o smaltimento, e lo stoccaggio di rifiuti in attesa di recupero o trattamento per un periodo inferiore a tre anni come norma generale, o lo stoccaggio di rifiuti in attesa di smaltimento per un periodo inferiore a un anno".

(b) il degrado dell'area stessa, consistente nell'alterazione permanente dello stato dei luoghi, nonché

(c) il deposito di una quantità consistente di rifiuti.

Ai fini della configurabilità della "gestione abusiva", infine, si deve dar luogo ad un'attività autonoma, successiva alla realizzazione, che implichi l'attivazione di un'organizzazione di mezzi e persone volti al funzionamento della Discarica stessa.

15.1. Attività sensibili

In relazione ai reati contemplati nel paragrafo precedente, le aree di operatività ritenute più specificamente a rischio risultano essere le seguenti:

- Smaltimento di rifiuti in genere
- Smaltimenti di rifiuti particolarmente dannosi e sottoposti a regimi particolari (rifiuti sanitari)
- Scarico di acque reflue
- Gestione illecita di rifiuti non pericolosi

15.2. Principi generali di comportamento

Obiettivo della presente Parte Speciale è che tutti i destinatari, nella misura in cui gli stessi possano essere coinvolti nello svolgimento di Attività Sensibili, si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi di fattispecie di reato rilevanti. In particolare, la presente Parte Speciale ha la funzione di:

- fornire un elenco dei principi generali e delle procedure specifiche cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.
- In particolare, nell'espletamento delle attività considerate a rischio, i Destinatari dovranno attenersi ai seguenti principi generali di condotta:
- astenersi dal tenere comportamenti tali da integrare le fattispecie di reato previste in questa parte speciale del Modello;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

E', inoltre, necessario:

- che tutte le attività e le operazioni svolte per conto dell'ISTITUTO SANTA CECILIA SRL, nonché la scelta delle controparti contrattuali (es. fornitori, consulenti, etc.) e la fissazione delle condizioni commerciali siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di professionalità, indipendenza e trasparenza, e in riferimento a essi sia motivata la scelta;
- che sia assicurata la veridicità e la genuinità dei documenti prodotti in ambito di autorizzazioni ambientali e normative collegate;
- che sia garantito il rispetto della normativa vigente, nonché delle procedure e dei protocolli aziendali, in materia di gestione dei rifiuti, ivi incluso per ciò che attiene l'espletamento dei necessari controlli, anche preventivi, sulle risorse di provenienza straniera;
- che sia mantenuta una condotta chiara, trasparente, diligente e collaborativa con le pubbliche Autorità, con particolare riguardo alle Autorità giudicanti ed inquirenti, mediante la comunicazione di tutte le informazioni, i dati e le notizie eventualmente richieste;

15.3. Divieti

Nell'attività di gestione dei rifiuti, è fatto divieto ai Destinatari del presente Modello, ciascuno nell'ambito delle rispettive competenze, di:

- porre in essere qualsiasi condotta che possa generare un danno per l'ambiente come definito dalla normativa vigente;

16. REATI IN MATERIA DI DELITTI INFORMATICI E DI ILLECITO TRATTAMENTO DI DATI PERSONALI (ART. 24-BIS D.LGS. 231/2001)

L'incessante diffusione delle tecnologie dell'informazione e della comunicazione per questioni legate principalmente alla riduzione dei costi, all'interoperabilità ed alla standardizzazione ha, da un lato, introdotto nuove opportunità ma, dall'altro, generato il proliferarsi di nuove condotte penalmente rilevanti.

I reati informatici sono facilitati dalla continua evoluzione dello spazio virtuale che consente la delocalizzazione delle risorse e la loro raggiungibilità da ogni luogo e distanza anche, e soprattutto, grazie alla nuova dimensione IT offerta dal Cloud Computing. Il crimine coinvolge la struttura della tecnologia dell'informazione, compreso l'accesso illegale, l'intercettazione, le interferenze illecite a dati e sistemi, la contraffazione, la frode informatica, il furto di identità digitale e il trattamento illecito dei dati.

Oggigiorno si parla di cybercrime e cybersecurity come inquietanti rischi per lo sviluppo globale, sia per la rilevanza delle infrastrutture critiche informatizzate per l'economia nazionale e la sicurezza, che per l'interazione con le politiche che affrontano la privacy e la protezione dei dati.

L'articolo 24-bis del D.lgs. n. 231/2001 ha inserito, tra i reati presupposto per la punibilità dell'ente, i seguenti reati contro la privacy:

- trattamento illecito dei dati (art. 167 del D.lgs. 196/2013 come modificato dal D.lgs. 101/2018);
- falsità nelle dichiarazioni al Garante (art. 168 del D.lgs. 196/2013 come modificato dal D.lgs. 101/2018);
- inosservanza dei provvedimenti del Garante (art. 170 del D.lgs. 196/2013 come modificato dal D.lgs. 101/2018).

In relazione al campo di operatività di ISTITUTO SANTA CECILIA SRL, risulta astrattamente configurabile il rischio di commissione dei seguenti reati:

- trattamento illecito dei dati (art. 167 del D.lgs. 196/2013);
- inosservanza dei provvedimenti del Garante (art. 170 del D.lgs. 196/2013).

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

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

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.”.

Il reato si potrebbe configurare laddove:

1. ci si introduca abusivamente (ovvero senza il consenso del titolare dello ius excludendi) in un sistema informatico protetto. L'introduzione è un processo che si qualifica in due fasi consistenti nell'accesso fisico (accensione del computer) e accesso logico (inizio del colloquio con il software). L'integrazione del reato si configura con l'accesso logico, ovvero con il momento in cui vengono superate le barriere (fisiche e logiche) che presidiano l'accesso alla memoria, con l'effetto di poter richiamare dati contenuti nel software o, comunque di aver libertà di movimento;

2. dopo l'accesso (anche non abusivo), il soggetto agente continui a permanere in un sistema informatico protetto nonostante il titolare dello ius excludendi abbia esercitato, anche tacitamente, tale diritto. Questa condotta, secondo la dottrina prevalente, viene integrata qualora a seguito di una introduzione casuale, oppure solo inizialmente autorizzata (in termini temporali e/o di modalità di permanenza), l'agente permanga nel sistema oltre i limiti e/o le modalità consentite. Si rileva inoltre che in caso di accesso lecito, l'assenza del dissenso alla permanenza da parte del titolare, esclude la configurazione della fattispecie criminosa in esame.

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

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

Il reato si potrebbe configurare qualora:

siano distrutte, deteriorate, cancellate, alterate o sopprese informazioni, dati o programmi informatici altrui. La condotta viene quindi realizzata con interventi di alterazione o modificazione del software, e delle basi di dati, che non intaccano l'integrità dell'hardware.

Esempi di condotte potrebbero essere:

1. l'accesso non autorizzato ad archivi tramite tecniche di hacking, con conseguente prelievo e/o danneggiamento dei dati.

2. l'accesso ai dati registrati nei sistemi gestionali e/o contabili con modalità non controllata, e conseguente manipolazione dei dati stessi. L'accesso potrebbe essere effettuato tramite:

- userID scaduta non cancellata;
- userID generiche;
- userID e pwd scoperte in vario modo;
- accesso fisico a PC altrui incustodito;
- uso di apparecchiature dimesse ma non distrutte;
- accesso alla consolle di amministrazione del sistema

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

“Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all’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 è punito con la reclusione da uno a cinque anni.

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

Il reato si potrebbe configurare laddove:

siano distrutte, deteriorate, cancellate, alterate o soppresse 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.

La fattispecie in esame oltre a ricomprendere tutte le condotte esemplificate sub articolo 635-bis estende la sua portata incriminatrice anche alle condotte di chi effettua danneggiamenti a distanza di sistemi informatici o telematici altrui mediante programmi virus o dati maligni introdotti nella rete (trojan horses e logic bomb) per rendere in tutto o in parte inservibili quegli stessi sistemi informatici o telematici.

Le condotte menzionate possono a titolo esemplificativo configurarsi mediante:

- l'invio di e-mail a cui sono allegati documenti affetti da virus;
- l'accesso alla rete target (tramite meccanismi di hacking) e sostituzione di file puliti con file affetti da virus;
- diffusione dei virus per mezzo di dispositivi di memoria rimovibili

16.1. Attività sensibili

In relazione ai reati contemplati nel paragrafo precedente, le aree di operatività ritenute più specificamente a rischio risultano essere le seguenti:

- Conservazione e trattamento dei dati personali e sensibili del personale e dei pazienti;
- Errata gestione delle misure di sicurezza (fisiche ed informatiche) nella gestione dei dati

Inoltre, sono state considerate, in astratto, talune variabili di impresa suscettibili di ingenerare o accrescere i rischi in esame:

- consuetudini o usi comuni di settore sostanzialmente illeciti, ma vissuti dagli operatori come irrinunciabili o addirittura come positivi anche sul piano etico.
- assume fondamentale importanza il rispetto dei provvedimenti emessi dal Garante della Privacy, soprattutto in tema di trattamento dei dati del lavoratore (anche per i c.d. controlli difensivi), di uso di internet e della posta elettronica, di amministratore di sistema.

16.2. Principi generali di comportamento

Obiettivo della presente Parte Speciale è che tutti i destinatari, nella misura in cui gli stessi possano essere coinvolti nello svolgimento di Attività Sensibili, si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi di fattispecie di reato rilevanti. In particolare, la presente Parte Speciale ha la funzione di:

- fornire un elenco dei principi generali e delle procedure specifiche cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- In particolare, nell'espletamento delle attività considerate a rischio, i Destinatari dovranno attenersi ai seguenti principi generali di condotta:
- astenersi dal tenere comportamenti tali da integrare le fattispecie di reato previste in questa parte speciale del Modello;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

È, inoltre, necessario:

- che tutte le attività e le operazioni svolte per conto di ISTITUTO SANTA CECILIA SRL, nonché la scelta delle controparti contrattuali (es. fornitori, consulenti, etc.) e la fissazione delle condizioni commerciali siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di professionalità, indipendenza e trasparenza, e in riferimento a essi sia motivata la scelta;
- che sia assicurata l'assoluta riservatezza delle informazioni e dei dati personali;
- che sia mantenuta una condotta chiara, trasparente, diligente e collaborativa con le autorità di controllo, mediante la comunicazione di tutte le informazioni, i dati e le notizie eventualmente richieste;

Al fine di prevenire ed impedire il verificarsi dei Reati Informatici, i Destinatari coinvolti nello svolgimento delle Attività Sensibili nelle Aree a Rischio Reato individuate, sono tenuti al rispetto dei seguenti principi generali di condotta, fermo restando quanto indicato dal Codice Etico e dalle specifiche Procedure aziendali:

- astenersi dal porre in essere o partecipare alla realizzazione di condotte che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato indicate nei precedenti paragrafi;
- astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati indicati nei precedenti paragrafi, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi.

Le funzioni/unità organizzative aziendali e, in particolare, coloro i quali rivestono posizioni rilevanti nell'utilizzo e nell'amministrazione dei sistemi informatici, devono ispirare la loro azione ai seguenti principi generali:

- **Riservatezza** - garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- **Integrità** - garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- **Disponibilità** - garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

16.3. Divieti

Nell'attività di gestione dei rifiuti, è fatto divieto ai Destinatari del presente Modello, ciascuno nell'ambito delle rispettive competenze, di:

- porre in essere qualsiasi condotta che possa generare un danno per la privacy;
- falsificare o alterare documenti contenenti dati personali e sensibili;
- adottare condotte contrarie alla legge

A questo proposito, a titolo meramente esemplificativo e non esaustivo, è fatto divieto in particolare di:

- 1) introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto di accesso
- 2) accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati dell'Istituto, o a parti di esse, non possedendo le credenziali di accesso o mediante l'utilizzo di credenziali di altri colleghi abilitati;
- 3) distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad esso pertinenti o comunque di pubblica utilità;
- 4) introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- 5) alterare, mediante l'utilizzo di firma elettronica o comunque in qualsiasi modo, documenti informatici;
- 6) produrre e trasmettere documenti in formato elettronico contenenti dati falsi e/o alterati;

- 7) intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- 8) utilizzare dispositivi tecnici o strumenti software non autorizzati (ad esempio, virus, worm, trojan, spyware, dialer, keylogger, rootkit) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- 9) detenere, procurarsi, riprodurre e o diffondere abusivamente codici di accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- 10) procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- 11) rimuovere il software antivirus installato sugli strumenti informatici in dotazione agli utenti.