Centro Diagnostico Ostiense

CENTRO DIAGNOSTICO OSTIENSE SRL

Modello Organizzativo D. LGS. 231/01

Revisione del 06/10/2026

Centro Diagnostico Ostiense Srl

Sede Legale: Via Francesco Antonio Pigafetta 1,00154 Roma (RM)

Sede Operativa: Via Francesco Antonio Pigafetta 1,00154 Roma (RM)

Revisione	Motivazione	Data
00	Redazione del Modello Organizzativo ex D.Lgs 231/01	09/03/2015
01	Revisione del Modello Organizzativo ex D.Lgs 231/01	30/11/2015
02	Revisione del Modello Organizzativo ex D.Lgs 231/01	21/11/2016
03	Revisione del Modello Organizzativo ex D.Lgs 231/01	27/04/2017
04	Revisione del Modello Organizzativo ex D.Lgs 231/01	26/01/2018
05	Revisione del Modello Organizzativo ex D.Lgs 231/01	06/03/2019
06	Revisione del Modello Organizzativo ex D.Lgs 231/01	22/07/2020
07	Revisione del Modello Organizzativo ex D.Lgs 231/01	15/01/2024
08	Revisione del Modello Organizzativo ex D.Lgs 231/01	06/10/2026

Timbro e Firma Rappresentante Legale

CENTRO DIAGNOSTICO S.r.l.
Via A. Pigafetta, 1 - 00154 Roma
Partita IVA 04809221000

*Il presente documento contiene informazioni e dati di **Centro Diagnostico Srl.** Pertanto documento e contenuti non sono divulgabili in nessuna forma senza esplicito consenso del titolare*

PREMESSA 6

1 INTRODUZIONE 6

1.1 GENERALITÀ 6

1.2 STRUTTURA DEL MODELLO ORGANIZZATIVO 231 7

1.3 INTEGRABILITA' CON GLI ALTRI SISTEMI DI GESTIONE 8

1.3.1 APPROCCIO PER PROCESSI 9

1.3.2 METODOLOGIA APPLICATA PER LA DEFINIZIONE DEL MODELLO ORGANIZZATIVO 231 9

2 SCOPO E CAMPO DI APPLICAZIONE/PRESENTAZIONE E POLITICA DELLA SOCIETA' 9

2.1 GENERALITA' 9

2.2 SCOPO 9

2.2.1 MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO 9

2.3 APPLICAZIONE 10

2.4 PRESENTAZIONE DELLA SOCIETA' 10

2.5 MODIFICHE ED INTEGRAZIONI DEL MODELLO 11

2.6 AGGIORNAMENTO DEL MODELLO 11

2.7 VERIFICA DEL MODELLO 11

2.8 DESTINATARI DEL MODELLO 11

2.9 LA POLITICA 11

2.10 OBIETTIVI 12

3 RIFERIMENTI NORMATIVI 13

3.1 NORME E LINEE GUIDA 13

4 TERMINI E DEFINIZIONI 13

5 SISTEMA DI GESTIONE PER LA RESPONSABILITA' AMMINISTRATIVA (SGRA) ... 15

5.1 REQUISITI GENERALI 15

5.2 IL SISTEMA DI DELEGHE E PROCURE 16

6 PIANIFICAZIONE DELLA IDENTIFICAZIONE DEI POSSIBILI REATI E D.LGS 231/0116

6.1 GENERALITA' 16

6.2 DEFINIZIONE DI RISCHIO ACCETTABILE 17

6.3 IL LIVELLO DEI RISCHI E LA MATRICE DI VALUTAZIONE DEL RISCHIO 18

6.3.1 STRUMENTO DI LAVORO 18

6.4 POSSIBILI REATI PREVISTI DAL D.LGS 231/01 18

6.5 ASPETTI GENERALI 19

6.6 LE PROCEDURE 20

6.7 TENUTA SOTTO CONTROLLO DEI DOCUMENTI 21

6.8 L'ADOZIONE DEL MODELLO 21

7 CONTROLLO DELLA VALIDITA' DEL SISTEMA DI GESTIONE 21

7.1 DOCUMENTI RELATIVI AL PROGRAMMA DI AUDIT INTERNI 22

7.2 ATTUAZIONE E STANDARDIZZAZIONE DEL SISTEMA DI GESTIONE 22

8 RESPONSABILITA' DELLA DIREZIONE 22

8.1 IL SISTEMA DEI POTERI 22

8.2 IMPEGNO DELLA DIREZIONE 22

8.3 CODICE ETICO E POLITICA PER LA RESPONSABILITA' AMMINISTRATIVA 23

9 ORGANISMO DI VIGILANZA 24

9.1 RUOLO E COMPOSIZIONE 24

9.2 RISERVATEZZA 25

9.3 COMPITI E POTERI 25

9.4 FLUSSI INFORMATIVI 25

9.5 INIZIATIVA DI CONTROLLO 26

9.6 STRUMENTI DI CONTROLLO E AZIONE 27

9.7 LA RELAZIONE DELL'ODV 27

9.8 DISPOSIZIONI IN TEMA DI WHISTLEBLOWING 27

10 OPERAZIONI PROMANATE DIRETTAMENTE DAL VERTICE AZIENDALE 33

10.1 AMBITO DI RIFERIMENTO 33

10.2 ATTIVITA' DI CONTROLLO 33

10.3 RIESAME DELLA DIREZIONE 33

11 GESTIONE DELLE RISORSE UMANE 34

11.1 SCOPO 34

11.2 MESSA A DISPOSIZIONE DELLE RISORSE 34

11.3 FORMAZIONE, INFORMAZIONE, COMUNICAZIONE 34

12 SISTEMA DISCIPLINARE E SANZIONATORIO 34

12.1 PREMESSA 34

12.2 DEFINIZIONE E LIMITI DELLA RESPONSABILITÀ DISCIPLINARE 35

12.3 DIPENDENTI, COLLABORATORI, CONSULENTI 35

12.4 LE CONDOTTE RILEVANTI 36

12.5 LE SANZIONI 36

12.6 LE SANZIONI NEI CONFRONTI DEI DIPENDENTI 36

12.7 SANZIONI NEI CONFRONTI DEI TERZI DESTINATARI 36

12.8 IL PROCEDIMENTO DI IRROGAZIONE DELLE SANZIONI 37

PARTE SPECIALE 38

PREMESSA

Il Decreto Legislativo 8 giugno 2001, n. 231 ha introdotto nell'ordinamento italiano la responsabilità amministrativa degli enti per taluni reati commessi, nel loro interesse o a loro vantaggio, da soggetti che rivestono funzioni di rappresentanza, amministrazione o direzione dell'ente, ovvero da soggetti sottoposti alla direzione o alla vigilanza di questi ultimi.
Il sistema delineato dal D.lgs. n. 231/2001 ha conosciuto, nel tempo, un progressivo ampliamento del catalogo dei reati presupposto, per effetto di successivi interventi normativi che hanno esteso l'ambito applicativo della responsabilità amministrativa degli enti a una pluralità crescente di fattispecie criminose, anche in attuazione di obblighi derivanti dall'ordinamento dell'Unione europea e da convenzioni internazionali.
Nel suo assetto attuale, il Decreto ricomprende un catalogo articolato di reati, che comprende, tra gli altri, i delitti contro la Pubblica Amministrazione, i reati societari, i reati informatici, i delitti in materia di salute e sicurezza sul lavoro, i reati ambientali, i reati tributari, i delitti di riciclaggio e autoriciclaggio, i reati in materia di strumenti di pagamento diversi dai contanti, nonché ulteriori fattispecie introdotte dal legislatore in relazione all'evoluzione del quadro economico, organizzativo e regolatorio. In tale contesto devono essere considerate anche le più recenti estensioni del catalogo dei reati presupposto, ivi comprese quelle relative ai delitti in materia di violazione delle misure restrittive dell'Unione europea.
Alla luce di tale evoluzione normativa, il Modello di Organizzazione, Gestione e Controllo adottato dalla Società è stato elaborato tenendo conto del quadro normativo vigente alla data del suo aggiornamento e delle fattispecie di reato astrattamente rilevanti in relazione alle attività svolte dalla Società, al fine di garantire un sistema di prevenzione idoneo, aggiornato e coerente con l'assetto organizzativo e operativo aziendale.

- **Il Decreto prevede la responsabilità amministrativa (penale) degli Enti (persone giuridiche, società ed associazioni anche prive di personalità giuridica).**
- **La responsabilità dell'Ente si aggiunge a quella penale delle persone fisiche che materialmente hanno realizzato l'illecito.**
- **Gli Enti possono essere ritenuti responsabili, e quindi soggetti a sanzioni, per i reati previsti dal Decreto commessi, nel loro interesse o vantaggio, da amministratori, dirigenti o dipendenti.**
- **Il Modello Organizzativo, efficacemente attuato, può rappresentare per l'Ente una forma di esonero dalla responsabilità derivante dai Reati.**

1 INTRODUZIONE

1.1 GENERALITÀ

In tale ottica la Società **CENTRO DIAGNOSTICO S.r.l.** ha provveduto ad effettuare un'analisi del contesto aziendale per evidenziare le aree e le modalità con le quali si possono realizzare i reati previsti dal Decreto legislativo 231/2001 (attività di *risk assesment*), al fine di elaborare un modello organizzativo coerente con la specifica attività della Società, conformemente a quanto previsto dal Decreto legislativo 231/2001.
Si rileva comunque che i modelli organizzativi previsti dal Decreto legislativo 231/2001 non costituiscono un "quid novi", poiché l'attività di impresa svolta dalla Società è sostanzialmente caratterizzata da un proprio sistema di controllo, particolarmente rigoroso basato sull'implementazione di un Sistema di Gestione in accordo alle norme:

- UNI EN ISO 9001:2015;
- SGSL 81/08 per la sicurezza

di cui il modello organizzativo 231 descritto nel presente Manuale è parte integrante.

Ulteriormente la Società **CENTRO DIAGNOSTICO S.r.l.** ha adottato il Codice di autoregolamentazione per la protezione dei dati personali, con il quale intende assicurare che il trattamento dei dati personali avvenga in conformità al Regolamento Europeo 679/2016.
Per la società si è trattato, quindi, di effettuare un riscontro delle strutture organizzative interne già attive e operanti per verificarne la rispondenza, anche formale, al dettato del Decreto legislativo 231/2001 e integrare il Modello Organizzativo 231 nel Sistema di Gestione sempre in ottemperanza a quanto stabilito nel codice di Autoregolamentazione per la protezione dei dati personali previsto dal Regolamento Europeo 679/2016.
La Società è sensibile all'esigenza di diffondere e consolidare una cultura di correttezza, integrità e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria immagine e posizione, delle aspettative dei propri soci e del lavoro dei propri dipendenti ed è consapevole dell'importanza di dotarsi di un sistema di controllo idoneo a prevenire la commissione di comportamenti illeciti da parte dei propri amministratori, dipendenti, rappresentanti e partner d'affari.
A tal fine, la società ha avviato un programma di analisi dei propri strumenti organizzativi, di gestione e di controllo, volto a verificare la corrispondenza delle procedure aziendali già esistenti alle finalità previste dal Decreto e ad integrare i principi comportamentali e le procedure già adottate.
La Direzione ha dato attuazione al Modello Organizzativo con la nomina dell'apposito Organismo di Vigilanza. La direzione si riserva, a seguito di verifiche periodiche, anche sulla base delle proposte formulate dall'Organismo di Vigilanza, di procedere all'approvazione di ulteriori eventuali modifiche e/o integrazioni che si dovessero rendere necessarie in conseguenza di significative violazioni delle prescrizioni del Modello Organizzativo, significative modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività di impresa, modifiche normative al Decreto legislativo 231/2001.

1.2 STRUTTURA DEL MODELLO ORGANIZZATIVO 231

Il Modello Organizzativo 231 della Società **CENTRO DIAGNOSTICO S.r.l.** elaborato anche sulla base delle "Linee Guida" di Confindustria, si concretizza in un articolato piramidale di principi e procedure, che si può descrivere sinteticamente come segue:

- Codice etico, in esso sono rappresentati i principi generali (trasparenza, correttezza, lealtà) cui si ispira lo svolgimento e la conduzione degli affari;
- Sistema di controllo interno, è l'insieme degli "strumenti" volti a fornire una ragionevole garanzia in ordine al raggiungimento degli obiettivi di efficienza e di efficacia operativa, affidabilità delle informazioni finanziarie e gestionali, rispetto delle leggi e dei regolamenti, nonché salvaguardia del patrimonio sociale anche contro possibili frodi. Il sistema di controllo interno si fonda e si qualifica su alcuni principi generali, appositamente definiti nell'ambito del Modello Organizzativo il cui campo di applicazione si estende trasversalmente a tutte le diverse funzioni della Società.
- Attività di controllo interno, sono state elaborate per tutti i processi operativi a rischio e per i processi strumentali. Tali attività presentano un'analoga struttura, che si sostanzia in un complesso di regole volte ad individuare le principali fasi di ogni processo, i reati che possono essere commessi in relazione ai singoli processi, le specifiche attività di controllo per prevenire ragionevolmente i correlativi rischi di reato, nonché appositi flussi informativi verso l'Organismo di Vigilanza al fine di evidenziare situazioni di eventuale inosservanza delle procedure stabilite nei modelli di organizzazione. Gli schemi di controllo interno sono stati elaborati alla luce di tre regole cardine e precisamente:
- La separazione dei ruoli nello svolgimento delle attività inerenti ai processi;
- La c.d. "tracciabilità" delle scelte, cioè la costante visibilità delle stesse (ad es. mediante apposite evidenze documentali), per consentire l'individuazione di precisi "punti" di responsabilità e la "motivazione" delle scelte stesse;
- L'oggettivazione dei processi decisionali, nel senso di prevedere che, nell'assumere decisioni, si prescinda da valutazioni meramente soggettive, facendosi invece riferimento a criteri precostituiti.

Il Modello Organizzativo, peraltro, si completa con l'istituzione di un Organismo di Vigilanza, che, come previsto dall'art. 6 del Decreto legislativo 231/2001, deve essere dotato di autonomi poteri di iniziativa e di controllo, al fine di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello Organizzativo stesso curandone altresì il costante aggiornamento. Tale profilo è ulteriore condizione per l'applicazione dell'esimente prevista dalla norma.

Il Modello Organizzativo è cosi schematizzabile:

Identificativo della Parte	Titolo	Contenuti	Allegati
A CONTROLLO MIGLIORAMEMTO	Parte Generale	La responsabilità penale degli enti	Allegato 1: Fattispecie di reato
		Il Modello Organizzativo	Allegato 2: Aree a rischio reati
		Organismo di Vigilanza	
		Codice Etico (Rinvio)	
		Sistema Disciplinare	
B	Codice Etico		Allegato 3: Codice etico
C	Parte Speciale	Sezione Introduttiva	
		Reati contro la PA	
		Reati Societari	
		Sicurezza	
		Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita; Falsità in segni di riconoscimento, delitti contro l'industria e commercio;	
		Reati Informatici	
		Reati Ambientali	

1.3 INTEGRABILITA' CON GLI ALTRI SISTEMI DI GESTIONE

Per rendere il Modello Organizzativo 231 formalmente e sostanzialmente simile al proprio Sistema di Gestione interno la società ha scelto di applicare l'Approccio per Processi e la Metodologia PDCA (*Plan-Do-Check-Act*).

1.3.1 APPROCCIO PER PROCESSI

La Società **CENTRO DIAGNOSTICO S.r.l.** dopo aver individuato le attività nel cui ambito possano essere commessi reati rilevanti, ha utilizzato l'approccio per processi che evidenzia anche le interazioni tra i vari processi e ne consente la loro gestione al fine ottenere la deresponsabilizzazione amministrativa delle persone giuridiche e della Società stessa.

1.3.2 METODOLOGIA APPLICATA PER LA DEFINIZIONE DEL MODELLO ORGANIZZATIVO 231

La Società **CENTRO DIAGNOSTICO S.r.l.** per stabilire, documentare, attuare, mantenere attiva e migliorare l'efficacia del Modello Organizzativo, utilizza ove possibile la metodologia PDCA secondo la seguente corrispondenza di fasi:

ATTIVITA PREVISTE NEL MO	FASI DEL PDCA	RESPONSABILITA
PIANIFICAZIONE	PLAN	Tutte le Funzioni
IMPLEMENTAZIONE	DO	Tutte le Funzioni
CONTROLLO	CHECK	Organo di Vigilanza
MIGLIORAMEMTO	ACT	Tutte le Funzioni

2 SCOPO E CAMPO DI APPLICAZIONE/PRESENTAZIONE E POLITICA DELLA SOCIETA'

2.1 GENERALITA'

Il presente Manuale, descrive la struttura del Modello di Controllo con cui la struttura intende attuare e tenere sotto controllo le proprie attività al fine di prevenire la realizzazione dei reati secondo quanto previsto dal Decreto Legislativo 231/2001 ("Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300").

2.2 SCOPO

Scopo del Modello di Organizzazione, Gestione e Controllo è quello di fornire indicazioni sui contenuti del Decreto Legislativo e sul particolare tipo di responsabilità amministrativa degli enti che esso introduce nel nostro ordinamento per i reati commessi, nel loro interesse o vantaggio, dai propri esponenti o dipendenti. È inoltre volto ad indirizzare le attività interne affinché siano in linea con lo stesso e a vigilare sul suo funzionamento e sulla sua osservanza.

2.2.1 MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Per quanto riguarda la Mappatura dei rischi, sono state identificate delle attività che, esclusivamente in relazione ai loro specifici contenuti, potrebbero essere esposte (o maggiormente esposte) al rischio di commissione dei reati contemplati dal D.Lgs. 231/2001. Per la sua elaborazione, si è proceduto - previa l'opportuna ricognizione - ad associare ai processi organizzativi interni (nel cui svolgimento, in via teorica, potrebbero integrarsi gli estremi di reato di cui alla normativa in esame) le varie fattispecie di reato considerate dal Decreto. Le aree di rischio individuate sono da intendersi come un complesso in evoluzione, da adeguarsi periodicamente in relazione a modifiche normative e/o a variazioni interne.
Scopo del presente manuale è definire il Modello organizzativo 231 aziendale:

- Definendo un Sistema Organizzativo chiaro e formalizzato;
- assegnando dei poteri (autorizzazioni e firme) coerenti con le responsabilità gestionali della Società;
- stabilendo delle procedure per la registrazione, l'autorizzazione e la verifica di ogni operazione ritenuta critica;
- istituendo un Organismo di Vigilanza dotato di autonomi poteri di iniziativa e controllo;
- definendo le procedure di comunicazione al personale e formando lo stesso sulle caratteristiche del Modello e sulle responsabilità di ognuno per la sua corretta applicazione.

Il modello Organizzativo 231 descritto nel presente manuale è parte integrante del Sistema di Gestione per la Qualità adottato dalla Società.

2.3 APPLICAZIONE

Il modello organizzativo 231 si applica a tutti i settori di attività e a tutti i processi aziendali che presentano potenzialmente dei fattori di rischio in relazione alla realizzazione dei reati previsti dal D.lgs 231/2001.

2.4 PRESENTAZIONE DELLA SOCIETA'

Il Centro Diagnostico Ostiense è una struttura sanitaria poliambulatoriale di 5.000 mq strutturata su 4 piani, nata a Roma nel 1995 da una joint venture tra Ferrovie dello Stato e CDI-Centro Diagnostico Italiano, di Milano. Nel 2000 la Struttura entra a far parte di un prestigioso gruppo di aziende operanti nel settore sanitario a livello nazionale.
Dopo l'ingresso nel gruppo, le attività del Centro si sono progressivamente ampliate: l'intera struttura è stata ristrutturata per una più razionale ed efficiente distribuzione degli spazi, e sono stati attivati nuovi reparti e servizi altamente specializzati.
Tra le tappe più significative:
2001: apertura del reparto di Odontoiatria
2002: attivazione del Centro di Fisioterapia e del reparto di Chirurgia Ambulatoriale
2017: nasce il Polo Pediatrico, dedicato ai pazienti da 0 a 16 anni
A partire dal 2023, il Centro Diagnostico Ostiense ha avviato un profondo processo di modernizzazione strutturale e organizzativa, con l'obiettivo di consolidare il proprio ruolo di punto di riferimento nella sanità ambulatoriale romana.
Il Centro Diagnostico Ostiense si sviluppa su quattro piani, per una superficie complessiva di 5.000 mq, interamente dedicati all'attività sanitaria in regime privato.
Al suo interno trovano spazio:

- ambulatori specialistici
- laboratori di analisi cliniche
- reparto di diagnostica per immagini (Radiologia, TAC, M.O.C., RMN, ecografia)
- reparto di fisioterapia
- reparto di odontoiatria
- unità di chirurgia ambulatoriale PC2 ed endoscopia
- aree dedicate ai programmi di check-up personalizzati e medicina del lavoro
- polo pediatrico

Il Centro è una struttura di nuova concezione, orientata alla prevenzione, diagnosi precoce e terapia personalizzata, dove l'approccio multidisciplinare è al centro dell'attività clinica. I medici operano in équipe coordinate, assicurando un'elevata interdisciplinarità e la presa in carico integrata del paziente.
Tutti i processi, sia sanitari che organizzativi, sono gestiti attraverso l'utilizzo delle più avanzate tecnologie digitali, garantendo efficienza, tracciabilità e sicurezza dei dati.
La qualità, varietà e completezza delle prestazioni offerte – dalla prevenzione fino alla terapia, compresa la chirurgia in regime ambulatoriale – si integrano in un sistema progettato per rispondere in modo tempestivo e appropriato alle esigenze sanitarie di una collettività in continua crescita come quella romana.
Il Centro Diagnostico Ostiense rappresenta oggi un esempio concreto di integrazione tra innovazione tecnologica e competenze professionali, a beneficio dei pazienti.
In virtù della molteplicità delle discipline mediche presenti, la struttura dedica particolare attenzione al mondo delle aziende, dei fondi di assistenza sanitaria integrativa e delle compagnie assicurative, offrendo percorsi sanitari strutturati e flessibili. Tra questi spiccano i check-up interdisciplinari, progettati come veri e propri percorsi di salute: comprendono il coinvolgimento di diversi specialisti e l'esecuzione coordinata di esami biochimici e strumentali, concentrati in una sola mattinata, per rispondere efficacemente alle esigenze di prevenzione delle popolazioni aziendali.
Il Centro Diagnostico Ostiense offre prestazioni in regime privato ed è convenzionato con le più importanti compagnie assicurative e fondi integrativi che prevedono un trattamento di assistenza sia diretta che indiretta.
L'organizzazione e le attività del Centro Diagnostico sono coerenti con quanto prescritto dal Decreto del Commissario ad Acta in merito ai requisiti minimi autorizzativi per l'esercizio delle attività sanitarie e socio sanitarie.
Il Centro Diagnostico Ostiense è un'azienda certificata secondo i seguenti standard:

- UNI EN ISO 9001:2015 – Sistemi di gestione per la qualità per le seguenti attività: Prestazioni ambulatoriali polispecialistiche e di diagnostica strumentale: endoscopia e diagnostica per immagini. Centro analisi. Erogazione e gestione di servizi di medicina del lavoro, valutazione e consulenza della sicurezza sui luoghi di lavoro
- UNI EN ISO 14001:2015 – Sistemi di gestione ambientale
- UNI ISO 45001:2018 – Sistemi di gestione per la salute e sicurezza sul lavoro
- SA 8000:2014 – Sistemi di gestione di responsabilità sociale
- UNI/PdR 125:2022 – Sistemi di gestione per la parità di genere

2.5 MODIFICHE ED INTEGRAZIONI DEL MODELLO

Il presente Modello (in conformità alle prescrizioni dell'art. 6, comma 2, lettera a del Decreto) è un "atto di emanazione dell'organo dirigente" pertanto l'adozione dello stesso, così come le successive modifiche e integrazioni sono rimesse alla competenza della Direzione.
In particolare è demandato alla Direzione stessa il compito di valutare eventuali integrazioni del presente Modello, su segnalazione dell'organismo di Vigilanza in relazione ad ulteriori tipologie di reati che nuove previsioni normative colleghino all'ambito di applicazione del Decreto 231, o in conseguenza di modifiche strutturali dell'organizzazione dell'azienda.

2.6 AGGIORNAMENTO DEL MODELLO

L'adozione e l'efficace attuazione del Modello costituiscono, per espressa previsione legislativa, una responsabilità del Legale Rappresentante. Essendo il presente modello un "atto di emanazione dell'organo dirigente" (in conformità alle prescrizioni dell'art.6, 1° comma, lett. a del decreto) le successive modifiche e integrazioni di carattere sostanziale del modello stesso sono rimesse alla competenza della Direzione. Tale facoltà è giustificata dal fatto che al Modello deve essere garantito un costante e tempestivo adeguamento alle sopravvenute variazioni di natura operativa e/o organizzativa all'interno della Società. Le proposte di modifica ed integrazione del modello potranno essere sottoposte all'OdV da chiunque ne ravvisi l'opportunità e presentate dall'OdV alla Direzione. Successivamente la Direzione stessa valuterà le proposte e provvederà, eventualmente, ad integrare il presente modello, mediante apposita delibera, modificando le parti speciali già previste ovvero, se necessario, disponendone l'inserimento di ulteriori in relazione alle tipologie di reati-presupposto resi tali da nuove normative.

2.7 VERIFICA DEL MODELLO

Il presente modello sarà soggetto a due tipi di verifiche:

- verifiche delle procedure: l'OdV, conformemente ad una propria calendarizzazione, sarà tenuto ad accertare che le singole procedure implementate rispondano costantemente alle esigenze di effettività ed efficacia del modello.
- verifiche sugli atti: eventualmente, ogniqualvolta sia ritenuto necessario per la sussistenza di situazioni di criticità, l'OdV procederà ad un esame degli eventuali atti societari e dei contratti conclusi che abbiano comportato, nelle aree a rischio, mutamenti tali da richiedere una revisione, seppure parziale, del modello. Come esito delle verifiche, l'OdV dovrà stilare un rapporto da sottoporre all'attenzione della Direzione che evidenzi le possibili manchevolezze e suggerisca le azioni da intraprendere.

2.8 DESTINATARI DEL MODELLO

Il modello redatto dalla società **CENTRO DIAGNOSTICO S.r.l.** è destinato a tutti coloro che operano a qualsiasi titolo o ragione in nome e per conto della stessa, indipendentemente dalla tipologia di rapporto instaurato.
Ed in particolare, il modello si applica a coloro che:

- Rivestono funzioni di rappresentanza, amministrazione, direzione o controllo della struttura (di seguito "Esponenti Aziendali")
- Sono sottoposti alla direzione o alla vigilanza di uno dei soggetti di cui al punto che precede (di seguito, complessivamente, "Destinatari");
- A coloro che, pur operando all'esterno della società ne abbiano accettato il contenuto e gli effetti in virtù di specifiche clausole contrattuali e limitatamente allo svolgimento delle attività cui gli stessi sono preposti (di seguito i "Soggetti Esterni").

2.9 LA POLITICA

La politica della società **CENTRO DIAGNOSTICO S.r.l.** è sintetizzabile nei seguenti aspetti:

- Gestire e migliorare costantemente la soddisfazione di tutti coloro che usufruiscono dei servizi erogati, valutata attraverso appositi questionari di soddisfazione;

- Promuovere la costante crescita della professionalità e delle competenze del personale interno, attraverso la continua formazione ed aggiornamento dello stesso;
- Perseguire, compatibilmente con l'ottenimento delle autorizzazioni regionali e locali, l'obiettivo di mantenere attrezzature tecnologicamente all'avanguardia e dia acquistare eventuali nuove apparecchiature.

La politica è quindi quella di assicurare che i servizi erogati siano tesi a soddisfare tutte le esigenze esplicite ed implicite del paziente/cliente, con un approccio orientato alla piena soddisfazione di quest'ultimo, in un'ottica di innovazione e miglioramento continui.
Il D.Lgs. 231/2001 ha messo in evidenza la necessità di definire un preciso e chiaro schema di comportamento inteso ad orientare l'impegno professionale e la condotta di ciascun collaboratore, dipendente, libero professionista nonché qualsiasi altro soggetto operante all'interno della struttura. La società ha adottato il Modello Organizzativo 231 facendo anche riferimento alle linee guida emanate dalla Associazioni di categoria (Linee Guida di Confindustria e AIOP), finalizzato alla prevenzione dei reati previsti dal Decreto Legislativo 231.
In tale contesto è stato inserito ed aggiornato il Codice Etico comportamentale (in seguito, per brevità anche "Codice") nel quale sono rappresentati i principi di generali di trasparenza, correttezza e lealtà cui si ispirano lo svolgimento e la conduzione delle attività.
All'interno del Codice vengono stabilite le regole comportamentali e gli obiettivi da perseguire al fine della prevenzione dei reati previsti dal decreto. E' uno strumento che garantisce la gestione equa ed efficace delle attività di servizio, delle transazioni, delle relazioni umane, che sostiene la reputazione dell'azienda in modo da creare fiducia verso l'esterno, in primis verso gli utenti. L'obiettivo finale è quello di prevenire comportamenti irresponsabili e illeciti di chi opera in nome e per conto della struttura, introducendo una definizione chiara ed esplicita delle responsabilità etiche e sociali di propri dirigenti, quadri, dipendenti ma anche per tutti i soggetti esterni che hanno rapporti con la società **CENTRO DIAGNOSTICO S.r.l.**
Punto di forza del programma di miglioramento aziendale è certamente la formazione/informazione degli addetti in merito all'applicazione del Sistema di Gestione della responsabilità Amministrativa pertanto l'Organizzazione assicura che la propria Politica è compresa, attuata e sostenuta a tutti i livelli.
La politica è condivisa con tutto il personale.

2.10 OBIETTIVI

Organizzativi: Definizione delle responsabilità

- Separazione dei ruoli nello svolgimento delle attività aziendali
- Tracciabilità documentata delle decisioni in modo da poter risalire ad eventuali responsabilità individuali
- Definizione delle procedure per la registrazione, l'autorizzazione e la verifica di ogni operazione definita critica
- Istituzione dell'Organismo di Vigilanza dotato di poteri autonomi di decisione e di controllo

Formativi

- Formazione ed informazione continua del personale per promuovere la conoscenza della normativa ed i contenuti del Modello Organizzativo 231 in modo che tutti i dipendenti siano consapevoli e comprendano gli aspetti dei reati ed i rischi in relazione alla realizzazione di reato previsti dal D.lgs 231
- Divulgazione del Codice Etico nel quale sono rappresentati i principi generali di trasparenza, correttezza e legalità che devono essere alla base delle attività lavorative

Comportamentali

Tutte le azioni e negoziazioni compiute dal personale della società **CENTRO DIAGNOSTICO S.r.l.,** nello svolgimento delle attività lavorative devono essere ispirate alla massima Lealtà, Trasparenza, Correttezza e Professionalità.
In particolare sono interdetti i comportamenti pregiudizievoli al raggiungimento degli obiettivi indicati da Dlgs 231.
Il comportamento corretto è caratterizzato dall'osservanza di quanto stabilito nel Modello Organizzativo 231 e nell'ottemperamento dei valori contenuti nel Codice Etico.
Documenti di riferimento: CE Codice Etico.

3 RIFERIMENTI NORMATIVI

3.1 NORME E LINEE GUIDA

TITOLO	DESCRIZIONE
UNI EN ISO 9001:2015	"Sistemi di gestione per la qualità - Requisiti"
UNI EN ISO 9000:2005	"Sistemi di Gestione per la qualità – Fondamenti e Terminologia";
UNI 10999:2002	"Guida per l'elaborazione dei manuali della qualità"
UNI EN ISO 19011/2012	"Linee guida per audit di sistemi di gestione"
UNI EN ISO 11098:2003	"Linee guida per la rilevazione della soddisfazione del cliente e per la misurazione degli indicatori del relativo processo"
UNI EN ISO 11097:2003	"Indicatori e quadri di gestione per la Qualità –Linee guida Generali"
D. Lgs 81/08	E successive modifiche ed integrazioni "normativa sulla sicurezza del lavoro
D. Lgs. 196/03 RUE Regolamento Europeo 2016/679	Codice in materie di protezione dei dati personali Regolamento Europeo in materia di Privacy
D.Lgs 231/01	Responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica

I riferimenti normativi ivi riportati sono indicativi e non esaustivi.

4 TERMINI E DEFINIZIONI

Nel presente Manuale sono applicati i termini e le definizioni di cui alla ISO 9000:2005 oltre a quelli di seguito riportati:

Terminologia	DEFINIZIONE
Analisi dei Rischi	Attività d'analisi specifica della singola Organizzazione finalizzata a rilevare le attività nel cu ambito possono essere commessi i reati
Audit di sistema di gestione	Processo di verifica sistematico, indipendente e documentato, realizzato al fine di ottenere evidenze oggettive su registrazioni, dichiarazioni di fatti o altre informazioni necessarie a determinare se il sistema di gestione è conforme alle politiche, procedure o requisiti del sistema di gestione adottato dall'organizzazione
Codice Etico	Insieme di diritti, doveri e responsabilità dell'organizzazione nei confronti di terzi interessati quali: dipendenti, clienti, fornitori ecc. e finalizzati a promuovere raccomandare o vietare determinati comportamenti indipendentemente da quanto previsto a livello normativo
Decreto Legislativo 231/2001	Decreto Legislativo 8 giugno 2001 n. 231, "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica"
Direzione	Amministratore Unico
Modello Organizzativo(MO)	Insieme delle strutture delle responsabilità delle modalità di espletamento delle attività e dei protocolli/procedure adottati ed attuati tramite i quali si espletano le attività caratteristiche dell'organizzazione

Organo di vigilanza e controllo	Organismo di vigilanza previsto all'art. 6, comma 1, lettere b) del D.lgs 231/2001 cui è affidato il compito di vigilare sul funzionamento e sull'osservanza del Modello e di curarne l'aggiornamento
Politica per la prevenzione dei reati	Obiettivi ed indirizzi generali di un Organizzazione per quanto riguarda la previsione dei reati espressa in modo formale dalla Direzione
Rischio	Probabilità che sia raggiunta la soglia di commissione di un reato/illecito presupposto della responsabilità amministrativa ai sensi del D.lgs 231/01 e s.m.i
Rischio accettabile	Rischio che può essere ridotto ad un livello che può essere tollerabile per l'organizzazione con i riferimenti agli obblighi di legge e a quanto espresso dal SGRA, ovvero che preveda un sistema di prevenzione tale da non poter essere aggirato se non FRAUDOLENTEMENTE
SGRA	Acronimo che identifica il Sistema di Gestione per la Responsabilità Amministrativa.
Sistema Disciplinare e Sanzionatorio	Il sistema disciplinare di cui all'art. 6 comma 2 lettera e) del D.Lgs 231/01
Società	**CENTRO DIAGNOSTICO S.r.l.**
Soggetti in posizione apicale	I soggetti di cui all'art. 5 lett. a) del D.lgs 231/01
Soggetti sottoposti ad altrui direzione	I soggetti di cui all'art. 5 lett b) del D.lgs 231/01
Stakeholder	Persone fisiche o giuridiche, che intrattengono rapporti con la Società a qualunque titolo
Procedura	Modo specificato per svolgere un'attività o un processo (3.4.1).
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
Qualità	Grado in cui un insieme di caratteristiche (3.5.1) intrinseche soddisfa i requisiti
Riesame	Attività effettuata per riscontrare l'idoneità, l'adeguatezza e l'efficacia (3.2.14) di qualcosa a conseguire gli obiettivi stabiliti
Rilavorazione	Azione su un prodotto (3.4.2) non conforme per renderlo conforme ai requisiti.
Rintracciabilità	Capacità di risalire alla storia, all'applicazione o all'ubicazione di ciò che si sta considerando
Specifica	Documento (3.7.2) che stabilisce dei requisiti (3.1.2)
Struttura organizzativa	Insieme di responsabilità, autorità e interrelazioni tra persone

5 SISTEMA DI GESTIONE PER LA RESPONSABILITA' AMMINISTRATIVA (SGRA)

5.1 REQUISITI GENERALI

L'analisi effettuata ha portato alla identificazione delle attività che costituiscono le 4 fasi della metodologia PDCA

PLAN

Identificare i processi tramite i quali l'organizzazione svolge la sua attività:

- Stabilire la sequenza e l'interazione tra i processi.
- Definire tracciabilità e trasparenza di ogni attività
- Identificare i processi e le attività sensibili intesi quali processi/attività nel cui ambito possono essere commessi reati/illeciti rilevanti ex DLgs 231/01
- Valutare, per ogni processo le attività a potenziale pericolo di reato/illecito nell'interesse o a vantaggio dell'organizzazione ed il livello di rischio di commissione dei reati/illeciti in base ai criteri e alle metodologie di gestione in essere
- Predisporre le azioni necessarie per conseguire i risultati pianificati e l'ottimizzazione del SGRA.

DO

- Redigere l'analisi dei rischi;
- Garantire tracciabilità e trasparenza di qualsiasi attività;
- Definire le procedure di Controllo Interno;
- Formalizzare in un "Codice Etico" i principi d'autoregolazione dell'organizzazione al suo interno e dei rapporti con i terzi;
- Adottare, diffondere e dare concreta attuazione al Codice Etico di cui al precedente punto;
- Definire idonei mansionari che prevedano modalità di conferimento e revoca di responsabilità, deleghe e procure, facoltà e compiti nonché di attribuzione delle specifiche mansioni;
- Eseguire corsi di Formazione, Informazione e Comunicazione;
- Assicurare l'adeguata disponibilità di Risorse;
- Creare l'Organismo di Vigilanza.

CHECK

- Affidare all'Organismo di Vigilanza il compito di vigilare sul funzionamento e sull'osservanza del SGRA e di verificarne il costante aggiornamento ed adeguamento, sulla base dell'evoluzione della legislazione, oltre che sulla base dell'evoluzione dell'organizzazione stessa.
- Implementazione del Programma di Audit Interni per verificare che le azioni pianificate ed implementate sono atte a prevenire la commissione dei reati ed in caso negativo reiterazione del processo PDCA.

ACT

- Standardizzare delle azioni pianificate, implementate e controllate;
- Aggiornare il SGRA con l'evoluzione legislativa, con i risultati dell'Analisi dei Rischi e con l'attività dell'organizzazione;
- Attuazione del sistema disciplinare e sanzionatorio.

Qualora si constati la necessità di adeguamento alle azioni intraprese al fine di prevenire i reati, è necessario promuovere la reiterazione del ciclo PDCA.

5.2 IL SISTEMA DI DELEGHE E PROCURE

La Direzione, nella persona del Legale Rappresentante, è l'organo preposto ad attribuire ed approvare formalmente le deleghe ed i poteri di firma. Il potere di rappresentare la Società è conferito in coerenza con il livello gerarchico del destinatario della delega o della procura o in relazione a specifiche attività. Se del caso, vengono di volta in volta conferite procure speciali ai responsabili di alcune funzioni in stretta relazione con le mansioni e l'attività svolta da ciascuno di essi. Le deleghe e le procure, quindi, sono comunicate formalmente ai singoli destinatari. Le procure vengono poi depositate presso il competente Ufficio Registro Imprese. Ciascuno di questi atti di delega o conferimento di poteri di firma fornisce, quindi, le seguenti indicazioni:

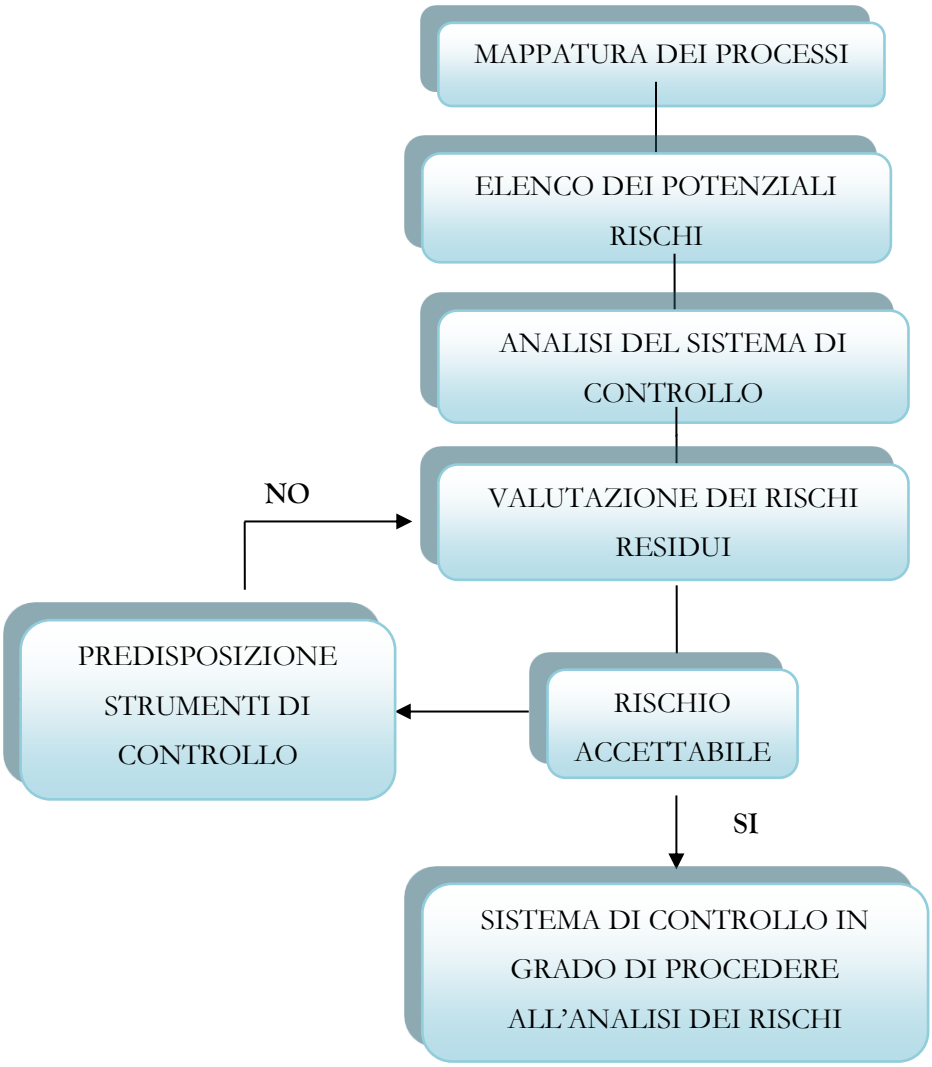
- ✓ soggetto delegante e fonte del suo potere di delega o procura;
- ✓ soggetto delegato;
- ✓ oggetto della delega/procura;
- ✓ limiti di valore entro cui il delegato è legittimato ad esercitare il potere conferito.

6 PIANIFICAZIONE DELLA IDENTIFICAZIONE DEI POSSIBILI REATI E D.LGS 231/01

(Fase PDCA:PLAN)

6.1 GENERALITA'

Il Decreto 231/2001, all'art. 6, co. 2, indica le caratteristiche essenziali per la costruzione di un modello di organizzazione, gestione e controllo. In particolare, la lettera a) della citata disposizione si riferisce espressamente, sebbene con l'utilizzo di una terminologia ed esposizione estranea alla pratica aziendale, ad un tipico sistema di gestione dei rischi (*risk management*). La norma segnala infatti espressamente come "l'identificazione dei rischi": ossia l'analisi del contesto aziendale per evidenziare dove (in quale area/settore di attività) e secondo quali modalità si possono verificare eventi pregiudizievoli per gli obiettivi indicati dal D.lgs 231/2001.
Nel diagramma di flusso che segue sono rappresentate le attività della valutazione dei rischi adottate dalla società **CENTRO DIAGNOSTICO S.r.l.** Attraverso la valutazione della situazione aziendale, della società, in relazione ai possibili reati, sono stati definiti rischi ed è stata determinata di conseguenza la necessità di predisposizione di strumenti di controllo aggiuntivi rispetto a quelli già presenti in azienda.



Se il rischio è accettabile il sistema di controllo è in grado di procedere all'analisi dettagliata dei rischi connessi alle diverse fasi dei processi aziendali, verificando e individuando le aree che risultano interessate dalle potenziali casistiche di reato.
Successivamente vengono evidenziate le tipologie di reato connesse alle specifiche attività, individuando le risorse che, potendo essere coinvolte nella gestione del rischio, devono essere oggetto del sistema di controllo pianificato.
Per ogni tipologia di reato/attività, viene assegnato un valore di "accettabilità" del rischio in base al livello di efficacia del sistema di controllo messo in atto per la gestione della specifica attività.
Per la tipologia di reati quali la violazione delle norme sulla sicurezza sul lavoro, quasi tutte le attività dell'azienda sono considerate a rischio.
L'applicazione della presente procedura di identificazione e valutazione dei rischi è necessaria durante le seguenti fasi:

- Durante la fase iniziale di implementazione del Modello Organizzativo 231, in conformità con il D.Lgs. 231/2001, in quanto costituisce la base per la definizione degli obiettivi e programmi ambientali e comunque prima di ogni riesame del sistema al fine di garantire un aggiornamento sistematico della valutazione dei rischi;
- Ogni qualvolta avvenga una variazione di processo, di prodotto o del sito o contesto in cui la struttura opera, quali ad esempio modifiche nel quadro legislativo di riferimento;
- Ad ogni riesame di Sistema.

6.2 DEFINIZIONE DI RISCHIO ACCETTABILE

Un concetto assolutamente nodale nella costruzione del sistema di controllo preventivo è quello di rischio accettabile.
Allo scopo è importante considerare da una parte l'impossibilità del "rischio zero" e dall'altra la quantità/qualità delle misure di prevenzione da introdurre per evitare o contenere gli effetti del danno (danno alla PA, danno economico-patrimoniale alla struttura, danno all'operatore, all'utente). Occorre pertanto definire una soglia di rischio accettabile che scaturisca dal bilanciamento sostenibile – dalla struttura – tra i costi (dei controlli e misure prevedibili da istituire) e i benefici (riduzione dei rischi).

In relazione al rischio di commissione della fattispecie di reato contemplate del D.L.gs. n. 231/2001 o di violazione dei principi etico-comportamentali previsti, nella struttura la soglia concettuale di accettabilità è rappresentata da un ***"sistema di prevenzione tale da non poter essere aggirato se non intenzionalmente".***
Pertanto il sistema di controllo preventivo deve essere in grado di:

- escludere che un qualunque soggetto operante all'interno delle strutture possa giustificare la propria condotta adducendo l'ignoranza delle direttive aziendali della struttura;
- evitare che, nella normalità dei casi, il reato o la violazione ai principi etico-comportamentali previsti possa essere causato dall'errore umano (dovuto anche a negligenza o imperizia) o dalla non ottemperanza alle politiche e alle procedure aziendali.

Data la definizione di rischio accettabile, si è stabilito che i rischi possono essere di tre livelli di importanza: accettabili, rilevanti e critici. In caso di reati ex D.Lgs 231/01 la cui probabilità di accadimento è valutata nulla o trascurabile, il rischio è considerato direttamente accettabile. Diversamente nei casi di reato di omicidio colposo e lesioni personali colpose commessi con violazione delle norme in materia di salute e sicurezza sul lavoro, la soglia concettuale di accettabilità, agli effetti esimenti del D.Lgs 231/2001, è rappresentata dalla realizzazione di una condotta (non accompagnata dalla volontà dell'evento-morte/lesioni personali) violativa del modello organizzativo di prevenzione (e dei sottostanti adempimenti obbligatori prescritti dalle norme prevenzionistiche) nonostante la puntuale osservanza degli obblighi di vigilanza previsti dal D.lgs. 231/2001 da parte dell'apposito organismo. Ciò in quanto l'elusione fraudolenta dei modelli organizzativi appare incompatibile con l'elemento soggettivo dei reati di omicidio colposo e lesioni personali colpose, di cui agli artt. 589 e 590 del codice penale.

6.3 IL LIVELLO DEI RISCHI E LA MATRICE DI VALUTAZIONE DEL RISCHIO

La metodologia adottata è basata sui seguenti passi:

a) Analisi dei rischi applicata ad un processo individua i rischi possibili rispetto ai valori etici a ai reati previsti dal D.Lgs. 231/01.
b) I rischi individuati vengono "pesati" e cioè ad ogni rischio viene assegnato un livello di importanza, calcolato come prodotto tra probabilità ed entità del danno causato;
c) La probabilità è un valore determinato dall'esperienza degli operatori interessati. Può assumere tre livelli: alta, media, bassa più il caso di probabilità nulla; l'attribuzione del livello viene esplicato e concordato anche con la collaborazione dei responsabili del processo.
d) L'entità del danno è quella stabilita a quattro danni possibili: a) danno alla P.A., b) danno economico-patrimoniale alla struttura, c) danno all'operatore, d) danno all'utente; si definisce entità del danno alta se si possono verificare quattro o tutti i tipi di danno, media se si verificano uno o due dei quattro tipi di danno e bassa se non si verifica nessuno dei quattro danni individuati.
e) I rischi che cadono in un livello di importanza accettabile, vengono considerati in linea con le procedure adottate, mentre i rischi che risultano in un livello critico o rilevante vengono sottoposti ad una misura preventiva.

6.3.1 STRUMENTO DI LAVORO

Sono evidenziati:

- I modi ipotizzati di commissione dell'illecito;
- Gli effetti derivanti dalla commissione dell'illecito;
- Le misure preventive già in atto;
- La gravità dell'evento;
- La probabilità di accadimento;
- La capacità di intercettazione dell'evento;
- L'indice di priorità del rischio.

6.4 POSSIBILI REATI PREVISTI DAL D.LGS 231/01

I reati presupposti previsti dal DLgs 231/01 e da altre normative ad esso collegate sono di seguito elencati. Una descrizione dettagliata di tali reati viene presentata nell'Allegato 1 – I Reati rilevanti ai sensi del D.Lgs 231/2001 al presente Manuale.

1. Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24, Decreto 231) [Articolo modificato dalla L. n. 161/2017 e dal D.Lgs n. 75/2020]

2. Delitti informatici e trattamento illecito di dati (art. 24-bis, Decreto 231) [articolo aggiunto dalla L. n. 48/2008]

3. Delitti di criminalità organizzata (art. 24-ter, Decreto 231) [articolo aggiunto dalla L. n. 94/2009]

4. Peculato, concussione, induzione indebita a dare o promettere altra utilità, corruzione e abuso d'ufficio (art. 25, Decreto 231) [articolo modificato dalla L. n. 190/2012, dalla L. n. 3/2019 e dal D.Lgs. n. 75/2020]

5. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis, Decreto 231) [articolo aggiunto dal D.L. n. 350/2001, convertito con modificazioni dalla L. n. 409/2001; modificato dalla L. n. 99/2009, modificato dal D.Lgs 125/2016]

6. Delitti contro l'industria e il commercio (art. 25-bis.1, Decreto 231) [articolo aggiunto dalla L. n. 99/2009]

7. Reati societari (art. 25-ter, Decreto 231) [articolo aggiunto dal D.Lgs. n. 61/2002, modificato da ultimo dalla L. n. 190/2012, dalla L. n. 69/2015 e dal D.Lgs 15 marzo 2017, n. 38]

8. Delitti con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (art. 25-quater, Decreto 231) [articolo aggiunto dalla L. n. 7/2003]

9. Pratiche di mutilazione degli organi genitali femminili (art. 583-bis c.p.) (art. 25-quater.1, Decreto 231) [articolo aggiunto dalla L. n. 7/2006]

10. Delitti contro la personalità individuale (art. 25-quinquies, Decreto 231) [articolo aggiunto dalla L. n. 228/2003, come da ultimo modificato dalla L. n. 199/2016]

11. Reati di abuso di mercato (art. 25-sexies, Decreto 231) [articolo aggiunto dalla L. n. 62/2005]

12. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies, Decreto 231) [articolo aggiunto dalla L. n. 123/2007 e successivamente sostituito dalla L.n.81/2008]

13. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies, Decreto 231) [articolo aggiunto dal D.Lgs. n. 231/2007; modificato dalla L. n. 186/2014]

14. Delitti in materia di violazione del diritto d'autore (art. 25-novies, Decreto 231) [articolo aggiunto dalla L. n. 99/2009]

15. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies, Decreto 231) [articolo aggiunto dalla L. n. 116/2009]

16. Reati ambientali (art. 25-undecies, Decreto 231) [articolo aggiunto dal D.Lgs. n. 121/2011 e modificato dalla L. n. 68/2015]

17. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies, Decreto 231) [articolo aggiunto dal D.Lgs. n. 109/2012, come da ultimo modificato dalla L. n. 161/017]

18. Reati di razzismo e xenofobia (art. 25-terdecies, Decreto 231) [articolo aggiunto dalla L. n. 167/2017]

19. Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-quaterdecies, Decreto 231) [articolo aggiunto dalla L. n. 39/2019].

20. Reati transnazionali (L. n. 146/2006).

21. Reati Tributari (art.25 quinquiesdecies Decreto 231) [articolo aggiunto dalla L. n. 157/2019 e dal D.lgs. n. 75/2020]

22. Contrabbando (Art. 25 sexiesdecies, D.Lgs 231/2001) [art. aggiunto dalla D.Lgs. n. 75/2020]

Il sistema organizzativo e gestionale dell'organizzazione è mirato a garantire lo svolgimento delle attività nel rispetto della normativa vigente e delle prescrizioni del Codice Etico.

6.5 ASPETTI GENERALI

La documentazione del SGRA della società **CENTRO DIAGNOSTICO S.r.l.** comprende:

- La documentazione del SGRA della società;

- Il Manuale del Sistema di Gestione per la responsabilità Amministrativa, Rappresentativo del Modello di organizzazione, gestione e controllo realizzato dalla società **CENTRO DIAGNOSTICO S.r.l.** comprensivo del ***Sistema disciplinare e sanzionatorio;***
- Dichiarazioni documentate sulla politica per la responsabilità amministrativa riportate nel Codice Etico;
- Procedure del sistema di gestione per la qualità;
- Funzionamento e controllo dei Processi e degli Audit
- Registrazioni del sistema qualità, della sicurezza, della privacy e del sistema di gestione per la responsabilità amministrativa.

Il manuale organizzativo della struttura per prevenire i reati ex D.lgs. 231/01 richiama ed include:

- La descrizione dei processi e della loro interazione, con l'indicazione degli impatti diretti e indiretti che questi possono avere sulla commissione dei reati;
- L'analisi dei rischi;
- Le procedure, i protocolli e le misure predisposte per il SGRA;
- L'atto istitutivo dell'Organismo di Vigilanza inclusa l'individuazione e le modalità di trasmissione dei flussi informativi obbligatori;
- La pianificazione e la registrazione della formazione del personale come descritto nel sistema qualità.

6.6 LE PROCEDURE

Le attività della società **CENTRO DIAGNOSTICO S.r.l.** soggette ad eventuale rischio di reato sono regolamentate dalle procedure di controllo interno e dalle procedure del Sistema di Gestione.
La società per ogni processo individuato ha definito procedure di controllo interno, finalizzate alla corretta gestione del processo stesso sulla base dei seguenti criteri:

- Le scelte operative sono rese tracciabili in termini di caratteristiche e motivazioni e devono essere individuabili coloro che hanno utilizzato, effettuato e verificato le singole attività;
- Lo scambio di informazioni fra fasi/processi contigui prevede meccanismi per garantire l'integrità e la completezza dei dati gestiti;
- Le risorse umane sono selezionate, assunte e gestite secondo criteri di trasparenza e in coerenza con i valori etici e gli obiettivi definiti dall'azienda;
- Periodicamente, le conoscenze e le competenze professionali disponibili nei settori operativi, sono analizzate in termini di congruenza rispetto agli obiettivi assegnati;
- Il personale è formato e addestrato per lo svolgimento delle mansioni assegnate;
- L'acquisizione di beni e servizi per il funzionamento aziendale avviene sulla base di analisi dei fabbisogni e da fonti adeguatamente selezionate e monitorate.

In ogni procedura (sia per i processi operativi che per quelli strumentali) sono individuati:

- Le attività di controllo, volte a contrastare le possibilità di reato descritte precedentemente;
- Le indicazioni comportamentali, per evitare il generarsi di situazioni ambientali "compatibili" con i reati ("cosa non fare");
- I flussi informativi verso l'Organismo di Vigilanza per evidenziare le aree a rischio e agevolare l'attività di vigilanza sull'efficacia del Modello Organizzativo "231".

Il controllo delle attività sensibili e i flussi informativi sono rappresentati nelle diverse procedure di controllo interno descritte di seguito nel presente Manuale:

- Processo di erogazione dei servizi;
- Processo amministrativo e finanziario (registrazione, redazione e controllo dei documenti contabili e extra contabili)
- Processo di gestione delle risorse umane
- Processo di valutazione dei rischi sulla salute e sicurezza sul lavoro e sugli aspetti ambientali
- Consulenze e prestazioni professionali
- Autorizzazioni e rapporti con le istituzioni
- Accordi transattivi

Le procedure di controllo interno del Modello Organizzativo 231 sono strettamente correlate alle procedure del Sistema di Gestione per la Qualità adottato dalla società **CENTRO DIAGNOSTICO S.r.l.** e ne fanno parte integrante attraverso specifici riferimenti nel presente Manuale.
Tali procedure sono parte integrante del Modello Organizzativo 231 per quello che riguarda:

- La verificabilità e documentabilità di ogni operazione rilevante ai fini del D.Lgs. 231/01;
- Il rispetto del principio della separazione delle funzioni;

- La definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
- I flussi informativi interni ed esterni verso e dall'Organismo di Vigilanza;
- Le verifiche ispettive;
- La responsabilità del personale.

Per quanto riguarda la gestione e la registrazione dei documenti del Sistema di Gestione della responsabilità amministrativa si fa riferimento alla procedura di gestione e registrazione dei documenti disciplinata all'interno del sistema di gestione della qualità.

6.7 TENUTA SOTTO CONTROLLO DEI DOCUMENTI

A tal fine la società **CENTRO DIAGNOSTICO S.r.l.** si è dotata di una procedura in cui sono definite le modalità di:

- Approvazione dei documenti per la loro adeguatezza, prima della relativa emissione;
- Riesame ed aggiornamento, per quanto necessario, e approvazione dei documenti;
- Assicurare che le modifiche e lo stato di revisione vigente dei documenti siano identificati;
- Assicurare che le versioni pertinenti dei documenti applicabili siano disponibili nei punti di utilizzazione;
- Assicurare che i documenti rimangano leggibili e facilmente identificabili;
- Prevenzione dell'utilizzazione involontaria dei documenti obsoleti, e di adottare una loro adeguata identificazione, qualora siano conservati per qualsiasi scopo.

6.8 L'ADOZIONE DEL MODELLO

La predisposizione del Modello ha richiesto una serie di attività volte all'aggiornamento e all'adeguamento del sistema di prevenzione e di gestione dei rischi alle disposizioni del Decreto. L'analisi del contesto aziendale è stata attuata attraverso il preventivo esame della documentazione (organigrammi, attività della struttura, processi principali, sistema delle deleghe, Statuti, procedure aziendali, ecc.) e una serie di interviste con i soggetti chiave operanti nelle aree maggiormente esposte al rischio di commissione di Reati, individuate tramite il suddetto esame. L'analisi svolta è stata funzionale all'identificazione dei processi aziendali esposti ai rischi di Reato e alla verifica dell'efficacia dei controlli già esistenti al fine di garantire la conformità alla legge. A seguito di tale attività, la società **CENTRO DIAGNOSTICO S.r.l.** con delibera del Legale Rappresentante, ha adottato il presente Modello. Contestualmente, tutti i soggetti coinvolti in sede di approvazione hanno dichiarato di impegnarsi al rispetto dello stesso e hanno preso atto della sua adozione.

7 CONTROLLO DELLA VALIDITA' DEL SISTEMA DI GESTIONE (FASE PDCA:CHECK)

L'Organismo di Vigilanza, dotato di autonomi poteri di iniziativa e controllo, ha la responsabilità di vigilare sul funzionamento del Sistema di Gestione per la responsabilità Amministrativa (SGRA) e di verificarne il costante aggiornamento e adeguamento sulla base dell'evoluzione della legislazione, oltre che sulla base dell'evoluzione dell'Organizzazione stessa.
Per vigilare sull'effettività del Modello Organizzativo, che si sostanzia nella verifica della coerenza tra i comportamenti concreti ed il Modello istituito, l'Organismo di Vigilanza:
Pianifica e conduce attività di Audit.
Scopo principale dell'attività di Audit è la:

- verifica dell'attuazione e dell'effettiva funzionalità delle soluzioni proposte;
- valutazione dell'adeguatezza del Modello nella sua reale capacità di prevenire i comportamenti non voluti.

In caso di Non Conformità, il Responsabile dell'area sottoposta ad *Audit* deve assicurare che ogni correzione ed azione correttiva, necessaria per eliminare la Non Conformità rilevante e la sua causa, vengano effettuate senza indebito ritardo.
L'organismo di vigilanza deve verificare la validità dell'AZIONE Correttiva apportata e discuterne durante il riesame della Direzione.
Qualora l'Organismo di Vigilanza constati la necessità di adeguamento del Modello Organizzativo, al fine di prevenire i reati, deve promuovere la reiterazione del ciclo PDCA.

Inoltre l'Organismo di Vigilanza utilizza come strumenti di controllo e azione quelli propri del sistema di gestione per la qualità, quali le non conformità, le Azioni Correttive e Preventive, i Piani di Attività quali il Piano di formazione e il Programma *Audit*, il Riesame della Direzione e il rapporto di adeguatezza del Sistema.

7.1 DOCUMENTI RELATIVI AL PROGRAMMA DI AUDIT INTERNI

A tal fine la società **CENTRO DIAGNOSTICO S.r.l.** ha adottato:

- Programma di Audit Interno;
- Rapporto di Audit Interno.

7.2 ATTUAZIONE E STANDARDIZZAZIONE DEL SISTEMA DI GESTIONE

Tutte le funzioni aziendali, ciascuna per il proprio campo di attività, sono responsabili della osservanza nel Manuale del Modello Organizzativo.
Quando tutto quello che è stato pianificato ed attuato è stato sottoposto a dovuto controllo con esito positivo, si procede alla:

- Standardizzazione del sistema tramite la conferma delle procedure definite.

In base all'evoluzione legislativa, ai risultati dell'Analisi dei Rischi e eventuali cambiamenti dell'attività dell'organizzazione è necessario procedere all'aggiornamento del sistema per la Responsabilità Amministrativa SGRA e all'attuazione del Sistema Disciplinare e del Meccanismo Sanzionatorio.
Le attività sensibili e i flussi informativi sono monitorizzati tramite le procedure di Controllo interno e del Sistema di Gestione per la qualità allegate al presente manuale.

8 RESPONSABILITA' DELLA DIREZIONE

8.1 IL SISTEMA DEI POTERI

Il sistema dei poteri deve essere coerente rispetto ai seguenti principi ispiratori:

- corretta allocazione dei poteri rispetto alle finalità ed all'articolazione interna;
- coerenza tra le responsabilità organizzative e gestionali assegnate ed i poteri;
- puntuale indicazione delle soglie di approvazione delle spese;
- separatezza delle funzioni.

Nel rispetto di tali principi, la società si è dotata di un sistema di deleghe strutturate in modo ritenuto coerente con la missione e le responsabilità dei singoli organi/funzioni interne. Per prevenire efficacemente la commissione dei reati, il Sistema dei poteri è costruito in modo da regolamentare l'attuazione delle decisioni della società **CENTRO DIAGNOSTICO S.r.l.** e rendere documentabili e verificabili le diverse fasi nelle quali si articola il processo decisionale nelle singole unità interne. Per quanto inoltre attiene ai criteri che consentono di individuare, fermo restando il dettato normativo di cui all'art. 5 del Decreto e la relativa prassi applicativa, i soggetti in posizione apicale (per i quali si rinvia al precedente capitolo "Generalità"), essi possono essere così sintetizzati:

- collocazione gerarchica al vertice della struttura o al primo livello di riporto;
- assegnazione di poteri di spesa e di deleghe che consentano di svolgere talune attività, anche verso l'esterno, con un certo margine di autonomia.

I predetti requisiti devono sussistere congiuntamente e non sono alternativi. È pertanto possibile identificare i soggetti apicali avvalendosi dell'organigramma aziendale.

8.2 IMPEGNO DELLA DIREZIONE

Il sistema di controllo interno è definito come processo presidiato dalla Direzione e dagli altri membri della struttura aziendale, che si prefigge di fornire una ragionevole certezza in merito al conseguimento dei seguenti obiettivi:

- Efficacia ed efficienza delle attività operative;
- Affidabilità delle informazioni e delle reportistica economico/finanziaria ove richiesta da enti preposti;
- Conformità alle leggi e ai regolamenti
- Salvaguardia del patrimonio aziendale.

Il sistema di controllo interno si qualifica con principi generali il cui campo di applicazione si estende con continuità attraverso i diversi livelli organizzativi.

Il sistema di controllo interno è integrato con i diversi processi aziendali sia di natura operativa che gestionale. In particolare i processi gestionali di controllo delle attività sono strutturati secondo quanto previsto dal sistema documentale del Sistema di gestione per qualità e DPS per la protezione dei dati personali in conformità al nuovo regolamento Europeo Rue 679/2016.

8.3 CODICE ETICO E POLITICA PER LA RESPONSABILITA' AMMINISTRATIVA

Un sistema di gestione per la Responsabilità amministrativa deve prevenire i reati previsti dal D.lgs 231/01 tramite la chiara definizione delle responsabilità, la tracciabilità di tutte le attività e la creazione di un opportuno Organismo di Vigilanza.
L'impegno della società **CENTRO DIAGNOSTICO S.r.l.** in tal senso, è rivolto:

- Alla formazione/informazione continua del personale per promuovere la conoscenza della normativa, i risvolti pratici che da essa discendono ed i contenuti del presente Modello Organizzativo.
- Divulgazione del Codice Etico nel quale sono rappresentati i principi generali di trasparenza, correttezza e legalità che devono essere alla base della conduzione delle attività aziendali
- Esigere la tracciabilità delle operazioni 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.

Mentre Il Modello Organizzativo si pone come obiettivo quello di prevenire, per quanto possibile, la commissione di Reati, attraverso la previsione di regole di comportamento specifiche, Il Codice Etico è, invece, finalizzato alla promozione di una deontologia aziendale, che rappresenta uno strumento di portata generale. Entrambi sono strettamente integrati tra loro e formano un corpus unico e coerente di norme interne finalizzate ad incentivare la cultura dell'etica e della trasparenza aziendale.

9 ORGANISMO DI VIGILANZA

L'Organismo di vigilanza è l'organismo dell'Ente che:

- ✓ Ha il compito di vigilare sul funzionamento e l'osservanza del Modello;
- ✓ È dotato di autonomi poteri di iniziativa e di controllo;
- ✓ Cura l'aggiornamento del Modello;
- ✓ Relaziona i vertici aziendali; - riceve le segnalazioni dai Destinatari del Modello.

Il sistema di controllo è soggetto ad attività di supervisione continua per le valutazioni periodiche ed il costante adeguamento.
Responsabile del controllo è in prima istanza l'Organismo di Vigilanza che raccoglie tutte le informazioni sull'andamento del Modello Organizzativo previste del sistema di controllo interno, le esamina ed esprime un parere di conformità che viene sottoposto alla Direzione. Ulteriormente l'ODV, in base agli esiti dell'attività di riesame del MO, può fornire delle indicazioni alla Direzione su eventuali attività finalizzate o al rispetto della conformità o al miglioramento del Modello stesso.
In affiancamento all'ODV è prevista la figura del responsabile del Modello Organizzativo 231 al quale competono funzioni di assistenza alla raccolta delle informazioni, all'organizzazione dell'attività dell'ODV e in generale come primo livello di controllo del sistema anche per dare ulteriore garanzia in termini di sorveglianza dell'intero processo organizzativo.
I flussi informativi, le segnalazioni, gli indicatori dei processi sensibili, le non conformità e le azioni correttive di competenza dell'ODV sono gestiti attraverso le specifiche procedure, istruzioni operative e moduli del sistema di gestione.

9.1 RUOLO E COMPOSIZIONE

L'art. 6 del Decreto legislativo 231/2001, nel ricondurre l'esonero da responsabilità dell'ente all'adozione e alla efficace attuazione di un modello di organizzazione, gestione e controllo idoneo a prevenire la realizzazione degli illeciti penali considerati da tale normativa, ha previsto l'istituzione di un Organismo di Vigilanza interno all'ente cui è assegnato specificamente il "compito di vigilare sul funzionamento e l'osservanza del modello organizzativo e di curarne il relativo aggiornamento".
I compiti assegnati all' OdV richiedono che lo stesso sia dotato di autonomi poteri di iniziativa e controllo.
L'organismo di Vigilanza si caratterizza per i seguenti requisiti:

- **Autonomia e indipendenza**
  I requisiti di autonomia e indipendenza sono fondamentali affinché l'Odv non sia direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo. Tali requisiti si possono ottenere, tra l'altro, garantendo l'insindacabilità delle scelte dell'OdV da parte degli organi dell'ente e prevedendo un'attività di reportistica alla Direzione.
- **Professionalità**
  L'OdV deve possedere al suo interno competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere; tali caratteristiche, unite all'indipendenza, garantiscono l'obiettività di giudizio.
- **Continuità di azione**
  L'OdV deve:
  - Lavorare costantemente sulla vigilanza del Modello Organizzativo con i necessari poteri di indagine;
  - Essere una struttura interna, in modo da garantire continuità dell'attività di vigilanza;
  - Curare l'attuazione del Modello Organizzativo e assicurarne il costante aggiornamento;
  - Non svolgere mansioni operative che possono condizionare la visione d'insieme delle attività aziendali che ad esso si richiede.

In tale quadro ed in relazione alle dimensioni ed alla esigua complessità delle attività svolte dalla società, l'OdV assume la veste dell'organo dirigente come previsto dal D.lgs 231/2001 all'art. 6 co.4. Come detto in precedenza, a supporto della Direzione, è prevista la figura del responsabile del Modello Organizzativo 231 il quale assume la funzione di controllo di primo livello in modo da creare una sorta di doppio controllo con la Direzione e garantire ulteriormente l'efficacia del Modello.

9.2 RISERVATEZZA

I membri dell'OdV sono tenuti al segreto in ordine alle notizie ed informazioni acquisite nell'esercizio delle loro funzioni. I membri dell'OdV assicurano la riservatezza delle informazioni di cui vengono in possesso, in particolare se relative alle segnalazioni che agli stessi dovessero pervenire in ordine a presunte violazioni del Modello Organizzativo. Inoltre, i membri dell'OdV si astengono dal ricevere e utilizzare informazioni riservate per fini diversi da quelli ricompresi tra i loro compiti e doveri, e comunque per scopi non conformi alle funzioni proprie dell'OdV, fatto salvo il caso di espressa e consapevole autorizzazione. In ogni caso, ogni informazione in possesso dei membri dell'OdV deve essere trattata in conformità con la vigente legislazione in materia e, in particolare, in conformità al Decreto legislativo 196/2003 ("codice Privacy"). L'inosservanza dei suddetti obblighi costituisce giusta causa di revoca dalla carica di membro dell'OdV.

9.3 COMPITI E POTERI

All'OdV sono attribuiti i seguenti compiti:

1. Verifica l'efficacia e l'efficienza del Modello Organizzativo adottato rispetto alla prevenzione ed all'impedimento della commissione dei reati attualmente previsti dal D.Lgs 231/2001 e di quelli che in futuro dovessero comunque comportare una responsabilità amministrativa della persona giuridica;
2. Verificare il rispetto delle modalità e delle procedure previste dal Modello Organizzativo e rilevare gli eventuali scostamenti comportamentali che emergessero dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie funzioni.
3. Formulare proposte alla Direzione per gli eventuali aggiornamenti ed adeguamenti del Modello Organizzativo adottato da realizzarsi mediante le modifiche e/o le integrazioni che si rendessero necessarie in conseguenza di (a) significative violazioni delle prescrizioni del Modello Organizzativo; (b) significative modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività di impresa;(c) modifiche legislative al D.lgs 231/2001 o che comunque prevedano nuove ipotesi di responsabilità diretta della persona giuridica.
4. A seguito dell'accertamento di violazioni del Modello Organizzativo, segnalare tempestivamente le stesse alla Direzione per gli opportuni provvedimenti disciplinari che dovranno essere irrogati; l'OdV ha l'obbligo di informare immediatamente la Direzione qualora le violazioni riguardassero i soggetti di vertice della Società.
5. Predisporre una relazione informativa, su base semestrale, per la Direzione, in ordine alle attività di verifica e controllo compiute ed all'esito delle stesse.

Per l'espletamento dei suddetti compiti, all'organismo di vigilanza sono attribuiti i più ampi poteri. In particolare:

- le attività poste in essere dall'OdV non potranno essere sindacate da alcun altro organismo o struttura aziendale;
- è autorizzato il libero accesso dell'OdV 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 231/2001;
- l'OdV potrà avvalersi dell'ausilio di tutte le strutture della Società o della quale questa si avvale, ovvero di consulenti esterni perché collaborino nell'esecuzione dell'incarico sotto la diretta sorveglianza e responsabilità dell'Organismo stesso, nonché chiedere ai rappresentanti aziendali, di volta in volta identificati dall'OdV, di partecipare alle relative riunioni;
- è attribuita all'OdV, per l'espletamento delle attività proprie, piena autonomia economico/gestionale, non condizionata da limiti di spesa.

9.4 FLUSSI INFORMATIVI

L'Art. 6 c. 2 lett. D) del Decreto legislativo 231/2001 individua specifici obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli.

E' previsto un sistema di reportistica, sistematico e strutturato, in merito a temi/fatti a rischio, la cui rilevazione ed analisi costituisca il punto dal quale possono originare azioni di riscontro e approfondimento dell'OdV su eventuali situazioni anomale e/o di reato.

A tal fine, è prevista come componente integrante, l'attivazione di specifici flussi informativi verso l'OdV. Dovranno essere comunicati all'Organismo di Vigilanza tutte le informazioni/dati/notizie identificate dallo stesso e/o da questi richieste alle

singole strutture della Società, nonché ogni altra informazione, di qualsivoglia genere, proveniente anche da terzi ed attinente l'attuazione del Modello nelle aree di attività "sensibili" ed il rispetto delle previsioni del Decreto, che possa risultare utile ai fini dell'assolvimento dei compiti dell'Organismo di Vigilanza.
Le funzioni aziendali coinvolte in occasione di ispezioni, accessi e/o verifiche presso la Società dovranno darne immediata notizia all'Organismo di Vigilanza.
Ogni informazione, segnalazione, *report* da o verso l'Organismo di Vigilanza raccolta nel corso di ogni anno dovrà essere adeguatamente custodita per un periodo di sei anni in un apposito *Data Base* (informatico o cartaceo) salvo il caso di contestazione dell'illecito amministrativo dipendente da reato. In tale ultimo caso tutta la relativa documentazione dovrà essere conservata sino alla completa definizione del suddetto giudizio di contestazione. L'accesso al *Data Base* sarà consentito esclusivamente ai membri dell'Organismo di Vigilanza.
l numero e il tipo di informazioni possono variare nel tempo in seguito a:

- Inadeguatezza e/o incompletezza delle informazioni a fornire indicazioni utili ad agevolare l'attività di vigilanza sull'efficacia del Modello Organizzazione;
- Rilevanti cambiamenti dell'assetto interno della società e/o delle modalità di svolgimento dell'attività d'impresa;
- Modifiche normative al Decreto legislativo 231/2001 o che comunque prevedano nuove ipotesi di responsabilità diretta della persona giuridica.

L'OdV deve essere informato attraverso segnalazioni di Dipendenti, Dirigenti, altre Società, *stakeholders* in generale in merito a fatti che potrebbero generare la responsabilità di **CENTRO DIAGNOSTICO S.r.l.** ai sensi del D.lgs 231/01.
Valgono al riguardo le seguenti prescrizioni.
Segnalazioni da parte di esponenti aziendali o da parte dei terzi

- i dipendenti, collaboratori interni ed esterni ed i dirigenti che siano a conoscenza di fatti o comportamenti che possono configurare una violazione del Modello o che non siano in linea con le regole di condotta adottate dalla Società, hanno la possibilità di segnalarlo all'OdV;
- i segnalanti devono essere garantiti contro qualsiasi forma di ritorsione e in ogni caso sarà assicurata la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela di chi venga accusato erroneamente e/o in mala fede;
- l'OdV valuterà le segnalazioni ricevute e le eventuali conseguenti iniziative a sua discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunte violazione e motivando per iscritto eventuali rifiuti di procedere ad una indagine interna;
- le segnalazioni dovranno essere in forma scritta, indirizzate all'OdV, alla casella email CentroDiagnostico@eco231.it appositamente predisposta;
- le segnalazioni pervenute devono essere raccolte e conservate in un apposito archivio al quale sia consentito l'accesso ai soli membri dell'OdV;
- in modo analogo i consulenti hanno la facoltà di segnalare all'OdV eventuali violazioni di cui siano venuti a conoscenza.

Obblighi di informativa relativi ad atti ufficiali
Oltre alle segnalazioni sopra riportate, devono essere obbligatoriamente trasmesse le informative inerenti:

- atti, provvedimenti, comunicazioni e/o notizie provenienti da organi di polizia giudiziaria o altra autorità, attinenti ad indagini, ove e quando emerga che le stesse sono svolte in correlazione ad ipotesi di commissione di alcuno dei reati di cui al D.lgs 231/01;
- le richieste di assistenza legale inoltrate da Dipendenti, Consulenti, etc. ad in caso di avvio di procedimento giudiziario;
- i rapporti preparati dai responsabili di funzioni aziendali nell'ambito della loro attività di controllo e dai quali possono emergere fatti o omissioni con profili di criticità rispetto all'osservanza alle norme del decreto;
- le notizie relative ai procedimenti sanzionatori o provvedimenti di archiviazione degli stessi con le relative motivazioni, qualora essi siano legati a commissione di reati di cui al D.Lgs. 231/01;
- l'inizio di indagini o ispezioni da parte di Autorità Giudiziaria o di Controllo.

Il materiale raccolto dall'OdV verrà conservato per 10 anni.
Per ciascuna Area a rischio possono essere, inoltre, designati dalla Direzione, previa informativa all'Organismo di Vigilanza, dei Responsabili Interni, che costituiscono il primo presidio per prevenire la commissione di Reati nonché i referenti diretti dell'Organismo di Vigilanza per ogni attività informativa e/o di controllo da questo predisposta.

9.5 INIZIATIVA DI CONTROLLO

L'OdV, avvalendosi della collaborazione delle funzioni di auditing interno, ovvero di consulenti esterni, si attiva con specifiche attività di *audit* sulla realtà della Società, laddove coinvolte, con le seguenti modalità:

- Con interventi "a piano", nei quali le attività di controllo relative all'efficacia del Modello Organizzativo sono parte integrante di un piano di lavoro più ampio; in questo tale attività viene specificatamente considerata e adeguatamente valorizzata, di concerto con l'OdV, in sede di *risk assesment* per la definizione del Piano Annuale di *Audit*;

Con interventi mirati in caso di:

- specifica richiesta formulata da parte degli altri organi di controllo della Società;
- in caso di non conformità derivanti dal flusso informativo correttamente operante nell'ambito del Modello organizzativo.

9.6 STRUMENTI DI CONTROLLO E AZIONE

L'Organismo di vigilanza, proprio per le caratteristiche intrinseche del Modello Organizzativo 231 di integrazione con il sistema di gestione per la qualità, utilizza come strumenti di controllo e azione quelli propri del Sistema di Gestione per la Qualità quali i report di soddisfazione del cliente, le procedure di gestione del miglioramento, i Piani di Attività quali il Piano di Formazione e il Programma di *Audit*, il Riesame della Direzione.

9.7 LA RELAZIONE DELL'ODV

Per l'espletamento dei suoi compiti, e ferma restando ogni altra attività necessaria a tal fine, l'OdV si riunisce periodicamente durante l'anno e, in ogni caso, ogni qual volta se ne ravvisi l'opportunità o la necessità. L'OdV riferisce alla direzione secondo i seguenti criteri:

- su base continuativa, riferisce direttamente alla Direzione;
- annualmente, redige il piano di attività per l'anno successivo, che sarà oggetto di discussione e delibera. Nello specifico presenta alla Direzione una relazione, ovvero il rapporto consuntivo sull'attività esercitata nell'anno trascorso, motivando, ove necessario, le scelte e le modifiche adottate.

La relazione dell'OdV ha ad oggetto l'illustrazione dell'attività svolta e le eventuali criticità emerse, sia con riferimento a comportamenti o avvenimenti interni che all'efficacia del Modello. La relazione deve riportare in maniera esaustiva ogni elemento utile al fine di valutare l'efficace attuazione del Modello.

9.8 DISPOSIZIONI IN TEMA DI WHISTLEBLOWING

Ai sensi del Decreto 24, che ha considerevolmente esteso le tutele a coloro che effettuano le segnalazioni in conformità alla normativa di cui si tratta (di seguito le "Segnalazioni"), sono destinatari della presente Policy (di seguito "Destinatari" o "Segnalanti") i soggetti che seguono:

- lavoratori subordinati;
- lavoratori autonomi e collaboratori che svolgono la propria attività lavorativa presso l'Azienda;
- liberi professionisti e consulenti che prestano la propria attività presso l'Azienda;
- volontari e tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso l'Azienda;
- azionisti e persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso l'Azienda.

Si applicano le tutele proprie delle persone segnalanti (cd destinatari) anche a coloro il cui rapporto giuridico/di lavoro (vedi art.3, comma 3, D.Lgs. 24/2023) non sia ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali; ovvero durante il periodo di prova ovvero ancora successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni siano state acquisite nel corso del rapporto stesso.

Qualora un Amministratore, un Dirigente, un componente degli organi sociali, un dipendente o un collaboratore dovessero ricevere una Segnalazione attraverso canali diversi da quello interno WB, essi hanno l'obbligo di trasmettere all'Organismo di Vigilanza la Segnalazione medesima, con immediatezza ed in via esclusiva, sempre secondo le modalità di seguito esposte, completa di tutta la eventuale documentazione di supporto pervenuta, non trattenendone copia ed astenendosi dall'intraprendere autonome iniziative di analisi e/o approfondimento. La mancata comunicazione di una Segnalazione ricevuta costituisce una violazione della presente procedura, oltre che del Codice Etico e del Modello, con applicazione in caso di accertata malafede di tali condotte, delle conseguenti sanzioni previste dal sistema disciplinare del Modello.

La procedura è oggetto di ampia comunicazione e diffusione, così da costituire un costante riferimento nelle attività aziendali. Ai fini dell'attuazione della procedura, la formazione al personale è gestita dall'Organismo di Vigilanza della Società (di seguito "OdV") e d'intesa con i responsabili di altre funzioni aziendali preposte (Amministrazione e Controllo, Ufficio del Personale, etc.). Per i Terzi è prevista analoga informativa e pubblicità della procedura, anche secondo modalità differenziate, ad esempio pubblicazione sui siti web del Gruppo, eventualmente distinguendo in relazione alla tipologia di rapporto contrattuale o di relazione con la Società.

9.9.1. SCOPO E AMBITO DI APPLICAZIONE

L'obiettivo perseguito dalla procedura è quello di descrivere e regolamentare il processo di segnalazione delle violazioni di illeciti o irregolarità, fornendo al segnalante chiare indicazioni operative circa l'oggetto, i contenuti, i destinatari e le modalità di trasmissione delle Segnalazioni, nonché riguardo alle forme di tutela che vengono predisposte dalla Società in conformità alle disposizioni normative.

La presente procedura ha altresì lo scopo di disciplinare le modalità di accertamento della validità e fondatezza delle Segnalazioni e, conseguentemente, di intraprendere le azioni correttive e disciplinari opportune a tutela della Società.

Per tali motivi, non saranno prese in considerazione segnalazioni riguardanti vicende o interessi personali ovvero inerenti richieste, contestazioni o rivendicazioni legate alla sfera individuale attinente al proprio rapporto di lavoro, e che non ricoprano carattere di informazioni relative a violazioni gravi, lesive per il segnalante e per l'azienda, tali da poter essere perseguite con esposti o denunce presso le competenti autorità civili, penali o amministrative.

La presente procedura si applica nell'ambito di tutte le attività aziendali delle Società e deve essere applicata fedelmente dai Destinatari, in coerenza con gli standard previsti dal Modello della Società nonché nel rispetto degli obblighi di legge che potrebbero derivare dalla segnalazione: in particolare, in tema di obbligo di denuncia all'Autorità Giudiziaria e in materia di trattamento dei dati personali e tutela della privacy.

9.9.2 IL CANALE DI SEGNALAZIONE INTERNO ex art. 4, Decreto 24/2023

In conformità all'art. 4 del D.Lgs. 24/2023, la Società ha attivato l'apposito canale di segnalazione interno dedicato ai flussi di segnalazione cd "*whistleblowing*", assicurando caratteristiche di confidenzialità e riservatezza per tutti/e coloro che intendano effettuare Segnalazioni.

9.9.3 L'ORGANISMO DI VIGILANZA. RUOLO E RESPONSABILITA'

Il soggetto preposto alla gestione del canale di segnalazione interna (di seguito "canale WB"), destinatario della ricezione e dell''esame delle segnalazioni è l'Organismo di Vigilanza (di seguito "OdV"), ufficio interno autonomo il cui membro è specificamente formato per la gestione del canale interno poiché dotato di comprovati titoli e qualità professionali. La gestione e la verifica della fondatezza delle circostanze rappresentate nella segnalazione sono dunque affidate all'OdV, che agisce, nel rispetto dei principi di imparzialità e riservatezza, effettuando ogni attività ritenuta opportuna, inclusa l'audizione personale del segnalante e di eventuali altri soggetti che possono utilmente riferire sui fatti.

L'OdV svolge direttamente tutte le attività finalizzate all'accertamento dei fatti oggetto della segnalazione. Può anche avvalersi del supporto e della collaborazione di strutture e funzioni aziendali quando, per la natura e la complessità delle verifiche, risulti necessario un loro coinvolgimento, come anche di consulenti esterni.

L'Organismo di Vigilanza, al quale è affidata la gestione delle segnalazioni interne, fornirà avviso di ricevimento della segnalazione entro 7 giorni dalla data di ricezione del flusso. Fornirà il dovuto riscontro entro 3 mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione. Le segnalazioni sono gestite con specifica procedura "whistleblowing" condivisa dalla Direzione con il personale.

L'Organismo di Vigilanza, una volta investito della segnalazione, opera in qualità di Responsabile al Trattamento ai sensi del Reg. UE 679/26, cui si rimanda, ed alle normative correlate.

9.9.4. OGGETTO E CONTENUTO DELLA SEGNALAZIONE – ATTIVITA' ISTRUTTORIA

Costituiscono segnalazioni rilevanti ai sensi della normativa di cui si tratta le segnalazioni aventi ad oggetto comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità della Società, di cui il segnalante sia venuto a conoscenza nel contesto lavorativo e che consistono in:

- condotte illecite rilevanti ai sensi del D.Lgs. n. 231/2001 e violazioni del Modello 231, quali, a titolo esemplificativo: comportamenti corruttivi verso la Pubblica Amministrazione, violazioni in materia di Salute e Sicurezza sul Lavoro, violazioni della normativa in materia Ambientale, etc.

Si evidenzia che tali segnalazioni potranno essere effettuate esclusivamente per il tramite dei canali di segnalazione interni;

- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione Europea relativi ai seguenti settori:
  - appalti pubblici;
  - servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo;
  - sicurezza e conformità dei prodotti;
  - sicurezza dei trasporti;
  - tutela dell'ambiente;
  - radioprotezione e sicurezza nucleare;
  - sicurezza degli alimenti e dei mangimi e salute e benessere degli animali;
  - salute pubblica;
  - protezione dei consumatori;
  - tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi.
- atti od omissioni che ledono gli interessi finanziari dell'Unione Europea;
- atti od omissioni riguardanti il mercato interno, comprese le violazioni delle norme UE in materia di concorrenza e di aiuti di Stato nonché in materia di imposte sulle società;
- gli atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione Europea nei settori sopra indicati.

Sono escluse dall'ambito delle segnalazioni rilevanti le contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale del segnalante che attengono esclusivamente ai propri rapporti individuali di lavoro ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate.
Le Segnalazioni possono avvenire anche in forma anonima; tuttavia, si raccomanda che le stesse siano nominative, al fine di consentire una più efficiente attività d'indagine, applicando in ogni caso le tutele previste e accordate dal Decreto 24.
La Segnalazione, anche anonima, deve essere circostanziata e fondata su elementi precisi e concordanti, di cui il segnalante sia venuto a conoscenza nell'ambito dell'attività lavorativa, così da fornire ogni elemento utile per consentire un'appropriata attività di verifica sulla fondatezza dei fatti segnalati.
Ad avvenuta ricezione della segnalazione, a cura dell'Organismo di Vigilanza, la Procedura si articola nelle seguenti fasi:

- Ricezione e verifica preliminare della segnalazione
- Istruttoria
- Definizione di un piano d'azione
- Reporting e Monitoraggio

Pertanto, è importante che il Segnalante:

- riporti in modo chiaro, completo e circostanziato i fatti oggetto di segnalazione, le modalità con le quali ne ha avuto conoscenza, la data e il luogo in cui sono accaduti;
- indichi generalità o altri elementi che consentano di identificare le persone coinvolte;
- indichi eventuali altri soggetti che possano riferire sui fatti oggetto di segnalazione;
- indichi/fornisca eventuali documenti che possano confermare la fondatezza della denuncia;
- fornisca ogni altra informazione che possa consentire un utile riscontro circa la sussistenza di quanto segnalato.

In ogni caso, ai fini della presente procedura, si intendono per:

- **Riservatezza il** massimo riserbo sulle generalità del segnalante
- **Confidenzialità l'**assunzione di cautele in ordine alle modalità di gestione della segnalazione a tutela della riservatezza del segnalante
- **Anonimato l'**assenza di riferimenti in ordine all'identità del segnalante senza indicazioni su possibili riscontri in ordine a persone fatti e circostanze

Con riferimento a ciascuna Segnalazione laddove, a seguito di verifiche preliminari, emergano o siano comunque desumibili elementi utili e sufficienti per una valutazione della fondatezza della Segnalazione medesima, fatto salvo il diritto alla difesa del segnalato, l'OdV provvede a:

- avviare analisi specifiche, avvalendosi delle strutture competenti, eventualmente anche tramite attività di audit, nonché coinvolgendo le funzioni aziendali interessate dalla Segnalazione;
- concludere l'istruttoria in qualunque momento se, nel corso dell'istruttoria medesima, sia accertata l'infondatezza della Segnalazione e procedere pertanto all'archiviazione;
- avvalersi, se necessario, di esperti o periti esterni;
- concordare col responsabile della Funzione interessata dalla Segnalazione, l'eventuale "*action plan*" necessario alla rimozione delle criticità rilevate, garantendo, altresì, il monitoraggio dell'attuazione;
- concordare con le Funzioni interessate eventuali iniziative da intraprendere a tutela degli interessi dell'ente (ad es. azioni giudiziarie, sospensione/cancellazione di fornitori dall'Albo Fornitori);

- sottoporre alla valutazione delle Funzioni interessate gli esiti degli approfondimenti della Segnalazione, qualora risulti fondata, affinché vengano intrapresi i più opportuni provvedimenti. Sarà poi cura delle suddette Funzioni informare tempestivamente l'Organismo di Vigilanza di tali provvedimenti;
- differire l'esercizio di diritti propri dell'interessato al fine di non pregiudicare il buon esito della procedura. Il differimento -ai sensi dell'art. 2-undecies, nuovo Codice Privacy- sarà deciso di volta in volta ma ogni restrizione, qualunque sia l'attore all'interno della precedente procedura dovrà essere documentata.

Nel caso di segnalazione interna ritenuta conforme alla presente procedura, l'OdV sottopone al segnalante apposita informativa e richiesta di consenso al trattamento dei dati personali.
Nel caso di audizioni degli interessati nonché di testimoni o periti, è redatto verbale a cura dell'Organismo di Vigilanza, che viene sottoscritto dai partecipanti. Il verbale è redatto ai fini della tracciabilità delle operazioni svolte.

9.9.5 LE SEGNALAZIONI ESTERNE
In conformità al Decreto Legislativo 24/2023, ex artt. 6 e 7, i/le segnalanti possono effettuare una segnalazione "esterna" rispetto ai canali WB interni messi a disposizione dalla Società (vd. Punto 4, pag. 4, della presente procedura) all'Autorità Anticorruzione/ANAC, se ricorrono le condizioni che seguono:

a) Non è prevista nel contesto/ambiente di lavoro l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o non risulta conforme secondo i requisiti di Legge (art. 4)
b) Il/la segnalante ha già effettuato una segnalazione all'interno dei canali messi a disposizione dalla Società e la segnalazione non ha avuto seguito;
c) Il/la segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, ad essa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsioni;
d) Il/la segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse

Ove ricorra anche solo una di tali condizioni, pertanto, il/la segnalante può effettuare una segnalazione cd esterna presso ANAC, i cui canali sono dotati di strumenti di crittografia a garanzia e tutela della riservatezza dell'identità del/della segnalante, dei soggetti coinvolti nella segnalazione e del contenuto della segnalazione.
Le segnalazioni cd "esterne" sono effettuate in forma scritta tramite piattaforma informatica ovvero in forma orale attraverso linee telefoniche o sistemi di messaggistica orale messi a disposizione dell'Autorità Anticorruzione ovvero ancora, su richiesta del/della segnalante, mediante un incontro diretto, da fissare e concordare con il personale addetto dell'Ufficio.
Tutte le informazioni necessarie alla effettuazione delle segnalazioni cd "esterne" sono accessibili sul sito istituzionale dell'ANAC

L'ANAC **può <u>non</u> dare seguito** alle segnalazioni che riportano violazioni di lieve entità e procedere alla loro archiviazione

9.9.6 DIVIETO DI RITORSIONE (ART. 17, D.LGS. 24/2023)
Ai sensi del Decreto 24, gli enti, le società, le aziende e le persone segnalanti che operano al loro interno o che comunque interagiscono con l'Ente (art. 3, D.Lgs. 24/2023) non possono subire alcuna ritorsione a causa della segnalazione.
Il divieto di ritorsione è lo strumento previsto dal D.Lgs. 24/2023 per garantire la tutela della "*persona segnalante*", *cioè il divieto di porre in essere qualsiasi comportamento minacciato o tentato, commissivo od omissivo in conseguenza della segnalazione, che possa provocare direttamente o indirettamente un danno ingiusto al segnalante.*

A titolo esemplificativo, costituiscono ritorsione:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione/demansionamento o la mancata promozione;
- il mutamento di funzioni, il cambiamento della sede di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione nell'accesso alla formazione; le note di merito negative o le referenze negative;
- l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o comunque il trattamento sfavorevole;
- la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- Il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;

- I danni, anche alla reputazione della persona, in particolare sui social media o i pregiudizi economico o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
- l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
- la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- l'annullamento di una licenza o di un permesso;
- la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

9.9.7 MISURE DI TUTELA DEL SEGNALANTE

L'Ente garantisce la riservatezza del soggetto segnalante sin dal momento della presa in carico della segnalazione, anche nelle ipotesi in cui la stessa dovesse rivelarsi successivamente errata o infondata. Ad eccezione dei casi in cui si configuri una responsabilità a titolo di calunnia e di diffamazione ai sensi delle disposizioni del codice penale o dell'art. 2043 c.c., nonché delle ipotesi in cui l'anonimato non è opponibile per legge (come per es. indagini penali, tributarie o amministrative, ispezioni di organi di controllo), l'identità del segnalante è comunque protetta in ogni fase successiva alla segnalazione; pertanto, fatte salve le eccezioni di cui sopra, l'identità del segnalante non può essere rivelata senza il suo espresso consenso.
Per quanto concerne, in particolare, l'ambito del procedimento disciplinare, l'identità del segnalante può essere rivelata al responsabile della funzione aziendale titolare dei procedimenti disciplinari e/o all'incolpato solo nei casi in cui:
• vi sia il consenso espresso del segnalante;
• ovvero la contestazione dell'addebito disciplinare risulti fondata unicamente sulla segnalazione, e la conoscenza dell'identità del segnalante risulti assolutamente indispensabile alla difesa dell'incolpato, come da quest'ultimo richiesto e motivato per iscritto.
In tale circostanza, spetta al responsabile della funzione aziendale titolare dei procedimenti disciplinari valutare la richiesta dell'interessato e se ricorra la condizione di assoluta indispensabilità della conoscenza del nominativo del segnalante ai fini della difesa. Qualora la ritenga fondata, il responsabile della funzione dovrà avanzare richiesta motivata all'Organismo, contenente un'esposizione chiara e precisa delle ragioni per le quali risulti indispensabile la conoscenza dell'identità del segnalante.
Gravano sul responsabile della funzione competente per i procedimenti disciplinari gli stessi doveri di comportamento, volti alla riservatezza del segnalante, cui sono tenuti i componenti dell'Organismo.
Nel caso di trasmissione della segnalazione ad altre strutture/organi/terzi per lo svolgimento delle attività istruttorie, dovrà essere inoltrato solo il contenuto della segnalazione, espungendo tutti i riferimenti dai quali sia possibile risalire, anche indirettamente, all'identità del segnalante.
Nei confronti del segnalante non è inoltre consentita, né tollerata alcuna forma di ritorsione o misura discriminatoria, diretta o indiretta, sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla segnalazione.
CENTRO DIAGNOSTICO S.r.l. persegue condotte di dolo o colpa grave del segnalante nonché le eventuali condotte di calunnia o diffamazione. In tali casi, oltre alle sanzioni previste dal Sistema disciplinare della Società, ricorre anche la cd. "clausola di esclusione" dalle tutele aziendali, così come prevista dalla Legge, in caso di accertamento nel giudizio di primo grado delle responsabilità a titolo di calunnia o diffamazione del segnalante in mala fede.
In ogni caso:

- sono vietati atti di ritorsione o discriminatori, diretti e/o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- sono previste sanzioni nei confronti di chi viola le misure di tutela dl segnalante, ma anche nei confronti di chi effettui con dolo o colpa grave segnalazioni che si rivelino infondate;
- l'onere di provare che tali condotte o atti sono motivati da ragioni estranee alla segnalazione, alla divulgazione pubblica o alla denuncia, è a carico di colui che li ha posti in essere: ricorre un nesso di causalità *juris tantum* tra il danno subito dal /dalla segnalante e la ritorsione subìta a causa della segnalazione;
- Il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo. Sono altresì nulli il mutamento di mansioni nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. In particolare, il Decreto 24/2023 ha inciso sull'art. 4 della L. 604/1966 in tema di licenziamenti, con l'introduzione della nuova fattispecie di "*licenziamento conseguente all'esercizio di un diritto ovvero alla segnalazione, alla denuncia all'*AG *od alla Corte dei Conti od alla divulgazione pubblica effettuate in base al D.Lgs. 24/2023".*
- È facoltà del segnalante comunicare le ritorsioni subite all'ANAC che informa l'Ispettorato Nazionale del Lavoro.

9.9.8 APPARATO SANZIONATORIO E DISCIPLINARE

Sono fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente procedura, quali segnalazioni riscontrate come infondate, effettuate con dolo o colpa grave, ovvero quelle manifestamente

opportunistiche e/o compiute al solo scopo di danneggiare il denunciato o altri soggetti, e ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione della presente Policy.
Resta inteso che **CENTRO DIAGNOSTICO S.r.l.** potrà intraprendere le più opportune misure disciplinari e/o legali nei confronti di chiunque, in mala fede, abbia effettuato segnalazioni false, infondate o opportunistiche e/o al solo scopo di calunniare, diffamare o arrecare pregiudizio al segnalato o ad altri soggetti citati nella segnalazione.
Le sanzioni saranno proporzionate all'entità e gravità dei comportamenti illeciti accertati e potranno anche giungere alla risoluzione del rapporto, nel rispetto delle disposizioni di legge e delle normative di CCNL applicabili.
Si richiamano qui e integralmente, le disposizioni e i principi generali contenuti nel Codice Etico e nel Modello di Organizzazione e Gestione ex D.Lgs. 231/2001.
Da ultimo, si evidenzia che ai sensi dell'art. 21 del Decreto 24 (Sanzioni), l'ANAC applica sanzioni amministrative anche al settore privato ove accerti che sono state commesse ritorsioni o che le segnalazioni siano state ostacolate o che si è tentato di ostacolarle o che è stato violato l'obbligo di riservatezza.

9.9.9 TRATTAMENTO DEI DATI PERSONALI

La segnalazione di un fatto illecito all'interno dell'organizzazione impatta significativamente sul trattamento dei dati personali di coloro che sono coinvolti dalla segnalazione: segnalante, segnalato, organo ricevente, testimoni, l'ente/società.
La Società si conforma nella presente procedura alla Legislazione vigente in tema privacy, già richiamata, al Modello di Organizzazione e Gestione 231, ai richiami del Garante Privacy così come intervenuto nel Decreto 24/2023 ed esplicitato nelle LL.GG. ANAC (artt. 3.2, pg. 35 e 4.1.3, pg.52 e segg.) nonché al ruolo dell'Organismo di Vigilanza. Il rapporto di lavoro con la Società ed il Modello 231 costituiscono le basi giuridiche e la liceità del Trattamento dei Dati, vincolante per tutti i destinatari, in relazione e per le finalità della presente procedura.
Ciò premesso, **CENTRO DIAGNOSTICO S.r.l.** impartisce le linee guida aziendali sui principi che seguono:

- ***Riservatezza***: i dati personali del segnalante e del segnalato sono trattati in conformità a principi di riserbo assoluto anche al fine di non pregiudicare l'iter procedurale e non esporre l'autore della segnalazione a rischi di ritorsione;
- ***Diritto all'informazione***: coloro che sono direttamente coinvolti nella Procedura, devono essere debitamente informati circa le modalità con cui i loro dati verranno trattati. Le informazioni devono essere rese note solo alle persone coinvolte nella procedura. È importante ricordare, comunque, che è possibile che in una fase iniziale ("istruttoria") il diritto all'informazione del segnalato –tra tutti, quello di conoscere l'identità del segnalante- possa essere differito al fine di non pregiudicare il buon esito della procedura. Il differimento sarà deciso di volta in volta, ma ogni restrizione ai diritti dell'interessato- qualunque attore egli sia all'interno della precedente procedura- dovrà essere documentato. L'OdV si assicura che, in caso di istanza di accesso ai dati, vengano rese disponibili esclusivamente le informazioni necessarie e non pregiudizievoli.
- ***Minimizzazione dei Dati***: si applica il principio della minimizzazione dei dati. Essi non verranno trattati in misura superiore a quella necessaria ai fini dell'istruttoria interna. Si procederà pertanto alla raccolta delle informazioni rilevanti immediatamente dopo la prima selezione fra quelle ritenute necessarie al prosieguo delle attività qui disciplinate per consentire l'applicazione dei limiti previsti dall'art. 2-undecies del Codice. Sarà oggetto di prudenziale valutazione il bilanciamento degli interessi coinvolti per le eventuali richieste di accesso, con quelli che attengono alla riservatezza ed al buon esito della procedura. L'accesso ai dati pertanto verrà concesso esclusivamente ai destinatari interni ed esterni, come correttamente individuati, e sarà limitato il trasferimento delle informazioni secondo criteri di necessità.
- ***Limitazioni ai diritti dell'interessato:*** ai sensi dell'art. 2-undecies del Codice, i diritti di cui agli articoli da 15 a 22 del GDPR non possono essere esercitati qualora dall'esercizio degli stessi possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante. L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato; ciò a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato stesso, al fine di salvaguardare gli interessi di cui alla presente procedura. In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante, previa informativa da parte dell'OdV.
- **Legittimo interesse** del Titolare del Trattamento: nell'ambito della presente Procedura, è sempre operato, laddove necessario, il debito e concreto bilanciamento di legittimi interessi della Società e i diritti fondamentali dell'interessato (il segnalato).
- **Conservazione e archiviazione** (art. 14, D.Lgs. 24/2023) Le segnalazioni, interne ed esterne, la relativa documentazione e tutti i dati personali correlati saranno trattati per il tempo necessario all'esecuzione delle attività funzionali alla presente procedura, fatti salvi i casi in cui la conservazione per un periodo ulteriore sia richiesta per eventuali contenziosi, richieste delle autorità competenti o ai sensi della normativa applicabile. **In ogni caso, il periodo di conservazione dei dati sarà determinato secondo criteri di proporzionalità e necessità, nel rispetto degli obblighi di legge, e comunque NON oltre i cinque anni a decorrere dalla data della comunicazione**

dell'esito finale dell'attività relativa alla gestione della segnalazione; scaduto detto termine, tutti i dati e la relativa documentazione saranno distrutti. È sempre garantita la tracciabilità delle attività e/o operazioni svolte, la cui documentazione è custodita ed archiviata, per il periodo previsto dalla Legge, presso separati

- Archivi, sia digitale (*directory*) che cartaceo, accessibili solo ai componenti dell'OdV ovvero a soggetti da questo espressamente autorizzati.

10 OPERAZIONI PROMANATE DIRETTAMENTE DAL VERTICE AZIENDALE

10.1 AMBITO DI RIFERIMENTO

Il Decreto Legislativo 231 non ha modificato il sistema normativo che disciplina l'amministrazione e il governo della società, sicché l'autonomia decisionale dei soggetti posti al Vertice Aziendale è sostanziale ed indefettibile espressione della libertà di gestione dell'impresa in forma societaria.
Tali soggetti sono identificabili nella Direzione ovvero nella figura del Legale Rappresentante.
La Direzione in via ordinaria decide operazioni che seguono i normali criteri previsti dal Modello Organizzativo, che lo stesso conosce e condivide. Pur tuttavia talvolta si rende necessario – nell' interesse della Società- 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.

10.2 ATTIVITA' DI CONTROLLO

Il sistema di controllo si basa su due elementi, quello della tracciabilità degli atti e quello del flusso informativo verso l'OdV. 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 esplicate 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 di vertice che ha attivato l'operazione "in deroga", verso l'OdV affinché possa attuare i dovuti riscontri con sistematicità e tempestività; l'assenza di operazioni in deroga nel periodo di riferimento dovrà comunque essere oggetto di specifica informativa all'OdV da parte del soggetto di vertice.

10.3 RIESAME DELLA DIREZIONE

Il riesame della Direzione è responsabilità della Direzione che annualmente verifica in collaborazione con l'OdV, lo stato di applicazione del Modello Organizzativo 231 e propone le possibili azioni di miglioramento del Modello stesso.
Elementi di ingresso per il riesame:

- L'eventuale commissione di un reato;
- Le risultanze di *Audit* precedenti condotti sia dall'Organismo di Vigilanza che da soggetti esterni indipendenti;
- L'analisi dei rischi nella sua revisione più aggiornata ed in quella immediatamente precedente;
- Le relazioni dell'Organismo di Vigilanza;
- Modifiche della normativa vigente;
- Informazioni circa anomalie o atipicità riscontrate a tutti i livelli nello svolgimento delle normali attività con particolare riguardo a quelle che configurano comportamenti difformi dal Codice Etico;
- Eventuali segnalazioni da terze parti esterne;
- Stato delle azioni correttive e preventive;
- Azioni derivanti da precedenti riesami della Direzione;
- Modifiche organizzative che potrebbero avere effetti sul SGRA;
- Raccomandazioni per il miglioramento.

Elementi in uscita dal riesame
Gli elementi in uscita dal riesame della Direzione comprendono ogni decisione ed azione relative:

- Al raggiungimento dell'efficacia del SGRA;
- Al miglioramento ed aggiornamento dei relativi processi in relazione ai requisiti del SGRA, con particolare riguardo all' analisi dei rischi.

11 GESTIONE DELLE RISORSE UMANE

11.1 SCOPO

Scopo della presente sezione è descrivere le attività che la società **CENTRO DIAGNOSTICO S.r.l.** compie per determinare:

- le risorse umane necessarie per stabilire e mantenere il Sistema di Gestione per la Responsabilità Amministrativa (SGRA);
- il grado di competenza e consapevolezza del proprio ruolo e delle responsabilità per ogni unità aziendale;
- il grado di consapevolezza e comprensione degli aspetti normativi e dei rischi dei reati previsti dal D.lgs. 231/01.

11.2 MESSA A DISPOSIZIONE DELLE RISORSE

Il personale che svolge attività che influenzano la conformità ai requisiti del SGRA deve essere competente sula base di istruzione, formazione-addestramento, abilità ed esperienza appropriati.

11.3 FORMAZIONE, INFORMAZIONE, COMUNICAZIONE

La formazione e la comunicazione costituiscono strumenti essenziali al fine di un'efficace implementazione e diffusione del Modello Organizzativo e del relativo Codice Etico.
Le risorse umane garantiscono, in stretta collaborazione e con la supervisione dell'OdV, una corretta conoscenza dei principi e delle regole di condotta adottati dalla Società sia alle risorse già presenti in Società sia a quelle future, con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nei processi operativi considerati sensibili e rilevanti.
Al momento dell'assunzione o inizio collaborazione, viene promossa la conoscenza del Modello Organizzativo 231 e del Codice Etico; in particolare ai nuovi arrivati viene consegnata un'informativa con riferimento all'applicazione della normativa di cui al Decreto legislativo 231/2001 nell'ambito della Società. L'attività di formazione è finalizzata a promuovere la conoscenza della normativa di cui al Decreto legislativo 231, a fornire un quadro esaustivo della stessa, dei risvolti pratici che da essa discendono, nonché dei contenuti e principi su cui si basa il Modello Organizzativo e il relativo Codice Etico fra tutti i dipendenti che, pertanto, sono tenuti a conoscerli, osservarli e rispettarli, contribuendo alla loro attuazione.
L'attività di formazione, eventualmente anche tramite corsi on line, 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 i destinatari funzioni di rappresentanza della Società.
Per i soggetti maggiormente coinvolti nelle attività considerate sensibili ai fini del Decreto legislativo 231, la Società organizza corsi di formazione *ad hoc*.
L'attività di formazione del personale, in termini di:

- Responsabilità;
- Pianificazione;
- Realizzazione;
- Verifica di efficacia;
- Registrazioni;

è gestita da un'apposita procedura, inserita all'interno del sistema qualità.
Tutte le informazioni sensibili sono gestite dalla società **CENTRO DIAGNOSTICO S.r.l.** attraverso il codice di autoregolamentazione per la protezione dei dati personali, con il quale si intende assicurare che il trattamento dei dati personali avviene in conformità a quanto disposto dal Regolamento Europeo RUE 679/2016.

12 SISTEMA DISCIPLINARE E SANZIONATORIO

12.1 PREMESSA

Ai sensi dell'art. 6, 2° comma, lett. e) e dell'art. 7, 2° comma, lett. b) del decreto, i modelli di organizzazione, gestione e controllo, la cui adozione ed attuazione (unitamente alle altre situazioni previste dai predetti articoli 6 e 7) costituisce "*conditio sine qua non*" per poter ottenere l'esenzione di responsabilità della società in caso di commissione dei reati di cui al Decreto, possono ritenersi efficacemente attuati solo se prevedano un sistema disciplinare idoneo a sanzionare il mancato

rispetto delle misure in essi indicate. L'applicazione delle sanzioni disciplinari prescinde ovviamente dall'avvio o dall'esito di un eventuale procedimento penale, in quanto il Modello ed il Codice Etico costituiscono regole vincolanti per tutti i destinatari, la cui violazione deve, al fine di ottemperare ai dettami del citato Decreto Legislativo, essere sanzionata indipendentemente dall'effettiva realizzazione di un reato o dalla punibilità dello stesso. Le regole di condotta imposte dal Modello sono, infatti, assunte dall'azienda in piena autonomia, al fine tanto del rispetto del precetto normativo che sull'azienda stessa incombe quanto di una buona governance aziendale. Peraltro, i principi di tempestività ed immediatezza rendono non soltanto non doveroso ma, altresì, sconsigliabile, ritardare l'irrogazione della sanzione disciplinare in attesa dell'esito del giudizio eventualmente instaurato davanti all'Autorità Giudiziaria.

12.2 DEFINIZIONE E LIMITI DELLA RESPONSABILITÀ DISCIPLINARE

La presente sezione del Modello identifica e descrive le infrazioni rilevanti ai sensi del D.Lgs. 231/2001 e successive modifiche, le corrispondenti sanzioni disciplinari irrogabili e la procedura diretta alla relativa contestazione ed irrogazione. La Società, conscia della necessità di rispettare le norme di legge e le disposizioni vigenti in materia, assicura che le sanzioni irrogabili ai sensi del presente Modello sono conformi a quanto previsto dai contratti collettivi nazionali del lavoro applicabili al settore e s.m.i.; la Società assicura, altresì, che l'iter procedurale seguito per la contestazione dell'illecito e per l'irrogazione della relativa sanzione è in linea con quanto disposto dall'art 7 della Legge 30 maggio 1970, n. 300 (c.d. "Statuto dei lavoratori"). Per i destinatari che sono legati da contratti di natura diversa da un rapporto di lavoro dipendente, in primis il personale medico esercente la propria attività con contratto a libera professione (ma in generale i soggetti terzi), le misure applicabili e le procedure sanzionatorie devono garantire il rispetto della legge e delle condizioni contrattuali.

12.3 DIPENDENTI, COLLABORATORI, CONSULENTI

Le inosservanze ed i comportamenti posti in essere dal personale, sia esso dipendente o collaboratore, in violazione delle regole individuate dal presente Modello Organizzativo, in applicazione del decreto legislativo 231/2001, determinano l'irrogazione di sanzioni disciplinari che sono applicate, secondo il criterio di proporzionalità previsto dall'art. 2016 c.c., tenendo conto – con riferimento a ciascun caso di specie – della gravità oggettiva del fatto costituente infrazione.
Il sistema disciplinare viene costantemente monitorato dall'OdV.
Per quanto riguarda l'accertamento delle suddette infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni restano di competenza della direzione sanitaria/tecnica o amministrativa. Viene previsto il necessario coinvolgimento dell'OdV nella procedura di accertamento delle violazioni e di irrogazione delle sanzioni per violazioni del Modello Organizzativo, nel senso che non potrà essere archiviato un provvedimento disciplinare ovvero irrogata una sanzione disciplinare per violazione del Modello stesso senza preventiva informazione e parere dell'OdV.
Il sistema disciplinare identifica le infrazioni ai principi, ai comportamenti e agli elementi specifici di controllo contenuti nel Modello, e a queste sono riconducibili le sanzioni previste, per il personale dipendente, dalle vigenti norme di legge e/o di contrattazione collettiva.
Il mancato rispetto e/o la violazione dei principi generali del Modello, delle regole di comportamento imposte dal Codice etico, dal Sistema disciplinare e dalle procedure aziendali, ad opera di lavoratori dipendenti della Società, costituiranno inadempimento alle obbligazioni derivanti da rapporto di lavoro ed illecito disciplinare.
Fermo restando il principio di collegamento tra i provvedimenti disciplinari irrogabili e le fattispecie in relazione alle quali gli stessi possono essere assunti, nell'irrogazione della sanzione disciplinare dovrà necessariamente essere rispettato il principio della proporzionalità tra infrazione e sanzione.
L'adeguatezza del sistema disciplinare alle prescrizioni del Decreto dovrà essere costantemente monitorata dall'Organismo di Vigilanza.
Con riguardo ai lavoratori dipendenti, il Decreto prevede che il sistema disciplinare debba rispettare i limiti connessi al potere sanzionatorio imposti dall'art. 7 della L. n. 300/1970 (c.d. "Statuto dei lavoratori") e dalla contrattualizzazione collettiva di settore e aziendale, sia per quanto riguarda le sanzioni irrogabili (che in linea di principio risultano "tipizzate" in relazione al collegamento con specificati indebiti disciplinari) sia per quanto riguarda la forma di esercizio di tale potere.
Con riferimento alle sanzioni irrogabili, si precisa che esse dovranno essere adottate ed applicate nel rispetto delle procedure previste dalle normative collettive nazionali ed aziendali applicabili al rapporto di lavoro.
In caso di violazioni commesse da parte dei dirigenti, l'assunzione dei provvedimenti ritenuti idonei dovrà tener conto della specifica qualifica dirigenziale e, dunque, del particolare vincolo fiduciario sottostante al rapporto di lavoro con la Società.
Infine, avuto riguardo alle violazioni della normativa vigente, del Modello, del Codice etico o del Sistema disciplinare commesse dagli altri soggetti con cui la Società entra in contatto nello svolgimento di relazioni d'affari, si dovrà fare riferimento alle previsioni contenute nei relativi contratti.
Per quanto riguarda i collaboratori e i liberi professionisti la società ha disposto che sia prevista nel relativo contratto individuale l'indicazione dei casi di violazione del modello e dei relativi provvedimenti da adottarsi, specificando in

un'apposita clausola contrattuale i valori perseguiti dalla società mediante l'adozione del modello stesso richiedendo che tutti si conformino alle regole, alle procedure ed ai principi in esso contenuti.

12.4 LE CONDOTTE RILEVANTI

Ai fini del presente Sistema disciplinare e nel rispetto della contrattazione collettiva applicabile alla struttura, costituiscono violazione del Modello o dei protocolli tutte le condotte, commissive o omissive (anche colpose), che siano idonee a ledere l'efficacia dello stesso quale strumento di prevenzione del rischio di commissione dei reati rilevanti ai fini del Decreto.
La funzione che gestisce il personale valuta le sanzioni irrogabili nel rispetto del principio di legalità e di proporzionalità e tenuto conto di tutti gli elementi e/o delle circostanze ad essa inerenti, secondo un ordine crescente di gravità da valutarsi ad opera dell'OdV.
.

12.5 LE SANZIONI

In caso di accertamento di una delle violazioni previste dal Modello ed in particolare dal presente Sistema disciplinare, si evidenzia che le sanzioni verranno applicate nel rispetto delle disposizioni contenute nel presente Modello, nella contrattazione collettiva tempo per tempo vigente e nel codice disciplinare adottato in azienda.
In ogni caso, l'individuazione e l'irrogazione delle sanzioni previste nel presente Sistema Disciplinare deve tener conto dei principi di proporzionalità ed adeguatezza delle stesse rispetto alla violazione contestata e dovranno pertanto tenersi in considerazione:

- la gravità della condotta o dell'evento che quest'ultima ha determinato;
- la tipologia della violazione compiuta;
  - le circostanze nel cui ambito si è sviluppata la condotta;
  - le modalità della condotta.

Ai fini dell'aggravamento della sanzione devono essere considerati i seguenti elementi:

- l'eventuale commissione di più violazioni nell'ambito della medesima condotta nel qual caso l'aggravamento sarà operato rispetto alla sanzione prevista per la violazione più grave;
- l'eventuale concorso di più soggetti nella commissione della violazione;
- l'eventuale recidività del suo autore.

12.6 LE SANZIONI NEI CONFRONTI DEI DIPENDENTI

Laddove venga accertata l'integrazione di una delle Condotte Rilevanti precedentemente descritte, da parte di un Dipendente saranno applicabili le seguenti sanzioni mutuate dal CCNL:

- Rimprovero verbale;
- Rimprovero scritto;
- Sospensione dal servizio e dal trattamento economico retribuzione per un periodo non superiore a 10 gg;
- Licenziamento per giustificato motivo;
- Licenziamento per giusta causa.

Resta salva la facoltà per la Società di rivalersi per ogni danno e/o responsabilità che alla stessa possano derivare da comportamenti di dipendenti in violazione del Modello.
Per i dirigenti non apicali, sono fatte salve le disposizioni applicabili previste dalle diverse previsioni rinvenibili nella contrattazione collettiva applicabile al caso concreto.
Quando sia richiesto dalla natura della mancanza o dalla necessità di accertamenti in conseguenza della medesima, l'impresa - in attesa di deliberare il definitivo provvedimento disciplinare – può disporre l'allontanamento temporaneo del lavoratore/lavoratrice dal servizio per il tempo strettamente necessario.

12.7 SANZIONI NEI CONFRONTI DEI TERZI DESTINATARI

Qualora sia accertata la commissione di una delle Condotte Rilevanti precedentemente indicate, da parte di un Terzo Destinatario, saranno applicate le seguenti sanzioni:

- la diffida al puntuale rispetto del Modello pena l'applicazione della penale di seguito indicata ovvero la risoluzione del rapporto negoziale intercorrente con la Società;
- l'applicazione di una penale, convenzionalmente prevista tra il 10% ed il 30% del fatturato totale lordo annuo;
- la risoluzione immediata del rapporto negoziale intercorrente con la Società.

Nell'ambito dei rapporti con i Terzi Destinatari, la Società inserisce nelle lettere d'incarico e negli accordi negoziali, apposite clausole volte a prevedere l'applicazione delle sanzioni previste dal presente Sistema Disciplinare in caso di violazione del Modello.

12.8 IL PROCEDIMENTO DI IRROGAZIONE DELLE SANZIONI

Il presente procedimento di irrogazione delle sanzioni consegue all'eventuale integrazione di una delle Condotte Rilevanti. Ai fini dell'effettività del Modello si ritiene opportuno descrivere il procedimento di irrogazione della sanzione con riguardo a ciascuna categoria di soggetti indicando per ciascuna:

- la fase di contestazione della violazione all'interessato;
- la fase di determinazione e successiva irrogazione della sanzione.

Il procedimento di irrogazione della sanzione ha inizio dalla ricezione da parte degli organi aziendali di volta in volta competenti come di seguito indicato, della comunicazione con cui l'OdV – in conseguenza delle verifiche condotte autonomamente ovvero di segnalazioni ricevute anche anonime o attraverso la procedura di allerta e ove gli accertamenti effettuati abbiano confermato l'esistenza della violazione – segnala la violazione del Modello.

In particolare, l'OdV, ricevuta una segnalazione, anche anonima o attraverso la procedura di allerta, ovvero acquisiti nel corso della propria attività di vigilanza e di verifica, gli elementi idonei a configurare il pericolo di violazione del Modello, ha l'obbligo di attivarsi al fine di espletare gli accertamenti ed i controlli rientranti nell'ambito della propria attività e ritenuti opportuni.

Esaurita l'attività di ricerca, verifica e controllo, l'OdV valuta sulla base degli elementi in proprio possesso se è stata realmente integrata un'ipotesi di violazione sanzionabile del Modello ed in caso positivo dovrà procedere alla segnalazione agli organi aziendali competenti. In caso negativo, procederà comunque a trasmettere segnalazione al responsabile della funzione che gestisce il personale ed all'Amministratore della Società per le eventuali valutazioni circa la rilevanza della condotta rispetto alla legge ed ai regolamenti applicabili.

Qualora gli organismi aziendali competenti per l'irrogazione della sanzione rilevino che la violazione del Modello riscontrata dall'OdV concreti anche una o più violazioni delle previsioni dei regolamenti aziendali e/o della contrattazione collettiva, all'esito del procedimento prescritto potranno irrogare anche una sanzione più grave rispetto a quella proposta dall'OdV e sempre tra quelle in concreto applicabili.

PARTE SPECIALE

PREMESSA

La Parte Speciale del Modello viene sviluppata in base alle specifiche attività sensibili e in relazione alle aree entro le quali è più alto il rischio della commissione di reati da parte di soggetti che svolgano la propria attività per la società.

Con la predisposizione della presente parte speciale si vogliono assicurare le adeguate condizioni di correttezza e trasparenza nella conduzione delle attività aziendali, in tutti i suoi rami, attraverso la conoscenza e la diffusione delle norme penali richiamate dal D. Lgs. n. 231/2001, al fine di chiarirne il significato e di renderlo accessibile indistintamente a tutti i destinatari del Modello.

Pertanto, conoscere gli elementi essenziali e le modalità realizzative delle singole fattispecie di reato punibili ai sensi del D. Lgs. n. 231/2001 è funzionale alla creazione, da una parte, di un sistema di conoscenza e conoscibilità delle relative fattispecie e dei comportamenti che possano dare luogo a fatti costituenti reati e, dall'altra, di un sistema di prevenzione e controllo idoneo a salvaguardare la Società dalla commissione di reati durante lo svolgimento di attività direttamente o indirettamente riconducibili alla Società stessa.

Considerata la realtà aziendale della società e la mappatura delle aree di rischio, alle quali si rimanda, le fattispecie di reato ipotizzabili possono essere principalmente ricondotte a:

- reati contro la P.A. (corruzione, concussione, malversazione ai danni dello Stato o di altro Ente Pubblico, indebita percezione di erogazioni, truffa in danno dello Stato o di un ente Pubblico);
- reati societari (false comunicazioni sociali, impedito controllo, operazioni in pregiudizio dei creditori, indebita restituzione dei conferimenti, illegale ripartizione degli utili e delle riserve, illecite operazioni sulle azioni o quote sociali, formazione fittizia del capitale e illecita influenza sull'assemblea);
- reato di omicidio colposo e lesioni colpose gravi o gravissime commessi con la violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro
- delitti informatici e trattamento illecito dei dati.
- reati ambientali (Inquinamento ambientale, traffico e abbandono di materiale ad alta radioattività, attività di gestione rifiuti non autorizzata)

Come anticipato nella parte generale, la normativa di riferimento disciplina anche altre fattispecie di reato (ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, abuso di informazioni privilegiate, associazione per delinquere, criminalità transnazionale, sfruttamento della prostituzione, tratta di persone, detenzione di materiale pornografico, beni o utilità di provenienza illecita, criminalità informatica, delitti di criminalità organizzata, delitti contro l'industria e il commercio, delitti in materia di diritti d'autore, ecc).

Dall'analisi svolta ai fini dell'individuazione delle aree sensibili ai sensi del D.Lgs. 231/01 della società non si è avuta evidenza circa la ragionevole possibilità di commissione dei suddetti reati nello svolgimento dell'attuale attività aziendale.

Nella stesura del Modello, pertanto, non si è provveduto alla specifica trattazione degli stessi, considerandoli atipici rispetto all'attività della struttura.

Di seguito, si riportano i risultati delle attività di risk assesment e risk management alla base della costituzione del Modello, che hanno consentito di individuare i reati di interesse per la società e i processi operativi ad alto/medio rischio esposti alla commissione di reati.

L'analisi dei rischi, rappresentata dalle tabelle riportate di seguito è svolta al netto delle misure di controllo e dei presidi definiti ed attuati dalla Società. Pertanto, i rischi reato sotto definiti sono da considerarsi per la Società a livello "accettabile" poiché irrilevanti o bassi o perché sufficientemente presidiati.

1 PROTOCOLLI GENERALI DI PREVENZIONE

Nell'ambito di tutte le operazioni che concernono le attività sensibili, si attuano i seguenti protocolli generali di prevenzione:

- ❖ sono legittimati a svolgere le attività sensibili solo i soggetti che siano stati preventivamente identificati mediante deleghe, procure, organigrammi, procedure o eventuali disposizioni organizzative;

- ❖ sono legittimati a trattare con tutte le controparti terze solo soggetti che siano stati previamente identificati a tale scopo;
- ❖ il sistema di deleghe e poteri di firma verso l'esterno è coerente con le responsabilità assegnate a ciascun soggetto e la conoscenza di tali poteri da parte dei soggetti esterni è garantita da strumenti di comunicazione e di pubblicità adeguati;
- ❖ la formazione e l'attuazione delle decisioni della Società rispondono ai principi ed alle prescrizioni contenute nelle disposizioni di legge, nello statuto e negli strumenti di attuazione del Modello;
- ❖ sono formalizzate le responsabilità di gestione, coordinamento e controllo;
- ❖ sono formalizzati i livelli di dipendenza gerarchica e sono descritte le diverse mansioni presenti;
- ❖ le fasi di formazione e i livelli autorizzativi degli atti della Società sono sempre documentati e ricostruibili;
- ❖ l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale sono congruenti con le posizioni di responsabilità e con la rilevanza e/o le criticità delle sottostanti operazioni economiche;
- ❖ i documenti riguardanti la formazione delle decisioni e l'attuazione delle stesse sono archiviati e conservati a cura della Funzione competente;
- ❖ l'accesso ai documenti già archiviati è consentito solo alle persone autorizzate in base alle procedure operative della Società, nonché al Revisore dei conti ed all'OdV;

L'OdV verifica che le procedure operative della Società che disciplinano le attività a rischio, che costituiscono parte integrante del Modello, diano piena attuazione ai principi ed alle prescrizioni contenuti nella presente Parte Speciale, e che le stesse siano costantemente aggiornate, anche su proposta dell'OdV stesso, al fine di garantire il raggiungimento delle finalità del presente documento.

INDIVIDUAZIONE DEI POSSIBILI REATI DERIVATI DALLE ATTIVITA' SVOLTE

L'attività di Risk Assesment e Risk Management ha pertanto consentito di individuare i seguenti processi/attività a rischio reato verso la Pubblica Amministrazione previsti dal D.Lgs. 231/01:

- Gestione delle attività di stipula o negoziazione o di rinnovo dei contratti o convenzioni con la Pubblica Amministrazione (Regione, ASL, ecc.);
- Gestione delle ispezioni svolte da parte di Enti/Funzionari della Pubblica Amministrazione presso la società (Nuclei operativi di controllo, funzionari della ASL e della Regione) e delle contestazioni rilevate da quest'ultimi;
- Erogazione di beni e servizi;
- Gestione delle attività amministrative e redazione del bilancio;
- Gestione previdenziale e assistenziale del personale (ad es. selezione, assunzione, formazione, valutazione e incentivazione), gestione dei relativi rapporti e delle ispezioni con la P.A. (INAIL, INPS, Ispettorato del Lavoro, Ufficio Provinciale del Lavoro, Comune, Provincia);
- Gestione delle risorse finanziarie (incassi, pagamenti, versamenti, prelievi con riferimento alla gestione della cassa e dei conti correnti della società)
- Adempimenti relativi ad attività di carattere ambientale e in materia di salute e sicurezza sul lavoro.

Sono stati individuati anche processi strumentali, nel senso che, pur non essendo direttamente esposti al rischio reato, si potrebbero, nel loro ambito, creare le condizioni strumentali per la commissione dei reati previsti dal Decreto legislativo 231/2001 (ad es. finanza dispositiva; selezione e assunzione del personale; gestione delle consulenze; gestione dell'omaggistica, ecc.):

- Accordi transattivi

11 I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

La presente Parte Speciale si applica alla tipologia di reati identificati dagli artt. 24 e 25 del Decreto.

Il concetto di Pubblica Amministrazione in diritto penale viene inteso in senso ampio, comprendendo l'intera attività dello Stato e degli altri enti pubblici. Pertanto, i reati contro la Pubblica Amministrazione perseguono fatti che impediscono o turbano il regolare svolgimento non solo dell'attività in senso tecnico amministrativa, ma anche di quella legislativa e giudiziaria.
La Pubblica Amministrazione è, dunque, intesa come l'insieme di tutte le funzioni pubbliche dello Stato o degli altri enti pubblici.
I soggetti che rappresentano la Pubblica Amministrazione ai fini del diritto penale sono coloro che svolgono una funzione pubblica o un pubblico servizio.
Per funzione pubblica si intendono le attività disciplinate da norme di diritto pubblico che attengono alle funzioni legislativa (Stato, Regioni, Province a statuto speciale, ecc.), amministrativa (amministrazioni statali e territoriali, Forze dell'Ordine, amministrazioni sovranazionali, Authority, Camere di Commercio, Commissioni Edilizie, collaudatori di opere pubbliche, periti del Registro Navale Italiano, ecc.), giudiziaria (giudici, ufficiali giudiziari, organi ausiliari dell'Amministrazione della Giustizia quali curatori o liquidatori fallimentari, ecc.).
La funzione pubblica è caratterizzata dall'esercizio di:

- *potere autoritativo*, cioè di quel potere che permette alla Pubblica Amministrazione di realizzare i propri fini mediante veri e propri comandi, rispetto ai quali il destinatario del comando si trova in una posizione di soggezione. Si tratta dell'attività in cui si esprime il cd. "potere d'imperio", che comprende sia il potere di coercizione (arresto, perquisizione, ecc.) e di contestazione di violazioni di legge (accertamento di contravvenzioni. ecc.), sia i poteri di supremazia gerarchica all'interno di pubblici uffici;
- *potere certificativo, cioè il potere di attestare un fatto con efficacia probatoria.*

Per *pubblico servizio* si intendono le attività disciplinate da norme di diritto pubblico, caratterizza te dalla mancanza dei poteri autoritativi o certificativi tipici della funzione pubblica, con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale. I soggetti che svolgono una funzione pubblica o un pubblico servizio sono denominati pubblici ufficiali o incaricati di pubblico servizio.
Il pubblico ufficiale è colui che può firmare o manifestare la volontà della Pubblica Amministrazione ovvero esercitare poteri autoritativi o certificativi. A titolo esemplificativo e non esaustivo si considerano pubblici ufficiali i membri delle amministrazioni statali e territoriali, i membri delle amministrazioni sovranazionali (ad es., dell'Unione Europea), NOC, NAS, i membri delle Autorità di Vigilanza, i membri delle Forze dell'Ordine e della Guardia di Finanza, i membri delle Camere di Commercio, gli amministratori di enti pubblici economici, i giudici, gli ufficiali giudiziari, gli organi ausiliari dell'Amministrazione della Giustizia (ad es., i curatori fallimentari).
L'incaricato di pubblico servizio svolge invece le attività attinenti alla cura di interessi pubblici o al soddisfacimento di bisogni di interesse generale assoggettate alla vigilanza di un'autorità pubblica. La giurisprudenza penalistica ha chiarito che l'inquadramento burocratico del soggetto nella struttura di un ente pubblico non costituisce criterio per riconoscere la qualifica di incaricato di pubblico servizio, poiché ciò che rileva è l'attività in concreto svolta dal soggetto. Pertanto, anche un privato o il dipendente di una società privata può essere qualificato quale incaricato di pubblico servizio quando svolge attività finalizzate al perseguimento di uno scopo pubblico e alla tutela di un interesse pubblico.
A titolo esemplificativo e non esaustivo possono essere considerati incaricati di pubblico servizio i dipendenti del SSN, gli addetti dell'ufficio casse di un ente pubblico, i dipendenti di enti ospedalieri, dell'INAIL, dell'INPS, i dipendenti di aziende energetiche municipali, di banche, uffici postali, uffici doganali, i membri dei consigli comunali, i dipendenti delle Ferrovie dello Stato, dell'ENI e di concessionari autostradali.

11.1 FATTISPECIE DI REATO RILEVANTI

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

 Concussione (art. 317 c.p.): Reato che si configura quando un pubblico ufficiale o un incaricato di pubblico servizio costringe una persona, abusando della propria posizione, a dare o promettere denaro o altri vantaggi.
 Corruzione per l'esercizio della funzione (art. 318 c.p.): Si verifica quando un pubblico ufficiale riceve o accetta promesse di denaro o altre utilità per l'esercizio delle proprie funzioni.

 Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.): Configurato quando il pubblico ufficiale riceve denaro o altra utilità per compiere atti contrari ai doveri d'ufficio.
 Corruzione in atti giudiziari (art. 319-ter c.p.): Quando le azioni di corruzione sono volte a influenzare l'esito di processi civili, penali o amministrativi.
 Induzione indebita a dare o promettere utilità (art. 319-quater c.p.): Quando un pubblico ufficiale o incaricato di pubblico servizio induce una persona a dare o promettere vantaggi economici o utilità.
 Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.) e **pene per il corruttore (art. 321 c.p.)**: Applicabili in analogia ai reati di corruzione sopracitati.
 Istigazione alla corruzione (art. 322 c.p.): Reato configurato quando qualcuno offre o promette vantaggi economici a un pubblico ufficiale per influenzarne l'operato, anche se l'offerta non è accettata.
 Reati di corruzione e concussione di membri delle istituzioni dell'Unione Europea e di Stati esteri (art. 322-bis c.p.): La legge estende le disposizioni italiane di corruzione e concussione ai funzionari delle istituzioni europee e di Stati esteri.
 Truffa in danno dello Stato, di altri enti pubblici o dell'UE (art. 640, comma 2, n. 1 c.p.) e Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.): Configurate quando una persona ottiene un vantaggio economico a spese dello Stato o dell'UE tramite raggiri.
 Malversazione a danno dello Stato (art. 316-bis c.p.): Reato commesso quando fondi o contributi pubblici vengono destinati a fini diversi da quelli previsti.
 Indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.): Ottenimento di fondi pubblici senza diritto, mediante dichiarazioni false o omissione di informazioni.
 Frode informatica ai danni dello Stato o di altri enti pubblici (art. 640-ter c.p.): Reato che si configura quando una persona altera sistemi informatici per trarre un vantaggio a danno dello Stato.

11.2 ATTIVITA' SENSIBILI

L'art. 6, comma 2, lett. a) del D.lgs. 231/2001 indica, quale elemento essenziale del modello di organizzazione, gestione e controllo, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati rilevanti ai fini dell'applicazione del D.lgs. 231/01. Di seguito sono indicate le attività sensibili e strumentali riferite a ciascuna funzione aziendale esaminata, così come si evince dal documento di mappatura al quale per gli aspetti di dettaglio si rinvia.

- Rappresentanza legale della società in giudizio: gestione delle azioni legali che coinvolgono l'ente, inclusi contenziosi e rapporti con il sistema giudiziario.
- Gestione dei rapporti con funzionari pubblici e con enti governativi: interazioni con Ministeri, aziende statali, enti pubblici locali, e altre autorità amministrative che possono influire sulla conformità normativa e sui rapporti con la Pubblica Amministrazione.
- Gestione dei contributi e degli oneri sociali: adempimento degli obblighi contributivi e sociali, compresa la corretta gestione delle dichiarazioni e dei pagamenti verso enti previdenziali.
- Acquisizione e gestione di finanziamenti pubblici e contributi: richiesta e utilizzo di finanziamenti, sussidi o agevolazioni concesse da enti pubblici nazionali e comunitari, assicurandone la destinazione agli scopi previsti.
- Rapporti e interazioni con i funzionari della Pubblica Amministrazione: monitoraggio delle relazioni con funzionari e rappresentanti della PA per garantire comportamenti etici e conformi alla normativa anticorruzione.
- Stipula e gestione dei contratti di consulenza e delle fatturazioni: valutazione, formalizzazione e monitoraggio dei contratti con consulenti e professionisti esterni, nonché verifica della correttezza delle relative fatturazioni.
- Gestione degli acquisti, delle donazioni, delle sponsorizzazioni e degli incentivi: inclusi gli acquisti di beni e servizi, le donazioni e sponsorizzazioni, e la distribuzione di incentivi, con particolare attenzione alla trasparenza e alla tracciabilità.
- Gestione dei processi relativi a rimborsi e utilizzo di carte di credito aziendali: assicurando che rimborsi spese e utilizzo delle carte di credito siano documentati e coerenti con le politiche aziendali, per evitare eventuali abusi o irregolarità.

Nell'ambito della Area si potrebbero configurare astrattamente le seguenti fattispecie di Reati: a) Reati societari: false comunicazioni sociali (2621 c.c.); impedito controllo (art. 2625 c.c.); indebita restituzione dei conferimenti (art. 2626 c.c.); illegale ripartizione degli utili e delle riserve (art. 2627 c.c.); illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.); operazioni in pregiudizio dei creditori (art. 2629 c.c.); formazione fittizia del capitale (art. 2632 c.c.); indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.); corruzione tra privati (art. 2635 c.c.); istigazione alla corruzione tra privati (art. 2635 - bis); illecita influenza sull'assemblea (art. 2636 c.c.). b) Reati contro e nei rapporti con la Pubblica Amministrazione: malversazione di erogazioni pubbliche (art. 316-bis c.p. – modificato da art. 2 D.l. 25 febbraio 2022 n. 13); indebita percezione di erogazioni pubbliche (art. 316-ter c.p. – modificato da art. 2 D.l. 25 febbraio 2022 n. 13); concussione (art. 317 c.p.); corruzione per l'esercizio della funzione (art. 318 c.p.); corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.) corruzione in atti giudiziari (art. 319 ter c.p.); induzione indebita a dare o promettere utilità (art. 319 quater c.p.); corruzione di persona incaricata di un pubblico sevizio (art. 320 c.p.); Istigazione alla corruzione (art. 322 c.p.); peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis c.p.); truffa (art. 640, comma 2, n. 1, c.p.); truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.); frode informatica ai danni dello stato (art. 640 ter c.p.). c) Reati transnazionali (l. n. 146/2006; induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.); favoreggiamento personale (art. 378 c.p.); associazione per delinquere (art. 416 c.p.); associazioni di tipo mafioso anche straniere (416 bis c.p.). d) Ricettazione e riciclaggio e impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio (artt. 648, 648-bis, art. 648 ter e 648-ter,1 c.p.- modificato dal D.lgs. n.195/2021). e) Associazione per delinquere (art. 416 c.p., ad eccezione del sesto comma); associazioni di tipo mafioso anche straniere (art. 416- bis c.p.). f) Delitti informatici e trattamento illecito di dati: falsità in un documento informatico (art. 491 bis c.p.); accesso abusivo ad un sistema informatico o telematico (art. 615 ter c-p); detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p. – modificato da art. 19 Legge 23 dicembre 2021, n. 238); danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.); danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.); danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.); danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.); frode informatica del certificatore di firma elettronica (art. 640 quinquies c.p.). g) Delitti con finalità di terrorismo o di eversione dell'ordine democratico: associazioni sovversive (art. 270 c.p.); associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270 bis c.p.).

11.3 SOGGETTI COINVOLTI

- Direzione
- Direttore Sanitario

Con riguardo alle attività individuate in questa sezione, sono equiparati ai soggetti coinvolti, sia i responsabili delle Aree che partecipano allo svolgimento del singolo processo, sia i professionisti e i Consulenti esterni, qualora abbiano rilievo nell'esecuzione delle suddette attività.

11.4 REGOLE GENERALI DI COMPORTAMENTO

Con riferimento ai rapporti con la Pubblica Amministrazione la Società ed i Destinatari devono ispirare le proprie attività alle seguenti Regole Generali di Comportamento:

1) è vietata qualsiasi forma di omaggio e/o regalia a funzionari pubblici italiani ed esteri, o a loro familiari, tale da poter influenzare la loro indipendenza di giudizio o indurli ad assicurare un qualsiasi vantaggio per l'azienda;
2) è vietato accordare vantaggi di qualsiasi natura in favore di soggetti legati anche indirettamente alla Pubblica Amministrazione per trarne un profitto;
3) le attività connesse alla gestione degli omaggi devono essere preventivamente pianificate e documentate;
4) i dipendenti aziendali che possono accordare omaggi devono essere individuati nel rispetto delle autorizzazioni necessarie;

5) le linee guida aziendali indicano il comportamento da adottare per la gestione degli omaggi;
6) è vietato effettuare elargizioni in denaro a pubblici funzionari italiani o stranieri al fine di trarne profitto;
7) è vietato promettere assunzioni e/o assumere soggetti legati direttamente alla Pubblica Amministrazione, italiana o straniera, per trarne un profitto;
8) i soggetti aziendali che intrattengono rapporti con la Pubblica Amministrazione devono essere preventivamente individuati;
9) alle ispezioni e/o accertamenti svolti dalla Pubblica Amministrazione (es. Ministero della Salute, Agenzia Entrate, Guardia di Finanza, Asp, VVFF, INPS, etc.) devono partecipare i soggetti preposti nel rispetto delle procedure e del presente Modello;
10) il Responsabile dell'ispezione e/o accertamento dà immediato avviso dell'ispezione e trasmette il rapporto riepilogativo delle attività svolte all'Amministratore, al Responsabile Amministrativo e all'OdV;
11) è vietato presentare dichiarazioni non veritiere ad organismi pubblici nazionali, regionali, provinciali e comunali al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
12) è vietato destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti a scopi diversi da quelli di destinazione;
13) è vietato effettuare qualsivoglia pagamento in contanti se non nei limiti di legge;
14) i soggetti aziendali nell'intraprendere e gestire i rapporti con la Pubblica Amministrazione devono rispettare i principi di correttezza e trasparenza e garanzia dell'integrità e della reputazione delle parti ed osservare le leggi, i regolamenti vigenti, i principi etici, e le procedure esistenti;
15) le procedure relative al rilascio ed alla gestione di licenze, autorizzazioni o concessioni, nonché i rapporti con le Autorità devono essere curate esclusivamente da soggetti aziendali a tal fine autorizzati e devono essere improntate alla massima trasparenza e correttezza, nel rispetto delle leggi e delle altre norme vigenti in materia;
16) la determinazione delle risorse lavorative deve essere effettuata a fronte delle necessità aziendali attraverso gli Organi Sociali a tal fine preposti;
17) ogni assunzione deve essere accompagnata da apposita documentazione da archiviare;
18) la selezione del personale deve avvenire con obiettiva comparazione tra i candidati selezionati;
19) i nuovi assunti devono osservare i principi etici-comportamentali adottati dalla Società;
20) le procedure interne aziendali devono fornire principi di comportamento e modalità operative per lo svolgimento delle Attività Sensibili nonché per le modalità di archiviazione della documentazione rilevante;
21) il sistema delle deleghe deve garantire l'applicazione del principio di separazione di funzioni, per cui l'autorizzazione all'effettuazione di un'operazione, deve essere sotto la responsabilità di persona diversa da chi esegue operativamente o controlla l'operazione;
22) la separazione delle funzioni è attuata anche attraverso l'utilizzo di sistemi informatici che abilitano certe operazioni solo a soggetti identificati ed autorizzati;
23) i poteri autorizzativi e di firma assegnati, devono essere coerenti con le responsabilità organizzative e gestionali e chiaramente definiti e conosciuti all'interno della Società;
24) i Consulenti e fornitori devono osservare i principi etici-comportamentali adottati dalla Società e devono essere selezionati sulla base di criteri di professionalità adeguati al servizio;
25) è vietato riconoscere compensi in favore di Consulenti che non trovino giustificazione in relazione all'incarico conferito.

11.5 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

In aggiunta agli eventuali flussi informativi previsti nella Parte Generale del presente Modello, la funzione coinvolta dovrà dare comunicazione all'OdV in un report annuale di:

1) erogazioni pubbliche, operazioni straordinarie di tesoreria o finanziarie, richieste, effettuate o ottenute dalla Società;
2) ispezioni svolte da Pubbliche Autorità, a seguito delle quali il Responsabile Amministrazione trasmetterà copia del report redatto in tale circostanza;
3) provenienza di fondi dall'estero.

11.6 AREA ACQUISTI

Nell'ambito dell'attività relativa agli acquisti sono stati identificati i seguenti Processi Sensibili:

- emissione richieste di acquisto
- approvvigionamento delle materie produttive e materiali di consumo
- gestione delle fatturazioni e dei rapporti con i collaboratori esterni.

Nell'ambito dell'attività relativa alla Gestione degli Acquisti sono stati identificati i seguenti Processi Sensibili:

- procedura di valutazione delle offerte dei fornitori e trattativa economica
- selezione dei fornitori di beni o servizi.

Nell'ambito dell'area in oggetto si potrebbero configurare astrattamente le seguenti fattispecie di Reati:

a) Reati societari: false comunicazioni sociali (art. 2621 c.c.); corruzione tra privati (art. 2635 c.c.).
b) Reati commessi in relazione ai luoghi di lavoro: omicidio colposo e lesioni colpose gravi o gravissime (artt. 589 e 590 c.p), commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
c) Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio (artt. 648, 648-bis, 648 ter c.p. e 648-ter.1, c.p.).
d) Reati informatici: falso in documenti informatici (art. 491-bis c.p.).

I soggetti che partecipano alle attività svolte dall'Area Acquisti devono adeguare il proprio comportamento, oltre che alle procedure interne adottate dalla Società, alle seguenti regole di condotta:

1. l'accesso ai sistemi informatici deve essere consentito solo a soggetti autorizzati dai Settori e dalle Aree interessate e deve garantire l'evidenza dei singoli passaggi e l'identificazione dei soggetti che inseriscono o correggono i dati contenuti nel sistema;
2. immediata e puntuale comunicazione al responsabile dell'Area Amministrativa di eventuali anomalie individuate, anche in relazione alla possibilità che le stesse abbiano potuto causare significative distorsioni sulla veridicità, legittimità e correttezza dei dati rilevati;
3. ogni acquisto deve essere supportato da idonea documentazione cartacea, debitamente archiviata dalla Responsabile Amministrativa;
4. la Direzione ha l'obbligo di verificare periodicamente lo stato degli ordini di acquisto aperti e mai chiusi;
5. la Responsabile Amministrativa deve gestire gli ordini di acquisto in relazione all'importo economico;
6. la direzione deve verificare la congruità della fatturazione alle prestazioni rese dai collaboratori esterni.

11.7 AREA GESTIONE DEL PERSONALE

Nell'ambito dell'attività relativa alla gestione del personale sono stati identificati i seguenti Processi Sensibili:

Assunzione del Personale

- richiesta di nuove risorse;
- identificazione e utilizzo dei canali di reclutamento;
- selezione dei candidati;
- individuazione dell'inquadramento del candidato;
- assunzione del candidato;
- gestione degli adempimenti previsti per l'assunzione del personale; archiviazione dei documenti relativi alle attività di selezione.

Retribuzioni e bonus

- pianificazione delle politiche e dei criteri di valutazione;
- applicazione dei criteri di valutazione;
- criteri di riconoscimento dei bonus;
- gestione documentazione di valutazione.

Gestione degli stipendi e adempimenti previdenziali e assistenziali

- elaborazione degli stipendi;
- calcolo e adempimenti previsti per i trattamenti previdenziali ed assistenziali;
- predisposizione dichiarazioni per i dipendenti;
- rimborsi presso INPS e INAIL;
- condoni previdenziali;
- gestione delle ispezioni, verifiche e accertamenti da parte delle Autorità (Inps, Inail, Ispettori del lavoro. etc.);
- comunicazioni alle Autorità competenti effettuate con mezzi informatici;
- gestione delle agevolazioni fiscali.

Formazione e finanziamenti

- individuazione dei fabbisogni formativi;
- riscontro dell'efficacia delle attività di formazione;
- gestione di finanziamenti pubblici e contributi agevolati anche in tema di formazione.

I soggetti che partecipano alle attività svolte dall'Area devono adeguare il proprio comportamento, oltre che alle linee guida interne adottate dalla Società, anche alle seguenti regole di condotta:

Selezione ed Assunzione del Personale

1. la determinazione del fabbisogno di risorse umane a tempo indeterminato deve essere svolta collegialmente nel contesto dei Processi di pianificazione delle risorse e debitamente documentato;
2. la richiesta di una nuova risorsa deve essere inoltrata da parte del soggetto richiedente attraverso la sottoscrizione di apposito modulo;
3. nel processo di selezione si devono osservare le regole di tracciabilità delle fonti e di reperimento dei curricula;
4. la selezione deve essere svolta almeno da due soggetti diversi (Responsabile richiedente e il responsabile dell'Area del Personale) ciascuno dei quali valuterà il candidato per gli aspetti di propria competenza;

Bonus e retribuzione

1. per i Dipendenti a cui la Società riconosce anche una parte variabile dello stipendio, questo deve essere calcolato sulla base di target predeterminati annualmente;
2. annualmente viene svolta una valutazione dei Dipendenti finalizzata allo sviluppo personale e professionale delle risorse;
3. al fine dell'elaborazione degli stipendi, la rilevazione delle presenze viene operata esclusivamente per il tramite di sistemi informatici;
4. l'inserimento in busta paga di voci retributive che non siano previste contrattualmente e/o normativamente, deve essere preventivamente autorizzato per iscritto dal Responsabile dell'Area Personale.

Nell'espletamento delle proprie attività, in aggiunta agli eventuali flussi informativi previsti nella Parte Generale del presente Modello, l'Area del Personale dovrà dare comunicazione scritta di:

1. ogni modifica rilevante della struttura e/o dell'organigramma aziendale;
2. eventuale ottenimento di benefici e/o sgravi fiscali solo per progetti regionali nonché dell'eventuale ottenimento di finanziamenti pubblici in relazione alla gestione e formazione del personale;
3. notizie relative ai comportanti da cui possono derivare procedimenti dovuti al mancato rispetto degli obblighi previsti dal Sistema disciplinare allegato al presente Modello;

eventuali accertamenti/ispezioni in materia previdenziale e/o comunque inerenti al personale.

12 REATI SOCIETARI

I Reati, qui di seguito considerati, trovano come presupposto i comportamenti che possano portare un beneficio alla Società attraverso l'esposizione di fatti materiali non rispondenti al vero oppure nell'omissione di informazioni la cui comunicazione è imposta dalla legge e finalizzata a fornire periodicamente il risultato economico e la situazione patrimoniale.

12.1 FATTISPECIE DI REATO RILEVANTI

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato, ai sensi dall'art. 25-ter del D.lgs. n. 231/2001, si rinvia all'Allegato n. 1 e si elencano qui di seguito i Reati ritenuti rilevanti.

- False comunicazioni sociali (art. 2621 c.c.)
- Impedito controllo (art. 2625 c.c.)
- Indebita restituzione dei conferimenti (art. 2626 c.c.)
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)
- Illecite operazioni sulle azioni o quote sociali o della Società controllante (art. 2628 c.c.)
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
- Formazione fittizia del capitale (art. 2632 c.c.)
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)
- Corruzione tra privati (art. 2635 c.c.)
- Istigazione alla corruzione tra privati (art. 2635 - bis)
- Illecita influenza sull'assemblea (art. 2636 c.c.).

12.2 ATTIVITÀ SENSIBILI

Attraverso l'analisi dei Processi della Società, così come descritta nella Parte Generale, sono state individuate le seguenti Attività Sensibili, nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25-ter del D.lgs. n. 231/2001:

- gestione della fatturazione attiva/passiva;
- gestione della documentazione, delle informazioni e dei dati necessari per l'elaborazione del bilancio, formazione ed elaborazione del bilancio di esercizio, della nota integrativa e della relazione sulla gestione (se obbligatori)
- predisposizione delle comunicazioni sociali relative alla situazione economica, patrimoniale e finanziaria della Società (bilancio di esercizio, relazione sulla gestione, relazioni periodiche);
- operazioni relative al capitale sociale (i.e. gestione dei conferimenti, dei beni sociali, degli utili e delle riserve, operazioni sulle partecipazioni e sul capitale);
- gestione dei conferimenti, degli utili e delle riserve e operazioni straordinarie;
- indicazione delle esigenze di accantonamenti ai fondi di svalutazione dei crediti;
- gestione albo fornitori;
- gestione degli acquisti di beni e servizi produttivi (es. materie prime, etc.) e non produttivi;
- gestione dei Consulenti e professionisti;
- gestione delle risorse economiche – finanziarie;
- gestione dei professionisti esterni;
- gestione dei flussi finanziari da e verso l'estero;
- calcolo e pagamento imposte, tasse e tributi;
- gestione e pagamenti dei servizi in outsourcing;
- gestione di agevolazioni fiscali, finanziamenti pubblici, sgravi, etc.

12.3 REGOLE GENERALI DI COMPORTAMENTO

Con riferimento ai Reati societari la Società ed i Destinatari devono ispirare le proprie attività alle seguenti Regole Generali di Comportamento:

1) i soggetti coinvolti in attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali devono tenere un comportamento corretto, trasparente e collaborativo nel rispetto delle norme di legge e delle procedure aziendali interne allo scopo di fornire ai soci ed ai Terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;

2) gli Organi Sociali devono osservare le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale al fine di non ledere le garanzie dei creditori e dei Terzi in genere;
3) gli Organi Sociali devono garantire ed agevolare le necessarie forme di controllo interno sulla gestione sociale previste dalla legge, nonché la libera e corretta formazione della volontà assembleare;
4) è vietato ai soggetti preposti alla formazione del bilancio e delle altre comunicazioni sociali di omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
5) è vietato ai soggetti preposti attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali rappresentare o trasmettere, per l'elaborazione e la rappresentazione in bilancio, relazioni, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società;
6) è vietato agli Organi Sociali restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale o nel rispetto della legge;
7) è vietato agli Organi Sociali ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
8) è vietato acquistare o sottoscrivere quote della Società fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;
9) è vietato agli Organi Sociali effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
10) è vietato agli Organi Sociali procedere a formazione o aumento fittizi del capitale sociale, attribuendo quote per un valore inferiore al loro valore nominale;
11) è vietato agli Organi Sociali distrarre beni sociali, in sede di liquidazione della Società, dalla loro destinazione ai creditori, ripartendoli tra i soci prima del pagamento dei creditori o dell'accantonamento delle somme necessarie a soddisfarli;
12) è vietato agli Organi Sociali determinare o influenzare il regolare procedimento di formazione della volontà assembleare con atti simulati o fraudolenti;
13) è vietato sollecitare o ricevere denaro o altra utilità non dovuti, o accettarne la promessa, per compiere o per omettere un atto in violazione;
14) è vietata la violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà verso la Società ovvero istigare tale comportamento;
15) ogni Direzione/Settore/Area è responsabile della comunicazione dei dati e delle informazioni anche quelli rilevati sistematicamente e necessari per una corretta rappresentazione economica, patrimoniale e finanziaria della Società;
16) ogni Direzione è responsabile della comunicazione dei dati per la valutazione degli accantonamenti in fondi rischio;
17) tutte le notizie e le consultazioni relative agli affari sociali richieste a norma dell'art. 2476 c.c. sono indirizzate dai Soci all'Amministratore;
18) tutte le transazioni di natura finanziaria, tra cui il rilascio di eventuali fideiussioni o impegni a pagare, sono effettuate sulla base di idonea documentazione nel rispetto delle deleghe concordate;
19) le attività di gestione delle risorse finanziarie devono svolgersi nel rispetto dei principi di separazione di responsabilità tra il soggetto che ordina, colui che autorizza il pagamento e colui che controlla i flussi finanziari;
20) il sistema dei pagamenti di fornitori e Consulenti rispetta un piano di scadenze programmato in base alle condizioni generali d'acquisto o termini contrattuali prestabiliti;
21) la Direzione verifica che per ogni pagamento vi sia specifica autorizzazione dell'Amministratore;
22) i Fornitori devono essere selezionati sulla base di specifici requisiti di professionalità;
23) ogni acquisto è supportato da idonea documentazione cartacea che deve essere debitamente archiviata;
24) la congruità tra i beni ordinati e quelli forniti viene verificata al momento della consegna attraverso il sistema informatico SAP;
25) i pagamenti dei servizi e le consulenze sono effettuati a seguito dell'autorizzazione da parte dei soggetti richiedenti tale servizio o consulenza;
26) la Società pianifica il conto economico e lo stato patrimoniale;

27) i dati contabili che confluiscono in un report sono elaborati periodicamente ed inviati ai soci;
28) è vietata la compensazione tra debiti e crediti dei fornitori;
29) i singoli Settori trasmettono alla Direzione ogni informazione rilevante ai fini della formazione del bilancio, per consentirne il controllo e garantirne veridicità, correttezza, precisione e completezza;
30) la trasmissione dei dati contabili deve avvenire mediante sistema informatico che consenta di tracciare i singoli passaggi e di identificare i soggetti che inseriscono e ricevono i dati.

12.4 PROCEDURE SPECIFICHE DI PREVENZIONE E CONTROLLO

I soggetti che partecipano alle attività svolte devono adeguare il proprio comportamento, oltre che alle procedure interne adottate dalla Società, alle seguenti regole di condotta:

Gestione dei sistemi informatici

1) l'accesso al sistema informatico deve essere consentito solo a soggetti autorizzati;
2) il sistema informatico deve garantire l'evidenza dei singoli accessi tracciandone l'identità dell'utente, gli inserimenti ed eventuali modifiche dei dati;
3) le attività di verifica, manutenzione ed aggiornamento del sistema informatico devono eseguirsi con periodicità almeno annuale;
4) la gestione dell'attività amministrativa e contabile della Società deve avvenire attraverso il sistema informatico.

Gestione documentale

1) i contratti e la documentazione amministrativo contabile deve essere registrata e conservata ad un unico protocollo;
2) Il responsabile d'area si assicura che l'utenza abbia potuto prendere visione della informativa privacy e abbia sottoscritto relativa dichiarazione;
3) Il responsabile d'area si assicura che la documentazione amministrativa informatica e cartacea sia accessibile esclusivamente ai soggetti autorizzati, all'uopo conservando la stessa in sistemi informatici dotati di password e schedari dotati di chiavi o combinazioni.

Gestione dei flussi

1) la comunicazione di dati e di informazioni contabili tra i soggetti coinvolti deve avvenire sempre per iscritto;
2) i soggetti che, nello svolgimento della propria attività, vengono a conoscenza di eventuali anomalie, anche in relazione alla veridicità, legittimità e correttezza dei dati, devono darne comunicazione immediata e puntuale al Responsabile di Area.

Elaborazione Bilancio e reportistica

1) l'elaborazione dei report contabili ai soci viene effettuata dalla Direzione;
2) con cadenza semestrale si svolge la pianificazione previsionale dei dati contabili relativi ai risultati operativi e una volta l'anno si effettua la pianificazione del budget per l'anno successivo; (Assegnazione che avviene attraverso apposita delibera);
3) l'aggiornamento del piano dei conti deve essere corredato di criteri esplicativi per ciascun settore di riferimento;
4) le chiusure di periodo contabile e le scritture contabili devono avvenire in base ad un calendario prestabilito;
5) i risultati contabili devono essere determinati nel rispetto dei criteri di trasparenza;
6) la valutazione degli accantonamenti a Fondi rischi viene effettuata dal Responsabile di Area di concerto con l'Amministratore;
7) l'Amministratore sottoscrive una dichiarazione annuale di veridicità dei dati e delle informazioni di maggior rilievo.

Gestione pagamenti ordini

1) il Responsabile dell'amministrazione ha l'obbligo di bloccare ogni pagamento qualora non sia presente un ordine d'acquisto, con eccezione di pagamenti relativi a tasse, imposte, e quant'altro specificatamente indicato in deroga;

2) ogni pagamento deve essere supportato da idonea documentazione che deve essere debitamente archiviata dal Responsabile Acquisti.

Verifiche e controlli

1) il Responsabile dell'amministrazione effettua il controllo dei dati contabili da far confluire in un report mensile
2) La Direzione deve elaborare apposito report attestante la provenienza di eventuali fondi dall'estero;
3) in caso di ispezioni da parte di Pubbliche Autorità (Agenzia delle Entrate, Guardia di Finanza, Ministero Sviluppo Economico, ASP, Regione, Ministero della Salute, etc.), l'amministratore è il soggetto preposto ad intrattenere rapporti con gli incaricati delle Pubbliche Autorità. All'esito dell'ispezione deve elaborare un report indicando eventuali partecipanti, documenti e tipo di ispezione svolta.

Gestione dei conti correnti

1) l'accesso ai sistemi telematici bancari è consentito all'Amministratore nonché ad eventuale altro soggetto a ciò espressamente autorizzato;
2) il Responsabile Amministrazione verifica periodicamente la corrispondenza tra incassi contabilizzati e quanto versato sul conto corrente bancario;
3) il Responsabile Amministrazione esamina costantemente le movimentazioni del conto corrente;
4) la direzione con l'ausilio del Responsabile Amministrazione effettua periodicamente le attività di riconciliazione sui conti correnti;
5) i pagamenti sono effettuati dall'Amministratore della società;
6) i pagamenti sono autorizzati previo ottenimento delle preliminari firme dei soggetti preposti in linea con il Sistema delle deleghe adottato.

12.5 SOGGETTI COINVOLTI

I principali soggetti coinvolti nella prevenzione dei reati societari sono:

- **Direzione**: Responsabile della trasparenza e correttezza dei dati contabili e delle comunicazioni sociali. Garantisce l'integrità delle operazioni contabili e la corretta gestione documentale.
- **Organismo di Vigilanza (OdV)**: Supervisiona il rispetto delle procedure e riceve segnalazioni di eventuali irregolarità.

12.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (OdV)

L'OdV deve ricevere periodicamente:

- Report di verifica contabile: Aggiornamenti periodici sull'andamento delle operazioni contabili.
- Segnalazioni di irregolarità: Comunicazioni di eventuali anomalie riscontrate nei dati e nelle operazioni contabili.
- Relazione di ispezione: In caso di verifiche o ispezioni da parte delle Autorità Pubbliche, redazione di un report con esito e documentazione relativa.

12.7 CONCLUSIONI

La società si impegna a garantire la massima trasparenza e conformità nelle proprie pratiche amministrative e societarie. L'applicazione rigorosa dei protocolli adottati e il rispetto delle regole comportamentali assicurano una gestione etica e trasparente.

13 REATI TRIBUTARI (Art. 25 quinquiesdecies)

A partire dal 25 dicembre 2019, con la legge di conversione n. 157 del 19 dicembre 2019, è stato introdotto l'art. 25-quinquiesdecies nel D.lgs. n. 231/2001, ampliando il novero dei reati presupposto e includendo specifici reati tributari. Successivamente, ulteriori modifiche normative hanno esteso e aggiornato tali fattispecie.

13.1 FATTISPECIE DI REATO

Le principali fattispecie di reato rilevanti ai sensi dell'art. 25-quinquiesdecies del D.lgs. n. 231/2001 includono:

- **Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.lgs. n. 74/2000):** Chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, utilizza fatture o altri documenti per operazioni inesistenti, indicando in dichiarazione elementi passivi fittizi.
- **Dichiarazione fraudolenta mediante altri artifici (art. 3 D.lgs. n. 74/2000):** Chiunque, con operazioni simulate o documenti falsi, indica in dichiarazione elementi attivi inferiori a quelli effettivi o elementi passivi fittizi, con l'intento di evadere le imposte.
- **Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.lgs. n. 74/2000):** Chiunque emette o rilascia fatture o altri documenti per operazioni inesistenti, consentendo a terzi l'evasione delle imposte.
- **Occultamento o distruzione di documenti contabili (art. 10 D.lgs. n. 74/2000):** Chiunque occulta o distrugge, in tutto o in parte, le scritture contabili o i documenti di cui è obbligatoria la conservazione, impedendo la ricostruzione dei redditi o del volume d'affari.
- **Sottrazione fraudolenta al pagamento di imposte (art. 11 D.lgs. n. 74/2000):** Chiunque, al fine di sottrarsi al pagamento di imposte, aliena simulatamente o compie altri atti fraudolenti sui propri o altrui beni, rendendo inefficace la procedura di riscossione.
- **Dichiarazione infedele (art. 4 D.lgs. n. 74/2000):** Chiunque, al fine di evadere le imposte, indica in dichiarazione elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi inesistenti, superando determinate soglie di punibilità.
- **Omessa dichiarazione (art. 5 D.lgs. n. 74/2000):** Chiunque, obbligato alla presentazione della dichiarazione dei redditi o IVA, omette di presentarla, con imposta evasa superiore a specifiche soglie.
- **Indebita compensazione (art. 10-quater D.lgs. n. 74/2000):** Chiunque utilizza in compensazione crediti non spettanti o inesistenti, non versando le somme dovute, oltre determinate soglie.

13.2 ATTIVITA' SENSIBILI

La valutazione del rischio di commissione dei reati tributari è stata effettuata secondo una valutazione che tiene conto della probabilità di commissione delle violazioni tributarie da parte della società e della presenza di un sistema di prevenzione del rischio reato predisposto dalla medesima. L'analisi dei processi aziendali ha permesso di individuare le seguenti attività sensibili, nelle quali potrebbero astrattamente realizzarsi le fattispecie di reato sopra elencate:

- Gestione delle operazioni straordinarie.
- Approvvigionamento di beni e servizi.
- Servizi generali.
- Consulenza e attività professionali.
- Pianificazione e controllo di gestione.
- Bilancio e comunicazioni periodiche.
- Gestione delle risorse finanziarie.
- Amministrazione del personale.
- Regalie, omaggi e spese di rappresentanza.
- Spese di sponsorizzazione.
- Tenuta e conservazione delle scritture contabili e fiscali.
- Gestione delle alienazioni di beni mobili, immobili e partecipazioni.

Protocollo per il processo decisionale relativo agli adempimenti fiscali

La Direzione procede al controllo sulla regolarità e correttezza delle scritture e dei libri/registri contabili /fiscali e dell'afferente documentazione.

La Società con contabilità ordinaria deve tenere i seguenti registri/libri:

- registro delle fatture emesse: ove registrare le fatture emesse;
- registro degli acquisti: ove registrare le fatture ricevute;
- registro dei corrispettivi: ove registrare gli incassi originati da scontrini e ricevute fiscali;
- registro dei cespiti ammortizzabili: ove registrare i beni strumentali soggetti ad ammortamento;
- libro giornale: ove registrare tutti i fatti economici e patrimoniali (acquisti, vendite, pagamenti, incassi ecc.);

- libro inventari: ove registrare la consistenza patrimoniale dell'impresa al termine di ogni esercizio.

13.3 REGOLE GENERALI DI COMPORTAMENTO

La Società e i Destinatari devono ispirare le proprie attività alle seguenti regole generali di comportamento:

Trasparenza e correttezza:

Ogni operazione o transazione deve essere autorizzata, verificabile, legittima, coerente e congrua.

Assicurarsi, prima di stabilire relazioni o stipulare contratti con clienti e partner, dell'integrità morale, della reputazione e del buon nome della controparte.

Conformità normativa:

Tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate all'emissione delle fatture, alla tenuta della contabilità e alla predisposizione dei bilanci.

Documentazione e tracciabilità:

Assicurare che tutto il processo di gestione della contabilità aziendale sia condotto in maniera trasparente e documentabile.

Le operazioni che comportano l'utilizzo o l'impiego di risorse economiche o finanziarie devono avere una causale espressa e essere documentate e registrate in conformità ai principi di correttezza e trasparenza contabile.

13.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

→ Per le operazioni riguardanti le attività di valutazione dei fornitori e dei clienti; di acquisto di prodotti finiti, beni e servizi; di presentazione di prodotti finiti, beni e servizi i protocolli prevedono che:

1. Nell'effettuare transazioni potenzialmente a "rischio", o "sospette" rispetto agli standard ed i principi richiesti dal Decreto, si effettui la valutazione di fornitori e clienti sulla base dei seguenti parametri orientativi:
   - Profilo soggettivo della controparte (es. reputazione opinabile; ammissioni o dichiarazioni della controparte in ordine al proprio coinvolgimento in attività criminose);
   - Verifica su esistenza e operatività del fornitore (camerale, fatturato, addetti, esistenza sede operativa);
   - Verifica di coerenza tra l'oggetto dell'attività e quanto descritto sulle fatture;
   - Verifica dei soggetti coinvolti dalla quale non devano emergere simulazioni soggettive (soggetti interposti);
   - Comportamento della controparte (es. comportamenti ambigui, mancanza di dati occorrenti per la realizzazione delle operazioni oggetto dell'affare o reticenza a fornirli);
   - Dislocazione territoriale della controparte (es. operazioni effettuate in paesi off-shore);
   - Profilo economico-patrimoniale dell'operazione (es. operazioni non usuali per tipologia, frequenza, tempistica, importo, dislocazione geografica);
   - Caratteristiche e finalità dell'operazione (es. uso di prestanomi, modifiche delle condizioni contrattuali standard, finalità dell'operazione).
2. La scelta dei partners commerciali avviene dopo aver svolto idonee verifiche sulla reputazione sull'affidabilità degli stessi all'interno del mercato, nonché dopo aver condiviso i fondamentali principi etici che guidano la Società.
3. I contratti che regolano i rapporti con i fornitori e con i clienti devono prevedere apposite clausole che indichino la volontà di costoro di rispettare i principi e i protocolli redatti all'interno del presente Modello e del Codice Etico, e in generale i postulati stabiliti dal Decreto.

→ Per le operazioni riguardanti la gestione dei flussi finanziari in entrata e in uscita, i protocolli prevedono che:

1. Siano predisposti, per tutti i soggetti dotati di poteri formali di movimentazione delle risorse finanziarie, specifici limiti per tipologia di operazione, frequenza, importo; inoltre è richiesta la firma congiunta di almeno due soggetti per operazioni sopra certe soglie di valore prestabilite.
2. Per la gestione dei flussi in entrata e in uscita, devono essere utilizzati esclusivamente i canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione europea o enti creditizi/finanziari situati in uno Stato extracomunitario, che imponga obblighi equivalenti a quelli previsti dalle leggi sul riciclaggio e preveda il controllo del rispetto di tali obblighi.

3. Sono vietati i flussi sia in entrata che in uscita in denaro contante, salvo che per tipologie minime di spesa espressamente autorizzate dal Legale Rappresentante o da suo delegato, ed in particolare per le operazioni di piccola cassa.
4. Le operazioni che comportano utilizzazione o impiego di risorse economiche o finanziarie hanno una causale espressa e sono documentate e registrate in conformità ai principi di correttezza e trasparenza contabile.
5. Gli incassi e i pagamenti della Società, nonché i flussi di denaro, sono sempre tracciabili e provabili documentalmente.

→ Per le operazioni riguardanti la corretta tenuta e custodia delle scritture contabili e fiscali, i protocolli prevedono che:

1. Debbano essere sempre osservate le norme civilistiche (unitamente al principio contenuto nell'articolo 8, comma 5 dello Statuto del contribuente - legge 212/2000), che prevedono il principio generale sulla conservazione delle scritture contabili secondo cui vanno conservati per 10 anni dalla data della loro ultima registrazione: i registri e le scritture contabili obbligatorie (Libro giornale Libro degli inventari, Libri sociali, Registri prescritti ai fini dell'imposta sul valore aggiunto, Scritture ausiliarie nelle quali devono essere registrati gli elementi patrimoniali e reddituali; Scritture ausiliarie di magazzino), le lettere, la corrispondenza commerciale, i telegrammi e le fatture.
2. Nel caso in cui sia in corso un accertamento, le scritture contabili obbligatorie devono essere conservate anche oltre questo termine e almeno fino a quando non siano definiti gli accertamenti relativi al corrispondente periodo d'imposta.
3. I documenti fiscali allegati alla dichiarazione dei redditi devono essere conservati fino al 31 dicembre del quarto anno successivo alla presentazione della stessa. Per 5 anni devono essere anche conservate le ricevute d'affitto, le utenze domestiche, le multe e le contravvenzioni.
4. Per quanto concerne invece i documenti informatici rilevanti ai fini tributari, come ad esempio le fatture attive e passive, i documenti di trasporto, i registri IVA e i registri contabili, essi non sono esonerati dal rispetto delle norme civilistiche (il riferimento è agli articoli 2220, 2214, 2215 bis e 2217 del Codice civile).
5. I documenti digitali (ossia i documenti dematerializzati) validi ai fini fiscali devono possedere i requisiti dell'immodificabilità, dell'integrità, dell'autenticità e della leggibilità.
6. Va osservata la disciplina vigente circa le modalità di segnalazione agli organi competenti in caso di eventi accidentali che possono deteriorare le scritture.
7. Vanno effettuate delle verifiche periodiche sulla corretta tenuta e conservazione dei registri e delle scritture contabili obbligatorie.
8. Devono essere esattamente individuate le funzioni aziendali incaricate e legittimate alla tenuta e movimentazione dei registri e delle altre scritture contabili obbligatorie.

13.5 SOGGETTI COINVOLTI

I principali soggetti responsabili della corretta gestione fiscale e della prevenzione dei reati tributari sono:

- **Direzione:** Responsabile della supervisione contabile e della conformità alle normative fiscali. Deve attenersi alle regole di registrazione e documentazione delle operazioni fiscali e garantire la trasparenza dei processi
- **Organismo di Vigilanza (OdV)**: Monitora l'aderenza alle procedure e riceve segnalazioni di possibili irregolarità fiscali.
- **Consulenti Esterni**

13.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

Per assicurare la supervisione dei rischi tributari, l'OdV deve ricevere periodicamente:

- Report di verifica delle scritture contabili: Aggiornamenti sui controlli periodici effettuati sulla contabilità.
- Segnalazioni di anomalie o irregolarità: Comunicazioni su eventuali discrepanze o sospette violazioni riscontrate.

- Accesso alla documentazione contrattuale e fiscale: Disponibilità di registri e contratti per eventuali verifiche di conformità.

13.7 CONCLUSIONI

La struttura si impegna a garantire il pieno rispetto delle normative tributarie, applicando misure rigorose per il controllo e la gestione dei processi fiscali. L'adozione dei protocolli previsti nel modello organizzativo contribuisce a tutelare la struttura da rischi di non conformità, assicurando la trasparenza e la correttezza delle operazioni contabili.

14 DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

Nei Reati contro l'industria e il commercio trovano tutela l'economia pubblica, gli scambi e gli interessi del sistema economico nell'esercizio delle attività industriali e/o commerciali.

14.1 FATTISPECIE DI REATO

Sebbene il rischio sia basso, è comunque possibile includere i reati di:

- **Turbata libertà dell'industria o del commercio (art. 513 c.p.)**
- **Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.)**

Questo permette di garantire che la struttura rispetti la normativa in caso di eventuali attività di marketing, politiche commerciali o partnership con consulenti.

14.2 ATTIVITÀ SENSIBILI

Le attività che potrebbero astrattamente presentare rischi di reati contro l'industria e il commercio sono:

- Comunicazione di informazioni riservate: Condivisione di dati interni su strategie commerciali o finanziarie con consulenti o partner, che devono essere regolamentati e riservati.
- Definizione e attuazione delle politiche commerciali: Creazione di accordi, promozioni o politiche di marketing che possano teoricamente influenzare la concorrenza.
- Vendita di servizi ai clienti: Comunicazioni e accordi con i clienti, per garantire che le pratiche commerciali siano corrette e trasparenti.

14.3 REGOLE GENERALI DI COMPORTAMENTO

Con riferimento ai Reati contro l'industria ed il commercio, la Società ed i Destinatari devono ispirare le proprie attività alle seguenti Regole Generali di Comportamento:

1) i contratti, le convenzioni, ed ogni altro documento che disciplinino i servizi offerti dalla società devono espressamente prevedere su quale delle parti contrattuali incomba l'onere di controllare il rispetto della normativa in materia di gestione dei brevetti;
2) i contratti, le convenzioni, ed ogni altro documento conclusi con i clienti devono essere definiti per iscritto, in tutte le loro condizioni e termini e contenere clausole specifiche al fine del rispetto dei principi contenuti nel D.Lgs. 231/2001 ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti previsti dal presente capitolo;
3) è vietato alla Società porre in essere forme intimidatorie di qualsivoglia natura nei confronti di una società concorrente;
4) è vietato utilizzare conoscenze usurpando il titolo di proprietà industriale o in violazione dello stesso;
5) è vietato importare nel nostro Stato merci destinate dal titolare del marchio ad essere commercializzate altrove;
6) i ruoli e le responsabilità dei Consulenti operanti per conto della società nell'attuazione delle politiche commerciali della società stessa devono essere preventivamente individuati;
7) i contratti con i Consulenti devono essere debitamente archiviati.

14.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

Per prevenire e controllare il rischio di violazioni delle normative relative all'industria e al commercio, la struttura deve adottare i seguenti protocolli:

- Verifica delle pratiche commerciali e marketing: Assicurarsi che tutte le politiche commerciali siano conformi alla normativa e non mirino a ostacolare la libera concorrenza o a interferire con le attività di altre strutture sanitarie.
- Protezione delle informazioni riservate: Regolamentare la gestione delle informazioni riservate e limitare l'accesso solo al personale autorizzato, per evitare la diffusione di dati sensibili che possano danneggiare la concorrenza.
- Controllo sui consulenti e partner esterni: Verificare che consulenti e partner rispettino le normative sulla concorrenza e non adottino comportamenti intimidatori o lesivi per i concorrenti della struttura.
- Documentazione dei contratti: Garantire che tutti i contratti con clienti e consulenti includano clausole di tutela della concorrenza e siano debitamente archiviati e accessibili per eventuali verifiche.

14.5 SOGGETTI COINVOLTI

I principali soggetti coinvolti nella gestione e prevenzione dei reati contro l'industria e il commercio sono:

- **Direzione**: Supervisiona le politiche commerciali, assicurandosi che siano conformi alle normative in materia di concorrenza. Assicura che tutte le operazioni commerciali e i contratti siano conformi alle normative e al codice etico aziendale. Assicura che tutte le operazioni commerciali e i contratti siano conformi alle normative e al codice etico aziendale.
- **Organismo di Vigilanza (OdV)**: Monitora il rispetto delle disposizioni del modello organizzativo, verificando l'aderenza alle normative.
- **Amministratore di sistema**: Gestisce e protegge le informazioni riservate, limitandone l'accesso e monitorando eventuali usi impropri.

14.6 CONCLUSIONI

La società si impegna a garantire la massima trasparenza e correttezza nelle proprie pratiche commerciali, nel rispetto della libera concorrenza e delle normative vigenti in materia di tutela dell'industria e del commercio. Attraverso l'adozione e l'applicazione rigorosa dei protocolli previsti, la società assicura che tutte le attività siano svolte con integrità e nel rispetto dei diritti di proprietà industriale e intellettuale.

15 VIOLAZIONE DEI DIRITTI D'AUTORE

I Reati, qui di seguito considerati, hanno come presupposto la gestione dei diritti d'autore attraverso la tutela delle opere dell'ingegno umano che si concretizzano nell'elaborazione di invenzioni e/o creazioni.

15.1 FATTISPECIE DI REATO RILEVANTI

Le principali fattispecie rilevanti per la società sono:

- **Protezione del diritto d'autore e di altri diritti connessi** (art. 171-ter della legge n. 633/1941): Questa disposizione punisce la duplicazione, riproduzione o condivisione non autorizzata di software, banche dati e altri materiali protetti da copyright. Rilevante in caso di installazione o utilizzo di software privi di licenza valida o di accesso non autorizzato a materiali protetti.

15.2 ATTIVITÀ SENSIBILI

Le attività potenzialmente esposte al rischio di violazione del diritto d'autore sono:

- Utilizzo di software e gestione delle licenze: Assicurare che tutto il software sia autorizzato e in conformità con le licenze d'uso.
- Predisposizione e archiviazione dei dati su supporti informatici: Monitorare l'archiviazione, trasmissione e custodia dei dati dei pazienti, garantendo che siano protetti da accessi non autorizzati e nel rispetto delle licenze.
- Accesso e navigazione in Internet: Prevenire l'uso improprio di Internet e l'accesso a siti non autorizzati per lo scaricamento di materiali protetti.

15.3 REGOLE GENERALI DI COMPORTAMENTO

Con riferimento alla violazione del diritto d'autore la Società ed i Destinatari devono ispirare le proprie attività alle seguenti Regole Generali di Comportamento:

1. i sistemi informatici aziendali devono essere utilizzati per finalità di natura esclusivamente professionale, attinenti allo svolgimento dell'attività lavorativa del dipendente che effettua l'accesso;
2. è vietato installare qualsivoglia programma, anche se attinente all'attività aziendale, senza essere autorizzato dalla Direzione;
3. è vietato duplicare o riprodurre opere protette dal diritto d'autore, in assenza di espressa autorizzazione da parte del titolare del diritto d'autore o degli aventi diritto;
4. è vietato diffondere o modificare opere protette dal diritto d'autore, in assenza di espressa autorizzazione da parte del titolare del diritto d'autore o degli aventi diritto;
5. è vietato concedere in locazione o detenere a scopo commerciale opere protette dal diritto d'autore, in assenza di espressa autorizzazione da parte del titolare del diritto d'autore o degli aventi diritto;
6. è vietato svolgere attività di file *sharing*, attraverso lo scambio e/o la condivisione di file ovvero attraverso piattaforme peer to peer in assenza di espressa autorizzazione da parte del titolare del diritto d'autore o degli aventi diritto;
7. è vietato utilizzare software/banche dati in assenza di valida licenza ovvero nel caso in cui la stessa sia scaduta;
8. i soggetti preposti alla gestione e protezione delle licenze software e delle banche dati devono essere specificatamente individuati;
9. le politiche di sicurezza e i criteri di autorizzazione per l'accesso alle banche dati devono essere specificatamente individuati.

15.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

Per prevenire violazioni del diritto d'autore, la struttura deve adottare i seguenti protocolli di controllo:

- Verifica delle licenze software: Assicurarsi che tutto il software utilizzato abbia licenze valide e aggiornate. Effettuare audit periodici per controllare la conformità delle licenze.
- Accesso limitato ai sistemi informatici: Implementare sistemi di controllo per autorizzare e monitorare l'accesso ai sistemi e ai dati, limitando l'uso alle persone autorizzate.
- Gestione delle autorizzazioni per l'installazione di software: Consentire l'installazione di software solo previa autorizzazione della Direzione, che deve garantire la legittimità e la sicurezza dei programmi.
- Monitoraggio dell'attività di navigazione in Internet: Controllare l'accesso a siti esterni per prevenire lo scaricamento e la condivisione non autorizzata di materiale protetto.
- Formazione continua del personale: Offrire alla personale formazione sulle normative relative al diritto d'autore, sulle politiche aziendali di utilizzo del software e sulle pratiche di file sharing.

15.5 SOGGETTI COINVOLTI

I principali soggetti coinvolti nella gestione e prevenzione delle violazioni del diritto d'autore sono:

- **Direzione**: Supervisiona l'uso del software e la gestione delle licenze, garantendo la conformità con le normative sul diritto d'autore.
- **Organismo di Vigilanza (OdV)**: Monitora l'aderenza al modello organizzativo e riceve segnalazioni su potenziali violazioni.
- **Personale che utilizza software e banche dati**: Deve rispettare le politiche aziendali sul diritto d'autore e segnalare qualsiasi anomalia riscontrata nell'uso dei programmi.

15.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

L'OdV deve ricevere periodicamente:

- Report di verifica delle licenze software: Documentazione sull'uso dei software e sulla conformità delle licenze.
- Segnalazioni di violazioni sospette: Informazioni su eventuali violazioni o accessi non autorizzati ai materiali protetti.

- Report periodici sulle attività di formazione: Report sulle attività di formazione effettuate per sensibilizzare il personale sul rispetto del diritto d'autore.

15.7 CONCLUSIONI

La società si impegna a garantire il rispetto rigoroso delle normative sul diritto d'autore e la protezione della proprietà intellettuale, attraverso un uso attento e responsabile dei software, delle banche dati e delle risorse digitali. L'adozione di protocolli specifici e di regole chiare per l'utilizzo delle risorse informatiche assicura che tutte le attività aziendali siano condotte in conformità con i diritti d'autore e a tutela della legalità e trasparenza.

16 REATI IN RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA E AUTORICICLAGGIO

I reati, qui di seguito considerati, hanno come presupposto le attività economicamente apprezzabili che abbiano ad oggetto lo scambio di denaro, di materie prime, di beni materiali ed immateriali in genere, provenienti da reato.

In data 4 novembre 2021, il Consiglio dei ministri, su proposta del Presidente Mario Draghi e dei Ministri competenti, ha approvato, in esame definitivo, dopo il previsto passaggio parlamentare, diciotto decreti legislativi di attuazione di norme europee già esaminati in via preliminare; in particolare, con il Decreto Legislativo 8 novembre 2021, n. 195 (pubblicato in Gazzetta 30 novembre 2021, n. 285), si è voluto dare seguito all'attuazione della Direttiva UE 2018/1673 del Parlamento Europeo e del Consiglio, sulla lotta al riciclaggio mediante il diritto penale, del 23 ottobre 2018. Lo scopo, come si legge al Considerando 3, è quello di allineare la disciplina giuridica europea agli standard internazionali dettati dalle raccomandazioni del GAFI (Gruppo di azione finanziaria internazionale) del 2012 e ai successivi aggiornamenti.

16.1 FATTISPECIE DI REATO RILEVANTI

I reati applicabili e rilevanti per il contesto sono:

- **Ricettazione (art. 648 c.p.)**: Si verifica quando qualcuno acquista, riceve o nasconde beni di provenienza illecita, sebbene non sia implicato nella loro origine illecita. Questo reato è rilevante in caso di beni acquistati indirettamente da fonti non autorizzate.
- **Riciclaggio (art. 648-bis c.p.)**: Si verifica quando vengono compiute operazioni che rendono difficilmente tracciabile la provenienza di beni o fondi illeciti, un rischio presente in transazioni o acquisti non monitorati.
- **Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)**: Rilevante se una struttura impiega fondi o risorse di origine illecita senza conoscere la provenienza illegale.
- **Autoriciclaggio (art. 648-ter.1 c.p.)**: Questo reato si verifica se la stessa struttura tenta di occultare l'origine illecita di fondi attraverso operazioni che ne mascherano la provenienza.

16.2 ATTIVITÀ SENSIBILI

Le attività sensibili per questi reati nella realtà della società sono:

- Pagamenti e incassi per forniture e servizi (compresi bonifici e altri trasferimenti di fondi);
- Rapporti con fornitori e partner sia nazionali che esteri, data la possibile esposizione a soggetti con interessi illeciti;
- Gestione di investimenti e operazioni finanziarie di particolare rilevanza;
- Sponsorizzazioni o altre forme di finanziamento che possono provenire da fonti non trasparenti.

→ Le attività sensibili ai fini dell'autoriciclaggio e relativi controlli

Di seguito sono indicate le attività sensibili riferite ai flussi finanziari astrattamente esposte al rischio di autoriciclaggio.

Tipologia entrata / incasso	Modalità incasso	Riferimenti
Incassi clienti	Bonifico bancario	Contratti

Altre entrate	Bonifico bancario	
Tipologia uscita / pagamento	**Modalità di pagamento**	**Riferimenti**
Fornitori	Bonifico bancario	Contratti
Pagamento per addizionale	Bonifico bancario modello f24	Decreto-legge 350/2003
Assicurazioni	Bonifico bancario	Contratti
Debiti vs amministratori / sindaci	Bonifico bancario	Delibera assembleare
Salari e stipendi dipendenti	Bonifico bancario	Contratti
Tesoreria INPS/Tfr e pensioni	Bonifico bancario	Legislazione sul personale
Irpef a dipendenti	Bonifico bancario modello f24	Legislazione sul personale
Tipologia uscita / pagamento	**Modalità di pagamento**	**Riferimenti**
Spese varie personale	Bonifico bancario	Contratti e accordi
IRAP e IRES a debito	Bonifico bancario modello f24	Leggi fiscali
Altre tasse	Bonifico bancario	Leggi fiscali
Interessi passivi su c/c	Addebito su c/c bancario	Contratto bancario
Commissioni bancarie	Addebito su c/c bancario	Contratto bancario
Commissioni carte credito	Addebito su c/c bancario	Contratto bancario

16.3 REGOLE GENERALI DI COMPORTAMENTO

Nello svolgimento delle attività previste dalla presente procedura, i soggetti coinvolti sono obbligati ad osservare le disposizioni di legge e i regolamenti relativi alle operazioni societarie identificate, nonché i principi contenuti nel Codice Etico e nel Modello Organizzativo.

La presente procedura prevede l'espresso divieto a carico di tutti i destinatari eventualmente coinvolti nei processi sensibili di:

- intrattenere rapporti commerciali con soggetti dei quali sia conosciuta e dimostrata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, del terrorismo e ai traffici illeciti;
- utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
- sostituire o trasferire denaro, beni o altre utilità provenienti da un qualsiasi delitto o compiere qualunque attività che ne agevoli l'acquisto, la ricezione o l'occultamento;
- sostituire o trasferire denaro, beni o altre utilità provenienti da illeciti, ovvero compiere in relazione ad essi altre operazioni che possano ostacolare l'identificazione della provenienza delittuosa;
- partecipare ad uno degli atti di cui ai punti precedenti, associarsi per commetterli, aiutare, istigare o consigliare qualcuno a commetterli o agevolarne l'esecuzione;
- effettuare o ricevere pagamenti su conti cifrati, in contanti se non entro il imiti della normativa antiriciclaggio di volta in volta vigente, tramite assegni bancari che non abbiano la clausola di "non trasferibilità".

Con riferimento ai sopra citati reati, inoltre, la Società ed i destinatari devono ispirare le proprie attività alle seguenti Regole Generali di Comportamento:

1) il processo acquisti deve essere suddiviso in diverse fasi (richiesta di acquisto, ordine di acquisto, fornitura del bene o servizio, fatturazione, pagamento);
2) le diverse fasi del processo acquisti devono essere svolte da soggetti diversi con attribuzione dei rispettivi poteri;
3) gli acquisti di beni e servizi sono soggetti a specifica autorizzazione, anche informatica, con relativa archiviazione cartacea dei documenti;
4) i fornitori sono selezionati sulla base di requisiti di professionalità;
5) la fornitura di beni o di servizi deve essere effettuata a condizioni di mercato;
6) il soggetto che riceve il bene o servizio verifica la congruità tra ordine e la richiesta di acquisto;
7) i pagamenti a favore della Pubblica Amministrazione, enti governativi, anche stranieri, devono essere contabilizzati con specifica evidenza;

8) i trasferimenti di fondi devono essere debitamente autorizzati e documentati.

16.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

Per prevenire e controllare il rischio di coinvolgimento in attività di riciclaggio o utilizzo di fondi di provenienza illecita, la struttura adotta i seguenti protocolli specifici:

- Verifica preliminare di fornitori e partner: Condurre un controllo approfondito sulla reputazione, affidabilità e autorizzazioni di fornitori e partner prima di instaurare rapporti commerciali, con particolare attenzione alle collaborazioni internazionali. La verifica deve includere l'analisi di eventuali precedenti legati a riciclaggio o attività illecite.
- Monitoraggio dei flussi finanziari: Implementare un sistema di monitoraggio continuo e dettagliato di tutte le transazioni finanziarie, sia in entrata che in uscita. Ogni operazione deve essere documentata accuratamente per garantire la piena tracciabilità e trasparenza dei fondi, in linea con le normative vigenti.
- Controllo dei conti bancari e delle transazioni: Garantire che tutte le operazioni di pagamento siano registrate nei sistemi aziendali e pienamente tracciabili, limitando l'utilizzo di contante secondo le soglie previste dalla normativa antiriciclaggio. I conti bancari aziendali devono essere controllati regolarmente per identificare e prevenire operazioni sospette o non autorizzate.
- Formazione continua del personale: Fornire al personale coinvolto nelle operazioni finanziarie una formazione continua e aggiornata sulle normative antiriciclaggio. Tale formazione deve includere linee guida per il riconoscimento di transazioni sospette e istruzioni dettagliate per segnalare tempestivamente eventuali anomalie o attività sospette alle autorità interne competenti.

16.5 SOGGETTI COINVOLTI

I principali soggetti coinvolti nella gestione e prevenzione dei reati di riciclaggio sono:

- **Direzione**: Monitora i flussi di cassa e autorizzano i pagamenti in linea con le normative antiriciclaggio. Deve seguire le procedure definite e segnalare eventuali anomalie.
- **Organismo di Vigilanza (OdV)**: Assicura la conformità al modello organizzativo e riceve segnalazioni di sospette irregolarità.

16.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

I compiti di vigilanza dell'OdV in relazione all'osservanza del modello per quanto concerne i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita sono i seguenti:

a) definire idonee istruzioni sugli atteggiamenti da assumere nell'ambito delle attività "*a rischio*";
b) con riferimento alle attività di cassa, l'OdV provvede a:
   - monitorare l'efficacia delle procedure interne al fine della prevenzione del reato;
   - esaminare le eventuali segnalazioni specifiche provenienti dagli organi di controllo o da qualsiasi dipendente ed effettuare gli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute.

17 REATI IN MATERIA DI MEZZI DI PAGAMENTO DIVERSI DAI CONTANTI

Con il D. Lgs. 8 novembre 2021, n. 184, in attuazione della Direttiva UE 2019/713, è stato introdotto l'art. 25-octies.1 nel D. Lgs. 231/2001, che disciplina i delitti in materia di strumenti di pagamento diversi dai contanti**.** L'obiettivo della normativa è prevenire e sanzionare l'utilizzo fraudolento di strumenti di pagamento, sia materiali che immateriali, per garantire sicurezza e trasparenza nei processi di pagamento e nelle transazioni elettroniche.

17.1 FATTISPECIE DI REATO RILEVANTI

Le principali fattispecie di reato previste dall'art. 25-octies.1 del D. Lgs. 231/2001, e rilevanti per il Modello Organizzativo includono:

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.);

- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici per la commissione di reati relativi agli strumenti di pagamento (art. 493-quater c.p.) [il reato in questione si considera improbabile per la natura e la struttura dell'attività svolta];
- Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.).

Questi reati riguardano in particolare condotte come la falsificazione o l'alterazione di strumenti di pagamento elettronici e l'uso non autorizzato di dispositivi per finalità fraudolente.

17.2 ATTIVITÀ SENSIBILI

A seguito dell'analisi dei processi aziendali specifici della società, sono state individuate le seguenti attività come particolarmente sensibili al rischio di commissione di reati relativi agli strumenti di pagamento diversi dai contanti:

- Gestione dei terminali POS e carte di credito per i pagamenti dei pazienti: include l'uso, la manutenzione e la sicurezza dei terminali di pagamento per garantire transazioni sicure e tracciabili;
- Verifica dei pagamenti elettronici e dei rimborsi: attività che coinvolgono l'uso di software di gestione e controllo delle transazioni, per assicurare che non si verifichino anomalie o usi impropri degli strumenti di pagamento;
- Gestione dei dati contabili e delle informazioni riservate: elaborazione, archiviazione e protezione dei dati relativi ai pagamenti e ai conti paziente;
- Controllo degli accessi al sistema contabile e al gestionale utilizzato per i pazienti: regolamentazione delle autorizzazioni per evitare accessi non autorizzati o manipolazioni fraudolente;
- Cancellazione degli account di utenti non più in organico: assicurare la chiusura degli accessi di ex dipendenti o collaboratori.

17.3 REGOLE GENERALI DI COMPORTAMENTO

Per mitigare il rischio di reati connessi all'utilizzo di strumenti di pagamento elettronici, il personale deve rispettare i seguenti principi:

- Trasparenza e tracciabilità: tutte le transazioni devono essere registrate in modo accurato e tempestivo, con la possibilità di monitorare ogni operazione.
- Autorizzazione e controllo degli accessi: ogni strumento di pagamento e sistema di gestione deve essere accessibile solo al personale autorizzato, tramite credenziali personali e monitorate.
- Protezione dei dati: le informazioni contabili e i dati riservati dei pazienti devono essere protetti in conformità alle normative vigenti (Regolamento UE 2016/679 - GDPR).

17.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

Per una gestione sicura ed efficace delle attività sensibili, il poliambulatorio ha predisposto i seguenti protocolli di prevenzione:

- Verifica delle transazioni: ogni pagamento e rimborso deve essere approvato da almeno due persone, garantendo così un controllo incrociato delle operazioni.
- Controllo dei terminali POS e delle transazioni elettroniche: i terminali devono essere sottoposti a verifiche periodiche per rilevare eventuali manomissioni, e tutte le transazioni devono essere tracciabili e accessibili a verifiche interne.
- Gestione degli accessi: l'accesso ai sistemi di pagamento e al gestionale pazienti è consentito solo al personale autorizzato, con monitoraggio periodico per assicurare il rispetto delle autorizzazioni assegnate.
- Audit periodico e revisione del sistema: un audit interno annuale verifica l'aderenza ai protocolli e aggiorna le misure di sicurezza informatica.

17.5 SOGGETTI COINVOLTI

Nel processo di gestione e prevenzione dei reati connessi agli strumenti di pagamento diversi dai contanti, sono coinvolti i seguenti soggetti:

- **Direzione**: supervisione delle operazioni di pagamento, controllo delle transazioni, gestione dei flussi di cassa e verifica dei rimborsi. Gestione pratica dei pagamenti e dei rimborsi, registrazione delle transazioni
- **Personale di accettazione**: interazione con i pazienti per le operazioni di incasso.
- **Amministratore di sistema**: gestione e monitoraggio dei sistemi informatici, controllo degli accessi ai dati sensibili e supervisione della sicurezza informatica in merito ai terminali POS e ai software utilizzati per la gestione dei pagamenti.
- **Organismo di Vigilanza (OdV)**: verifica della conformità del Modello 231 alle normative, revisione periodica dei protocolli di controllo e ricezione delle segnalazioni su eventuali anomalie.
- **Personale Autorizzato**: tutti i dipendenti che, in virtù del loro ruolo, hanno accesso ai sistemi di pagamento, sempre nel rispetto delle procedure di sicurezza e tracciabilità previste.

17.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

L'Organismo di Vigilanza deve ricevere report annuali, o essere immediatamente informato in caso di anomalie o sospetti di violazione, contenenti:

- Un riepilogo delle transazioni elettroniche effettuate;
- Eventuali incidenti o sospetti di uso improprio degli strumenti di pagamento;
- Esiti degli audit e dei controlli interni sulle operazioni finanziarie.

17.7 CONCLUSIONI

La società si impegna a garantire la sicurezza e la trasparenza nelle operazioni finanziarie e nell'utilizzo degli strumenti di pagamento elettronico, attraverso una costante verifica dei processi e dei protocolli di controllo. Queste misure preventive consentono di tutelare il laboratorio da potenziali rischi di frode, garantendo il rispetto della normativa vigente e la protezione degli utenti e dei dati sensibili.

18 REATI INFORMATICI

I reati informatici, secondo quanto previsto dall'art. 24-bis del D.lgs. 231/2001, presuppongono l'uso di strumenti software e hardware per la gestione di dati aziendali e l'accesso alla rete. Per una struttura sanitaria privata autorizzata, la tutela dei dati sanitari e contabili riveste particolare importanza, soprattutto rispetto a rischi di accesso abusivo, danneggiamento di dati e programmi, o diffusione di malware. Con il Decreto 28 giugno 2024, n. 91, sono state introdotte modifiche che ampliano le fattispecie di reato informatico e rafforzano la tutela contro attacchi che possono compromettere la sicurezza e la riservatezza dei dati, specialmente in contesti che gestiscono informazioni sensibili come quelle sanitarie.

18.1 FATTISPECIE DI REATO RILEVANTI

Nel contesto della società, le seguenti fattispecie di reato sono considerate rilevanti:

- Documenti informatici (art. 491-bis c.p.).
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.);
- Detenzione, diffusione e installazione abusiva di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615-quinquies c.p. - modificato da art.19 Legge 23 dicembre 2021, n. 238);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.- modificato da art. 19 Legge 23 dicembre 2021, n. 238)
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617quinquies c.p.- modificato da art. 19 Legge 23 dicembre 2021, n. 238);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis);
- Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.).

18.2 ATTIVITÀ SENSIBILI

In base all'analisi dei processi aziendali, le seguenti attività sensibili presentano un rischio di commissione per le fattispecie di reato sopra indicate:

- Creazione e gestione degli account di accesso ai sistemi aziendali: gestione delle credenziali di accesso con particolare attenzione ai sistemi contenenti dati sanitari e amministrativi.
- Assegnazione e gestione delle password: definizione di regole per la custodia, l'aggiornamento periodico e la sicurezza delle credenziali di accesso.
- Gestione e protezione dei dispositivi aziendali (PC, tablet, ecc.): dispositivi utilizzati per la gestione dei dati sanitari e contabili devono essere protetti da programmi antivirus e firewall aggiornati.
- Controllo degli accessi alla rete aziendale e autorizzazione per accessi remoti: monitoraggio degli accessi alla rete interna e gestione delle autorizzazioni per il lavoro da remoto, limitato ai soli dipendenti autorizzati.
- Sicurezza informatica e gestione del disaster recovery: attività di backup e ripristino dei dati sensibili per garantire la continuità operativa in caso di malfunzionamenti o attacchi informatici.
- Comunicazioni telematiche con la Pubblica Amministrazione e altre strutture sanitarie: gestione sicura dei dati e dei documenti sanitari trasmessi tramite canali informatici.
- Formazione del personale: formazione periodica per garantire la conoscenza delle regole di sicurezza e di protezione dei dati personali e sanitari, in linea con il GDPR.

18.3 REGOLE GENERALI DI COMPORTAMENTO

Il personale della società è tenuto a rispettare le seguenti regole generali di comportamento per prevenire i reati informatici:

1. Utilizzare le informazioni, le applicazioni e le apparecchiature aziendali esclusivamente per finalità aziendali e nel rispetto della normativa sulla sicurezza dei dati.
2. Installare software solo se autorizzato dalla Direzione, assicurandosi che sia conforme agli standard di sicurezza.
3. Non eludere i sistemi di protezione e sicurezza dei sistemi informatici aziendali.
4. Non accedere a sistemi informatici di terzi né alterare dati senza autorizzazione.
5. Custodire con riservatezza le credenziali di accesso (username e password) e non condividerle con altri dipendenti.
6. Utilizzare password robuste e modificarle periodicamente per garantire la sicurezza degli account.
7. Attivare il blocco automatico dei dispositivi aziendali in caso di inattività prolungata.
8. Segnalare immediatamente alla Direzione eventuali incidenti informatici o tentativi di accesso non autorizzato.
9. Trasferire all'esterno della struttura solo i file e i documenti autorizzati, previa verifica delle finalità aziendali.

18.4 PROTOCOLLI DI PREVENZIONE E CONTROLLO

Per garantire una gestione sicura delle attività sensibili, la società ha adottato i seguenti protocolli di prevenzione:

- Gestione degli accessi: vengono assegnate credenziali uniche a ciascun dipendente autorizzato, con monitoraggi periodici per prevenire accessi non autorizzati.
- Monitoraggio dei dati e delle transazioni: verifiche periodiche sui flussi di dati sanitari e contabili, con particolare attenzione a quelli scambiati con la Pubblica Amministrazione.
- Aggiornamento e protezione dei software aziendali: dispositivi aziendali aggiornati periodicamente per garantire protezione da minacce informatiche.
- Audit periodici sugli accessi: controlli regolari sugli accessi ai dati sensibili e ai sistemi aziendali per garantire la conformità al Modello 231 e al GDPR.

18.5 SOGGETTI COINVOLTI NEL PROCESSO

Nel processo di prevenzione dei reati informatici, i seguenti soggetti hanno responsabilità specifiche:

- **Amministratore di sistema:** gestisce la sicurezza dei sistemi informatici, sovraintende all'installazione di software e monitora gli accessi da remoto.
- **Direzione**: gestisce i dati contabili e sanitari nei sistemi aziendali, garantendo la protezione e il rispetto delle regole interne.
- **Dpo**: verifica che tutte le operazioni di trattamento dati siano conformi al GDPR e alle normative di protezione dati aziendali.
- **Organismo di Vigilanza (OdV)**: assicura l'efficacia del Modello 231 e monitora il rispetto dei protocolli di sicurezza, ricevendo segnalazioni di possibili violazioni.
- **Personale Autorizzato**: i dipendenti con accesso ai dati e ai sistemi informatici sono tenuti a seguire rigorosamente le regole e i protocolli aziendali.

18.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

L'Organismo di Vigilanza riceve report periodici su:

- Segnalazioni di incidenti informatici o tentativi di accesso non autorizzato;
- Modifiche rilevanti ai protocolli di sicurezza;
- Esiti degli audit interni sui sistemi informatici e sui dati sensibili.

18.7 CONCLUSIONI

La società si impegna a garantire la sicurezza dei propri sistemi informatici e la protezione delle informazioni aziendali attraverso l'adozione di protocolli di prevenzione e la formazione del personale. Questo approccio minimizza il rischio di reati informatici, tutelando la riservatezza e la continuità delle operazioni aziendali.

19 DELITTI DI CRIMINALITÀ ORGANIZZATA

I reati di criminalità organizzata, previsti dall'art. 24-ter del D.lgs. n. 231/2001, si configurano in contesti dove vi siano condotte volte alla promozione, costituzione, organizzazione o partecipazione ad associazioni criminali con finalità illecite. In una struttura privata autorizzata, pur trattandosi di una realtà sanitaria con rischi ridotti rispetto a settori più esposti, esistono aree in cui è necessario adottare controlli per prevenire potenziali infiltrazioni o influenze illecite, soprattutto nei rapporti con fornitori, consulenti e altri enti.

19.1 FATTISPECIE DI REATO RILEVANTI

Le seguenti fattispecie di reato, previste dal Codice penale e rilevanti ai fini del D.lgs. 231/2001, sono considerate astrattamente applicabili nel contesto della società:

- **Associazione per delinquere** (art. 416 c.p.): reato che punisce la promozione, costituzione, organizzazione o partecipazione ad associazioni criminali, con l'obiettivo di compiere attività illecite, tra cui il condizionamento di rapporti commerciali e l'ottenimento di vantaggi indebiti.
- **Associazione di tipo mafioso anche straniero** (art. 416-bis c.p.): punisce l'appartenenza a organizzazioni di tipo mafioso che utilizzano intimidazione e corruzione per influenzare attività economiche, inclusi i rapporti con fornitori o enti pubblici.

Queste fattispecie, sebbene poco ipotizzabili, richiedono un'attenta gestione dei rapporti con terzi e la verifica dell'onorabilità delle controparti.

19.2 ATTIVITÀ SENSIBILI

Attraverso l'analisi dei Processi della Società, così come descritta nella Parte Generale, sono state individuate le seguenti Attività Sensibili, nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 24 - ter del D.lgs. n. 231/2001:

- Selezione e gestione dei rapporti con collaboratori, consulenti e fornitori: garantire l'affidabilità delle controparti è fondamentale per prevenire eventuali legami con organizzazioni criminali. Tale rischio può riguardare in particolare l'approvvigionamento di beni e servizi sanitari e consulenze specialistiche.
- Gestione delle risorse finanziarie e delle transazioni: assicurare trasparenza e tracciabilità delle transazioni finanziarie riduce il rischio di coinvolgimento in attività illecite. Sebbene le operazioni siano prevalentemente ordinarie, la tracciabilità delle transazioni è cruciale.

- Rapporti con enti pubblici: i rapporti con enti pubblici per pratiche di accreditamento o per il rinnovo di autorizzazioni potrebbero teoricamente essere oggetto di tentativi di condizionamento o pressioni illecite.

19.3 REGOLE GENERALI DI COMPORTAMENTO

Con riferimento ai Reati di criminalità organizzata la Società ed i Destinatari devono ispirare le proprie attività alle seguenti Regole Generali di Comportamento:
La società ha adottato i seguenti protocolli di prevenzione e controllo per limitare il rischio di coinvolgimento in attività legate alla criminalità organizzata:

- Verifica preliminare dell'onorabilità delle controparti: svolgere controlli preventivi su fornitori, consulenti e collaboratori per garantire l'assenza di legami con associazioni criminali.
- Monitoraggio delle transazioni finanziarie: assicurarsi che le transazioni siano tracciabili, giustificate e conformi agli standard etici e legali, per ridurre il rischio di attività sospette.
- Documentazione dei rapporti con terzi: formalizzare ogni contratto o convenzione con terzi, includendo clausole di rispetto delle normative anticriminalità.
- Controllo delle sponsorizzazioni e liberalità: prevedere una procedura di approvazione per ogni richiesta di sponsorizzazione o donazione, garantendo trasparenza e finalità lecita.

19.4 SOGGETTI COINVOLTI

Nel processo di prevenzione dei reati di criminalità organizzata sono coinvolti i seguenti soggetti:

- **Direzione**: si occupa della gestione delle risorse finanziarie, monitorando le transazioni e i rapporti con i fornitori per garantire la conformità ai protocolli aziendali. Inoltre, gestisce la selezione e la verifica dei fornitori, con particolare attenzione ai criteri di onorabilità e affidabilità.
- **Organismo di Vigilanza (OdV)**: monitora il rispetto dei protocolli e verifica l'adeguatezza del Modello 231, ricevendo segnalazioni su possibili violazioni.
- **Personale Autorizzato**: tutto il personale coinvolto nella gestione di rapporti con terzi deve attenersi ai protocolli, rispettando i principi etici stabiliti dalla società.

19.5 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza riceve report periodici contenenti:

- Segnalazioni di anomalie nei rapporti con terzi;
- Modifiche ai protocolli di gestione di fornitori e consulenti, se necessario;
- Esiti degli audit e delle verifiche sull'onorabilità e affidabilità delle controparti.

19.6 CONCLUSIONI

La società adotta un approccio preventivo nella gestione dei rapporti con fornitori, consulenti e altre controparti, minimizzando il rischio di infiltrazioni o influenze illecite da parte di organizzazioni criminali. Questi protocolli, specifici e proporzionati al contesto, assicurano la conformità alla normativa e la protezione dell'integrità della struttura sanitaria.

20 DELITTI CON FINALITA' DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO

I reati con finalità di terrorismo o di eversione dell'ordine democratico, previsti dall'art. 25-quater del D.Lgs. n. 231/2001, si configurano quando le azioni sono volte a generare terrore nella collettività o a sovvertire l'ordine costituzionale dello Stato. Sebbene nella realtà del Centro il rischio di commissione di questi reati sia estremamente remoto, sono comunque previsti controlli su specifiche aree per ridurre ogni possibilità di coinvolgimento involontario in attività illecite, specialmente nei rapporti con consulenti, fornitori e nelle transazioni internazionali.

20.1 FATTISPECIE DI REATO RILEVANTI

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili, ai sensi dell'art. 25 - quater del D.lgs. n. 231/2001, si rinvia all'Allegato n. 1 e si elencano qui di seguito i Reati ritenuti rilevanti:

Associazioni con finalità di terrorismo o di eversione dell'ordine democratico (art. 270-bis c.p.): punisce la partecipazione a gruppi o associazioni aventi come scopo il compimento di atti terroristici. È rilevante in contesti con rapporti esterni non verificati adeguatamente, che potrebbero nascondere collegamenti con attività sospette.

Finanziamento del terrorismo (art. 270-quinquies c.p.): questo reato colpisce chi finanzia o fornisce risorse per sostenere organizzazioni con scopi terroristici. È ipotizzabile, sebbene in modo residuale, nelle transazioni non tracciabili o poco trasparenti.

20.2 ATTIVITÀ SENSIBILI

Attraverso l'analisi dei Processi della Società, così come descritta nella Parte Generale, sono state individuate le seguenti Attività Sensibili, nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25 - quater del D.lgs. n. 231/2001:

- Selezione e gestione dei rapporti con fornitori e consulenti: la scelta di fornitori e consulenti, soprattutto se esteri, richiede una verifica della loro affidabilità per evitare che siano, anche indirettamente, collegati a organizzazioni sospette.
- Gestione delle risorse finanziarie e delle transazioni: ogni operazione finanziaria deve essere tracciabile e documentata, evitando transazioni sospette o non giustificate, al fine di ridurre ogni rischio di finanziamento indiretto di attività illecite.
- Gestione delle donazioni, sponsorizzazioni e liberalità: verificare che donazioni e sponsorizzazioni siano trasparenti e rispettino tutte le normative, per evitare che fondi aziendali siano destinati a organizzazioni sospette.

20.3 REGOLE GENERALI DI COMPORTAMENTO

Per prevenire il rischio di reati con finalità di terrorismo o eversione, la società e i destinatari del Modello Organizzativo devono rispettare le seguenti regole generali di comportamento:

1. Non ostacolare in alcun modo eventuali verifiche o indagini interne o esterne volte a rilevare e contrastare comportamenti illeciti.
2. Redigere ogni contratto e convenzione con terzi (es. consulenti, fornitori, partner) in forma scritta, includendo clausole che richiedano il rispetto del D.lgs. 231/2001 e delle normative antiterrorismo applicabili.
3. Astenersi da ogni rapporto, diretto o indiretto, con soggetti che possano essere collegati a organizzazioni con finalità terroristiche o eversive.
4. Realizzare tutte le transazioni finanziarie in modo documentato e tracciabile, giustificando ogni spesa e registrando i trasferimenti di fondi.
5. Evitare rapporti con clienti, fornitori o partner che perseguano, anche indirettamente, finalità illecite.
6. Prima di intraprendere rapporti commerciali con soggetti di Paesi a rischio, effettuare verifiche preventive sull'affidabilità e sui requisiti di sicurezza.

20.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

La società adotta i seguenti protocolli di prevenzione e controllo per ridurre il rischio di collegamento, anche involontario, con attività con finalità terroristiche o eversive:

- Verifica dell'onorabilità delle controparti: prima di instaurare rapporti con fornitori, consulenti o partner, si effettuano controlli documentati per garantire che non abbiano legami con attività o organizzazioni sospette.
- Monitoraggio delle transazioni finanziarie: tutte le transazioni devono essere giustificate e tracciabili, con verifiche periodiche per rilevare eventuali anomalie.
- Controllo di donazioni, liberalità e sponsorizzazioni: le donazioni o sponsorizzazioni devono essere documentate, giustificate e approvate per evitare collegamenti con organizzazioni sospette.

20.5 SOGGETTI COINVOLTI

I principali soggetti coinvolti nella prevenzione dei reati con finalità di terrorismo o eversione sono:

- **Direzione**: sovrintende alla gestione dei fondi aziendali, assicurando che tutte le risorse siano tracciabili e destinate a fini giustificati. Si occupa della selezione dei fornitori e dei consulenti, verificando l'affidabilità delle controparti.
- **Organismo di Vigilanza (OdV)**: monitora l'efficacia del Modello 231 e verifica il rispetto dei protocolli adottati, ricevendo segnalazioni di possibili violazioni.
- **Personale Autorizzato**: tutto il personale che ha rapporti con controparti esterne è tenuto a seguire le regole di comportamento e i protocolli aziendali.

20.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza riceve report periodici contenenti:

- Segnalazioni di eventuali anomalie rilevate nelle transazioni finanziarie o nei rapporti con controparti esterne;
- Proposte di aggiornamento dei protocolli in base all'analisi dei rischi;
- Esiti delle verifiche sulla reputazione e affidabilità delle controparti esterne

20.7 CONCLUSIONI

La società adotta misure preventive specifiche per evitare qualsiasi legame, anche indiretto, con attività terroristiche o eversive. La gestione rigorosa delle transazioni finanziarie e la selezione accurata delle controparti esterne riducono al minimo il rischio di collegamento con attività illecite, assicurando la conformità normativa e la protezione dell'integrità aziendale.

21 INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORISÀ GIUDIZIARIA - ART. 25 DECIES

La presente Parte Speciale si applica alla tipologia di reato identificato dall'art. 25-decies del Decreto e segnatamente l'art. 377-bis c.p.

21.1 FATTISPECIE DI REATO RILEVANTI

La Legge 3 agosto 2009, n. 116, recante "Ratifica ed esecuzione della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione" adottata dall'Assemblea Generale dell'ONU il 31 ottobre 2003, ha introdotto la responsabilità amministrativa degli enti per il reato di cui all'art. 377-bis c.p. "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria" (art. 25-decies del Decreto 231).

Il reato considerato potenzialmente realizzabile è il seguente:

- **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 377-bis c.p.)**: punisce chi, mediante violenza o minaccia, o con l'offerta o la promessa di danaro o altra utilità, induce un soggetto a non rendere dichiarazioni o a rendere dichiarazioni false utilizzabili in un procedimento penale, quando tale soggetto ha la facoltà di non rispondere.

21.2 ATTIVITÀ SENSIBILI

Le seguenti attività sono state individuate come particolarmente sensibili al rischio di commissione del reato di cui all'art. 25-decies:

- Gestione di contenziosi giudiziali, stragiudiziali e procedimenti arbitrali: comprende tutte le attività connesse alla preparazione, partecipazione e gestione dei contenziosi in ambito civile, penale e amministrativo, inclusa la raccolta e gestione delle informazioni rilevanti.

- Rapporti con l'Autorità Giudiziaria e consulenti legali: include la gestione dei contatti diretti o indiretti con Giudici, Consulenti tecnici e ausiliari nell'ambito dei procedimenti giudiziari, con particolare attenzione alla nomina e alla gestione delle relazioni con i legali e i Consulenti tecnici e di parte.
- Preparazione e gestione delle testimonianze: riguarda l'organizzazione e il supporto alla preparazione di testimonianze da parte di dipendenti o collaboratori coinvolti in procedimenti giudiziari, assicurando che le dichiarazioni siano rese in modo conforme ai principi di verità e trasparenza.
- Redazione e revisione di documentazione legale: implica l'elaborazione di documenti e la loro presentazione agli organi giudiziari, prestando particolare attenzione alla veridicità e alla correttezza delle informazioni contenute.

21.3 PRINCIPI GENERALI DI COMPORTAMENTO

Per evitare il verificarsi dei reati previsti dal D.lgs. 231/2001, è fatto divieto a tutti i Destinatari di:

1. Indurre un soggetto a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria mediante minaccia o violenza al fine di occultare fatti che possano arrecare un danno alla Società.
2. Ricorrere alla forza fisica, minacce o intimidazioni o promettere, offrire o concedere indebite utilità per ottenere dichiarazioni false.
3. Riconoscere liberalità o altre utilità a dipendenti o terzi coinvolti in procedimenti penali per influenzarne le dichiarazioni.

I Destinatari del Modello sono tenuti a:

- Condurre la propria attività con legalità, trasparenza e collaborazione nei rapporti con l'Autorità Giudiziaria.
- Agevolare i controlli e le indagini da parte delle autorità sulle attività aziendali.
- Rendere dichiarazioni veritiere e complete nei rapporti con l'Autorità Giudiziaria.
- Avvertire tempestivamente il proprio Responsabile in caso di citazione a testimoniare o coinvolgimento in un procedimento penale.

21.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

La società adotta i seguenti protocolli per prevenire il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci:

- Identificazione formale dei soggetti autorizzati a rappresentare la Società nei rapporti con l'Autorità Giudiziaria.
- Fornitura di informazioni chiare e complete ai legali scelti dalla società per garantire la verità dei fatti.
- Flussi di reporting alla Direzione su eventi giudiziari rilevanti e procedure in corso.
- Rispetto rigoroso delle procedure aziendali e dei livelli autorizzativi per ogni transazione e azione legale.
- Selezione accurata di legali e consulenti basata su competenze documentate e criteri di serietà e competenza.
- Clausole contrattuali specifiche che richiedono il rispetto del Modello Organizzativo e del Codice Etico.
- Monitoraggio e rendicontazione dei compensi dei legali incaricati, con una chiara documentazione dell'attività svolta.

21.5 SOGGETTI COINVOLTI

I principali soggetti coinvolti nella prevenzione del reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci sono:

- **Direzione**
- **Organismo di Vigilanza (OdV)**: monitora il rispetto dei protocolli e verifica la conformità al Modello 231.
- **Personale interessato**: segue le regole di comportamento e i protocolli aziendali.

21.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

L'Organismo di Vigilanza riceve report periodici contenenti:

- Segnalazioni di eventi giudiziari rilevanti**.**

- Esiti delle verifiche e degli audit condotti sulle procedure aziendali.
- Modifiche rilevanti ai protocolli adottati**.**

21.7 CONCLUSIONI

La società adotta misure preventive mirate a evitare qualsiasi condotta che possa configurare il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci. Il rispetto dei protocolli e delle regole aziendali garantisce la conformità alla normativa vigente e preserva l'integrità della struttura aziendale.

22 REATI C.D. TRANSNAZIONALI

Con la L. 16 marzo 2006, n. 146, è stata data attuazione alla Convenzione delle Nazioni Unite contro la criminalità organizzata e ai relativi Protocolli Addizionali, mediante un meccanismo di introduzione automatica nell'ordinamento nazionale. Il fulcro del provvedimento legislativo è l'art. 3, che definisce la nozione di reato transnazionale, individuando come elemento costitutivo il coinvolgimento di un gruppo criminale organizzato, senza specificarne i requisiti. L'art. 2 della Convenzione definisce il gruppo criminale organizzato come "un gruppo strutturato, esistente per un periodo di tempo, composto da tre o più persone che agiscono di concerto al fine di commettere uno o più reati gravi al fine di ottenere, direttamente o indirettamente, un vantaggio finanziario o materiale".

22.1 FATTISPECIE DI REATO RILEVANTI

Nell'ottica transnazionale, acquisiscono rilevanza i seguenti delitti, come espressamente previsti:

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso anche straniera (art. 416-bis c.p.);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater DPR 23 gennaio 1973, n. 43);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 9 ottobre 1990, n. 309);
- Disposizioni contro le immigrazioni clandestine (art. 12 D.lgs. 25 luglio 1998, n. 286);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 377-bis c.p.);
- Favoreggiamento (art. 378 c.p.).

22.2 ATTIVITA' SENSIBILI

L'analisi dei processi aziendali ha permesso di individuare le seguenti attività sensibili, in cui potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dalla L. 146/2006, applicabili ai fini del D.lgs. 231/2001:

- Selezione e assunzione del personale: le procedure di selezione e assunzione devono essere trasparenti e conformi alle normative, per prevenire l'infiltrazione di soggetti legati a gruppi criminali organizzati.
- Gestione del personale: monitoraggio delle condizioni lavorative per garantire la conformità alle leggi, prevenendo possibili connessioni con attività illecite.
- Gestione del processo acquisti: controllo rigoroso sui fornitori, specialmente quelli esteri, per accertare l'assenza di legami con gruppi criminali.
- Rapporti con società estere: verifiche sulla trasparenza delle operazioni di fatturazione e fornitura di servizi per evitare il coinvolgimento in attività transnazionali sospette.
- Rapporti con enti pubblici nazionali e stranieri: gestione delle interazioni con enti, prestando attenzione alle consulenze e ai contratti per evitare compromissioni con attività criminali.
- Gestione del contenzioso: monitoraggio delle dispute legali per garantire che le operazioni siano condotte in modo lecito e trasparente.

22.3 PRINCIPI GENERALI DI COMPORTAMENTO

Per prevenire i reati transnazionali, la società e i suoi dipendenti devono:

1. Operare nel rispetto delle normative nazionali e internazionali.
2. Evitare qualsiasi coinvolgimento con soggetti o entità sospettati di attività illecite.
3. Mantenere alta la trasparenza e la tracciabilità in tutte le operazioni internazionali.
4. Segnalare tempestivamente eventuali comportamenti sospetti o situazioni che possano indicare il rischio di reati transnazionali.
5. Collaborare pienamente con le autorità competenti in caso di indagini o richieste di informazioni.

22.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

La società adotta protocolli per ridurre al minimo il rischio di coinvolgimento in reati transnazionali:

- Verifica preventiva e periodica dei fornitori e partner: controlli di due diligence per accertare l'affidabilità e l'assenza di legami con gruppi criminali.
- Procedure di controllo sui flussi finanziari: monitoraggio delle transazioni internazionali per prevenire operazioni sospette.
- Sistemi di controllo sulla documentazione contrattuale: i contratti con fornitori e consulenti devono includere clausole che impongano il rispetto del Modello 231.
- Audit regolari e reporting: audit periodici per monitorare la conformità ai protocolli e identificare possibili rischi.
- Formazione continua del personale: corsi di aggiornamento sui rischi di reati transnazionali e sulle procedure di prevenzione.

22.5 SOGGETTI COINVOLTI

I seguenti soggetti sono coinvolti nella prevenzione dei reati transnazionali:

- **Direzione**: supervisiona la gestione dei fondi e i rapporti con partner esteri. Garantisce la conformità dei fornitori ai protocolli aziendali.
- **Organismo di Vigilanza (OdV)**: monitora l'attuazione dei protocolli e riceve segnalazioni di possibili violazioni.
- **Personale Autorizzato**: segue le direttive aziendali e rispetta le procedure di controllo.

22.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

L'Organismo di Vigilanza riceve report periodici su:

- Eventuali anomalie riscontrate nei rapporti con partner esteri.
- Modifiche e aggiornamenti ai protocolli.
- Esiti degli audit e delle verifiche sui flussi finanziari e sulle attività sensibili.

22.7 CONCLUSIONI

La società adotta un approccio rigoroso per prevenire e monitorare i reati transnazionali, implementando protocolli specifici e promuovendo una cultura della legalità e della trasparenza. Queste misure garantiscono la conformità normativa e la protezione dell'integrità aziendale.

23 IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del D.lgs. 231/2001 è collegato il regime di responsabilità a carico della Società, è fondamentale per la prevenzione dei reati stessi e per l'intero sistema di controllo previsto dal Decreto. Di seguito, si fornisce una descrizione dettagliata del reato richiamato dall'art. 25-duodecies in tema di impiego di cittadini di paesi terzi il cui soggiorno è irregolare.

23.1 FATTISPECIE DI REATO RILEVANTI

Realizza il reato di cui all'art. 22, co. 12-bis, D.lgs. 25 luglio 1998, n. 286, il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, o con permesso scaduto e non rinnovato, revocato o annullato. La responsabilità dell'ente si configura nelle seguenti circostanze:

- Numero di lavoratori: quando i lavoratori occupati senza permesso di soggiorno sono più di tre.
- Minori in età non lavorativa: se i lavoratori sono minori al di sotto dell'età legale per il lavoro.
- Condizioni di sfruttamento: se i lavoratori sono impiegati in condizioni lavorative di particolare sfruttamento, come definito dal terzo comma dell'art. 603-bis del Codice penale.

23.2 ATTIVITA' SENSIBILI

Le seguenti attività aziendali sono state identificate come sensibili ai fini del D.lgs. 231/2001:

- Assunzione e impiego di cittadini di paesi terzi: comprende le procedure di selezione, verifica dei documenti e assunzione di lavoratori stranieri. Questo include il controllo dei permessi di soggiorno e la conformità alle normative sull'immigrazione.
- Verifica e monitoraggio delle condizioni lavorative: attività di supervisione per garantire che le condizioni lavorative rispettino le normative vigenti e prevenire situazioni di sfruttamento.
- Gestione dei contratti e della documentazione: controllo dei contratti di lavoro e della documentazione relativa, per assicurare che tutti i lavoratori siano regolarmente registrati e in possesso delle autorizzazioni necessarie.
- Interazione con le autorità e gli enti pubblici: gestione dei rapporti con gli enti preposti alle verifiche e agli adempimenti legali relativi all'impiego di cittadini stranieri.

23.3 PRINCIPI GENERALI DI COMPORTAMENTO

Per evitare la commissione dei reati richiamati dall'art. 25-duodecies del D.lgs. 231/2001, la società e i suoi dipendenti devono:

1. Garantire la verifica e la validità dei documenti dei lavoratori stranieri, controllando che i permessi di soggiorno siano validi e conformi alla legge.
2. Evitare l'impiego di lavoratori senza i requisiti legali richiesti.
3. Assicurare trasparenza e regolarità nelle procedure di assunzione e impiego.
4. Segnalare eventuali irregolarità o anomalie rilevate durante il processo di assunzione e gestione del personale.
5. Mantenere registri accurati e aggiornati riguardanti lo status legale dei lavoratori.

23.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

La società ha adottato i seguenti protocolli per prevenire il reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare:

- Procedure di verifica documentale: ogni assunzione è soggetta a un controllo rigoroso dei documenti di identità e dei permessi di soggiorno, con archiviazione delle copie nei registri aziendali.
- Monitoraggio periodico della conformità: controlli regolari per accertare che i permessi di soggiorno non siano scaduti e siano stati rinnovati entro i termini di legge.
- Audit interni: esecuzione di audit periodici per verificare il rispetto delle normative e l'efficacia delle procedure di controllo.

- Collaborazione con enti esterni: rapporti con consulenti legali e agenzie di verifica per assicurare la regolarità delle assunzioni e degli impieghi.

23.5 SOGGETTI COINVOLTI

I principali soggetti coinvolti nella prevenzione del reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare includono:

- **Direzione**: supervisiona l'assunzione e la verifica dei documenti dei lavoratori. Assicura la conformità dei processi di gestione del personale e l'archiviazione corretta della documentazione. deve rispettare le procedure aziendali e mantenere la conformità alle normative sull'immigrazione.
- **Organismo di Vigilanza (OdV)**: monitora il rispetto dei protocolli e riceve segnalazioni di eventuali violazioni.

23.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

L'Organismo di Vigilanza riceve report periodici contenenti:

- Segnalazioni di eventuali irregolarità riscontrate nei processi di assunzione e impiego.
- Esiti degli audit e delle verifiche periodiche.
- Modifiche ai protocolli in risposta a nuovi requisiti normativi o esigenze aziendali.

23.7 CONCLUSIONI

La società adotta un approccio proattivo nella gestione dell'impiego di cittadini di paesi terzi, implementando controlli e protocolli per garantire la conformità alle normative vigenti e prevenire rischi di violazioni legate all'assunzione di lavoratori stranieri in situazione irregolare. Questo approccio contribuisce a tutelare l'integrità aziendale e la conformità al D.lgs. 231/2001.

24 RAZZISMO E XENOFOBIA

Le fattispecie di reato richiamate dal D.lgs. 231/2001 sono rilevanti per la comprensione e la prevenzione dei reati, connessi alla responsabilità della Società ai sensi dell'art. 5 del Decreto. Una chiara conoscenza delle modalità realizzative e strutturali di tali reati contribuisce all'efficacia del sistema di controllo previsto dal Decreto stesso.

24.1 FATTISPECIE DI REATO APPLICABILI

Il reato di cui all'art. 604-bis c.p. (Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa) si configura quando:

- Propaganda di idee basate sulla superiorità o sull'odio razziale o etnico: include la promozione di teorie discriminatorie o razziste.
- Istigazione o commissione di atti di discriminazione per motivi razziali, etnici, nazionali o religiosi.
- Istigazione o commissione di violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi.
- Partecipazione a organizzazioni o gruppi che abbiano come scopo l'incitamento alla discriminazione o alla violenza.

24.2 ATTIVITÀ SENSIBILI

Le seguenti attività aziendali sono state individuate come sensibili ai fini del D.lgs. 231/2001 per il rischio di commissione dei reati di razzismo e xenofobia, tenendo conto delle specificità di una struttura sanitaria:

- Gestione dei rapporti interpersonali tra dipendenti e con i pazienti: monitoraggio e gestione delle interazioni quotidiane per prevenire comportamenti discriminatori o contrari ai principi etici della struttura.
- Comunicazione interna ed esterna: supervisione dei messaggi e delle comunicazioni ufficiali, inclusi i documenti medici e informativi, per garantire che siano privi di contenuti discriminatori.
- Accoglienza e trattamento dei pazienti: assicurare che le procedure di ammissione e le cure fornite siano erogate senza pregiudizi o discriminazioni basate sull'origine etnica, razziale o religiosa.

- Selezione e gestione del personale: adozione di pratiche di selezione e assunzione che garantiscano equità e assenza di discriminazioni, con particolare attenzione al background culturale e alle pari opportunità.

24.3 PRINCIPI GENERALI DI COMPORTAMENTO

Per prevenire la commissione dei reati di razzismo e xenofobia, la società e i suoi dipendenti devono:

1. Promuovere un ambiente di lavoro inclusivo e rispettoso, privo di qualsiasi forma di discriminazione, tenendo conto della diversità culturale e religiosa dei pazienti.
2. Evitare qualsiasi atto o comunicazione che possa incitare all'odio razziale, etnico, nazionale o religioso.
3. Rispettare e valorizzare la diversità in tutte le attività aziendali e relazioni esterne, inclusi i trattamenti medici e l'interazione con i pazienti.
4. Segnalare immediatamente eventuali episodi di discriminazione o comportamenti sospetti, anche se riguardano interazioni con pazienti o terze parti.
5. Attenersi alle linee guida contenute nel Codice Etico aziendale e nel Protocollo di gestione dei rapporti con soggetti terzi, con particolare attenzione alle normative aggiornate.

24.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

La società ha adottato i seguenti protocolli per prevenire i reati di razzismo e xenofobia, con particolare enfasi sul contesto sanitario:

- Procedure di segnalazione interna e protezione dei whistleblower: istituzione di canali riservati per consentire la segnalazione di episodi discriminatori, garantendo la tutela dell'identità del segnalante.
- Controlli sulla comunicazione aziendale: revisione e approvazione preventiva dei contenuti pubblicati o diffusi dalla società per assicurare la conformità alle normative vigenti e ai principi aziendali di inclusività.
- Formazione periodica obbligatoria: programmi formativi specifici per il personale medico e amministrativo, incentrati sulla gestione delle differenze culturali e sul rispetto dei diritti umani.
- Verifiche sui processi di selezione e gestione del personale: criteri trasparenti e pratiche che garantiscono assenza di discriminazioni, anche nell'assegnazione dei ruoli e nella gestione delle promozioni.
- Audit interni regolari: verifiche periodiche per valutare l'aderenza ai protocolli e l'efficacia delle misure adottate, con focus su interazioni e trattamenti verso i pazienti.
-

24.5 SOGGETTI COINVOLTI

I principali soggetti coinvolti nella prevenzione del reato di razzismo e xenofobia sono:

- **Direzione**: supervisiona la gestione dei rapporti interni e l'implementazione delle pratiche di inclusione e rispetto.
- **Organismo di Vigilanza (OdV)**: monitora l'efficacia dei protocolli, riceve segnalazioni di potenziali violazioni e garantisce l'aggiornamento delle misure preventive.
- **Dipendenti, personale medico e collaboratori**: devono agire in conformità con le politiche aziendali, promuovendo un ambiente inclusivo e rispettoso delle diversità.

24.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

L'Organismo di Vigilanza riceve report periodici contenenti:

- Segnalazioni di episodi di discriminazione o comportamenti non conformi alle politiche aziendali, anche durante le interazioni con i pazienti.
- Esiti degli audit interni e delle verifiche sui processi di comunicazione, gestione del personale e trattamento dei pazienti.
- Modifiche o aggiornamenti ai protocolli per migliorare le procedure di controllo e prevenzione in base a nuove normative o esigenze specifiche.

24.7 CONCLUSIONI

La società adotta un approccio preventivo per contrastare i reati di razzismo e xenofobia, implementando protocolli specifici e promuovendo un ambiente lavorativo rispettoso e inclusivo. Queste misure garantiscono la

conformità normativa, rafforzano la cultura aziendale e proteggono l'integrità della struttura, assicurando un trattamento equo e non discriminatorio verso tutti, inclusi i pazienti e il personale sanitario.

25 REATI DI FALSITÀ IN MONETA, IN CARTE PUBBLICHE DI CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO

L'art. 25-bis del D.lgs. n. 231/2001, introdotto dall'art. 6 del D.L. n. 350/2001, prende in considerazione una serie di fattispecie codicistiche relative alla falsità in monete, in carte di pubblico credito e in valori di bollo, con l'obiettivo di tutelare la certezza e l'affidabilità del traffico giuridico ed economico, ovvero la "fede pubblica".

25.1 FATTISPECIE DI REATO RILEVANTI

Le fattispecie di reato punibili, ai sensi dell'art. 25-bis del D.lgs. n. 231/2001, includono:

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.).
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.).
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.).
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.).
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.).
- Uso di valori di bollo contraffatti o alterati (art. 464 c.p.).

25.2 ATTIVITA' SENSIBILI

Le attività individuate come potenzialmente sensibili per il rischio di commissione di reati includono:

- Gestione delle operazioni di cassa e dei pagamenti: controllo accurato della validità delle banconote e delle monete.
- Verifica dei titoli di pagamento e delle carte di credito: verifica della genuinità e della regolarità degli strumenti di pagamento accettati.
- Uso e gestione dei valori di bollo: utilizzo di valori di bollo per la documentazione sanitaria e amministrativa.
- Trattamento di documenti ufficiali e cartacei: include la gestione di qualsiasi documento che richieda l'utilizzo di carta filigranata o ologrammi.

25.3 PRINCIPI GENERALI DI COMPORTAMENTO

Per prevenire la commissione dei reati di falsità in moneta, in carte pubbliche di credito, in valori di bollo e in strumenti o segni di riconoscimento, i dipendenti e i collaboratori della struttura devono:

1. Astenersi da qualsiasi comportamento che possa configurare le fattispecie di reato.
2. Seguire rigorosamente le procedure aziendali per la gestione dei pagamenti, dei documenti fiscali e dei valori di bollo.
3. Mantenere una condotta trasparente e corretta nella gestione della cassa e delle operazioni finanziarie.
4. Segnalare prontamente qualsiasi irregolarità o sospetto di falsificazione al responsabile diretto o all'Organismo di Vigilanza (OdV).
5. Assicurare la tracciabilità dei processi e la conformità alle normative vigenti.

25.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

Per garantire la conformità e la prevenzione di reati, la struttura ha adottato protocolli specifici, tra cui:

- Controlli approfonditi sulle operazioni di cassa: formazione del personale addetto per riconoscere banconote e monete false.
- Verifiche sui documenti di pagamento: utilizzo di dispositivi e strumenti di verifica per accertare la validità di assegni e carte di credito.

- Procedure per la gestione dei valori di bollo e della carta filigranata: monitoraggio e registrazione dell'utilizzo per evitare falsificazioni.
- Audit periodici e controlli interni: esecuzione di audit regolari per verificare l'aderenza ai protocolli e l'efficacia delle procedure di prevenzione.
- Formazione continua: corsi di aggiornamento per il personale sulle tecniche di riconoscimento delle falsificazioni e sull'utilizzo corretto degli strumenti di verifica.

25.5 SOGGETTI COINVOLTI

I principali soggetti coinvolti nella prevenzione dei reati di falsità in monete, carte pubbliche di credito e valori di bollo includono:

- **Direzione**: supervisiona le operazioni di cassa e verifica l'aderenza ai protocolli. Effettua controlli giornalieri sui pagamenti e i documenti fiscali.
- **Organismo di Vigilanza (OdV)**: monitora l'efficacia del Modello 231, riceve segnalazioni di anomalie e verifica l'applicazione delle procedure.

25.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

L'OdV riceve report periodici contenenti:

- Segnalazioni di eventuali irregolarità riscontrate nelle operazioni di cassa e nei controlli sui documenti.
- Esiti degli audit interni e delle verifiche periodiche.
- Modifiche e aggiornamenti ai protocolli in risposta a nuove normative o a esigenze operative.

25.7 CONCLUSIONI

La struttura adotta misure preventive e protocolli specifici per garantire che le operazioni finanziarie e amministrative siano conformi alle normative vigenti, minimizzando i rischi di commissione dei reati di falsità. Queste pratiche assicurano l'integrità delle operazioni e rafforzano la fiducia nella società.

26 I REATI IN TEMA DI SALUTE E DI SICUREZZA SUL LAVORO

L'art. 25-septies del D.lgs. n. 231/2001, introdotto dall'art. 9 della L. n. 123/2007 e riformulato dal D.lgs. n. 81/2008, prevede la responsabilità dell'ente in relazione ai delitti di cui agli articoli 589 e 590, terzo comma, c.p.: omicidio colposo e lesioni colpose gravi e gravissime commessi con la violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

26.1 FATTISPECIE DI REATO RILEVANTI

Omicidio colposo (art. 589 c.p.)

"Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni. Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro, la pena è della reclusione da due a sette anni. [...]".

La rilevanza per il Decreto si ha quando la condotta colposa che causa la morte deriva dalla violazione delle norme per la prevenzione degli infortuni sul lavoro. L'oggettività giuridica tutelata è la vita umana, protetta non solo nell'interesse dell'individuo, ma anche della collettività.

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

"Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione o la multa. Se la lesione è grave o gravissima e commessa con violazione delle norme per la prevenzione degli infortuni sul lavoro, la pena è aumentata."

Rilevano ai fini del Decreto le condotte che causano lesioni gravi o gravissime per colpa e per violazione delle norme antinfortunistiche. Le lesioni sono definite come alterazioni – anatomiche o funzionali – dell'organismo, comprese modificazioni psichiche. Sono considerate lesioni gravi quelle che comportano un pericolo per la vita o un'incapacità prolungata, mentre sono gravissime quelle che causano la perdita permanente di un senso o di un organo.

26.2 LE ATTIVITA' SENSIBILI

L'adozione e l'attuazione del Modello Organizzativo richiedono una valutazione preliminare dei rischi per identificare le aree sensibili. Le aree a rischio rilevanti per la società includono:

- Gestione delle attrezzature e dei dispositivi medici: verifiche periodiche e manutenzione degli strumenti utilizzati per assicurare che siano conformi alle normative e sicuri per l'uso.
- Ambienti di lavoro: controllo degli spazi operativi per garantire condizioni di sicurezza e prevenire incidenti.
- Manipolazione e smaltimento di materiali: gestione sicura dei materiali potenzialmente pericolosi e adozione di procedure adeguate allo smaltimento.
- Formazione e informazione dei lavoratori: sviluppo e implementazione di programmi di formazione continua sulla sicurezza.
- Gestione degli infortuni e delle emergenze: preparazione e applicazione di procedure per affrontare rapidamente situazioni di emergenza e incidenti.
- Sorveglianza sanitaria: monitoraggio della salute dei lavoratori attraverso visite mediche periodiche.

ATTIVITA'	DIREZIONE	PRESIDI
Nomina del RSPP	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Nomina Medico Competente	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro

Acquisizione documentazione per le Certificazioni obbligatorie	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Valutazione dei Rischi e elaborazione del relativo documento	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Elaborazione delle Procedure in materia di sicurezza, prevenzione incendi, primo soccorso e verifiche periodiche delle stesse	Datore di Lavoro in collaborazione con RSPP	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Individuazione ed elaborazione delle Misure preventive e protettive e dei DPI	Datore di Lavoro in collaborazione con RSPP	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Individuazione fattori a rischio	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Informazione ai lavoratori sui rischi per la salute e misure di prevenzione e protezione adottate	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Assegnazione mansioni	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Gestione Infortuni	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Controllo corretto utilizzo delle attrezzature	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Controllo utilizzo delle dotazioni di sicurezza (guanti, tappi, mascherine, tuta, scarpe, ecc)	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro

Informazione e Formazione dei lavoratori	Datore di Lavoro/RLS	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Invio informazioni al RSPP, al datore di lavoro e all'Organismo di Vigilanza	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Ispezioni per prevenzione incendi	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Programmazione riunioni periodiche sulla sicurezza	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro
Vigilanza sulle procedure adottate e delle istruzioni date ai lavoratori	Datore di Lavoro	Codice Etico Procedure implementate ai fini del D. Lgs n. 81/2008 PG Verifica degli adempimenti in materia di sicurezza sui luoghi di lavoro

26.3 PRINCIPI GENERALI DI COMPORTAMENTO

La società si impegna a rispettare l'obbligo generale di tutela della salute e della sicurezza sul lavoro sancito dall'art. 2087 c.c. e dal D.lgs. 81/2008. I principi generali di comportamento includono:

1. Rispetto rigoroso delle normative vigenti in materia di salute e sicurezza sul lavoro.
2. Coinvolgimento di tutta l'organizzazione nella gestione della sicurezza, con compiti e responsabilità chiaramente definiti.
3. Adozione delle migliori pratiche e tecnologie disponibili per garantire la sicurezza, indipendentemente dai costi.
4. Interruzione dell'attività in caso di impossibilità di garantire la sicurezza.
5. Informazione e formazione continua dei lavoratori sui rischi e sulle misure preventive.

26.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

La società ha adottato protocolli per garantire la conformità alle normative di salute e sicurezza:

- Nomina del Responsabile del Servizio di Prevenzione e Protezione (RSPP): figura centrale per la gestione della sicurezza.
- Elaborazione e aggiornamento del Documento di Valutazione dei Rischi (DVR): analisi dei rischi presenti in azienda.
- Procedure per l'uso dei dispositivi di protezione individuale (DPI): regole chiare sull'utilizzo obbligatorio dei DPI.
- Verifiche periodiche delle attrezzature e degli ambienti di lavoro per assicurare la conformità.
- Informazione e formazione obbligatoria: corsi periodici per tutto il personale.
- Monitoraggio e controllo da parte dell'Organismo di Vigilanza (OdV): verifica dell'applicazione dei protocolli e delle procedure.

26.5 SOGGETTI COINVOLTI

I principali soggetti coinvolti nella gestione della salute e sicurezza sul lavoro sono:

- **Direzione**: responsabile della sicurezza e della gestione delle risorse.
- **Responsabile del Servizio di Prevenzione e Protezione (RSPP)**: coordina le attività di prevenzione.
- **Preposto**: garantisce l'attuazione delle misure di sicurezza e il rispetto delle direttive ricevute, vigilando sulla corretta applicazione delle norme.
- **Medico Competente**: effettua la sorveglianza sanitaria.
- **Rappresentante dei Lavoratori per la Sicurezza (RLS)**: rappresenta i lavoratori e collabora con l'RSPP.
- **OdV**: monitora il rispetto delle misure adottate e riceve segnalazioni di eventuali violazioni.
- **Lavoratori**: devono rispettare le norme e le procedure aziendali e segnalare situazioni di pericolo.

26.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

L'OdV deve ricevere:

- Aggiornamenti e modifiche al DVR.
- Report periodici sulle attività di formazione e sulle verifiche effettuate.
- Informazioni sugli infortuni e sulle misure adottate per prevenirne la ricorrenza.
- Verbali delle riunioni periodiche sulla sicurezza.

26.7 CONCLUSIONI

La società adotta un approccio rigoroso alla gestione della sicurezza sul lavoro, garantendo conformità alle normative vigenti e minimizzando i rischi di incidenti. L'impegno costante nella prevenzione e nella formazione contribuisce a creare un ambiente di lavoro sicuro per tutti.

27 I REATI CONTRO LA PERSONALITÀ INDIVIDUALE

In riferimento alle ipotesi di reato contro la personalità individuale per le quali scatta la responsabilità amministrativa dell'ente, ai sensi dell'art. 25-quinquies, questa sezione del Modello intende fornire una descrizione dettagliata dei suddetti reati. Il testo integrale degli articoli del Codice penale è riportato in allegato al Modello Organizzativo per una consultazione completa.

27.1 FATTISPECIE DI REATO RILEVANTI

Di seguito sono riportate le principali fattispecie di reato contro la personalità individuale rilevanti per il Modello Organizzativo:

- **Riduzione in schiavitù** (art. 600 c.p.): questo reato si configura nei casi di condizioni lavorative degradanti o di sfruttamento in contesti in cui i rapporti lavorativi non sono adeguatamente regolamentati.
- **Tratta di persone** (art. 601 c.p.): reato potenzialmente applicabile qualora si verifichino condizioni di sfruttamento, in particolare per il personale assunto tramite agenzie esterne o con contratti poco chiari.
- **Prostituzione minorile** (art. 600-bis c.p.): si applica in caso di coinvolgimento di minori in attività di prostituzione.
- **Pornografia minorile** (art. 600-ter c.p.): concerne la produzione, detenzione o diffusione di materiale pornografico minorile.

27.2 ATTIVITÀ SENSIBILI

A seguito dell'analisi delle aree operative aziendali, sono state identificate le seguenti attività a rischio per la possibile commissione di reati contro la personalità individuale:

- Assunzione e gestione del personale: richiede un controllo accurato sull'integrità dei processi di assunzione e sulle condizioni contrattuali, per evitare potenziali fenomeni di sfruttamento.
- Rapporti con clienti e terze parti: necessità di prevenire qualsiasi comportamento illecito durante le interazioni con i pazienti e nelle relazioni con terze parti.
- Utilizzo dei sistemi informatici e accesso a internet: monitoraggio per prevenire l'accesso o la condivisione non autorizzati di materiale illegale.

27.3 PRINCIPI GENERALI DI COMPORTAMENTO

La società richiede ai suoi dipendenti e collaboratori di:

1. Astenersi dal tenere comportamenti che possano integrare le fattispecie previste dai reati contro la personalità individuale.
2. Rispettare le norme di legge e le procedure aziendali per evitare situazioni che potrebbero portare a violazioni.
3. Adottare comportamenti trasparenti e corretti, mantenendo il rispetto per la dignità umana.
4. Segnalare tempestivamente qualsiasi sospetto di violazione al responsabile diretto o all'OdV.

27.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

Per prevenire la commissione di reati contro la personalità individuale, la società adotta protocolli che includono:

- Controlli durante il processo di assunzione: verifiche sulla documentazione e sulle condizioni di lavoro offerte.
- Monitoraggio dell'uso dei sistemi informatici: implementazione di software per impedire l'accesso a contenuti non conformi.
- Formazione continua: programmi per sensibilizzare il personale sui comportamenti da adottare per garantire il rispetto della personalità individuale.
- Procedure di gestione delle segnalazioni: canali riservati per la comunicazione di eventuali comportamenti illeciti.

27.5 SOGGETTI COINVOLTI

I principali soggetti coinvolti nella prevenzione e gestione dei reati contro la personalità individuale sono:

- **Datore di Lavoro**: responsabile dell'implementazione e supervisione dei protocolli.
- **Direzione Sanitaria/Tecnica:** supervisione e controllo.
- **Preposto**: vigila sull'applicazione delle norme e delle procedure aziendali.
- **OdV**: monitora l'efficacia del Modello 231 e riceve segnalazioni di eventuali violazioni.
- **Lavoratori**: devono rispettare le procedure e segnalare eventuali anomalie.

27.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

L'OdV riceve:

- Segnalazioni di possibili violazioni dei protocolli.
- Report periodici sulle attività di formazione e sulle verifiche effettuate.
- Aggiornamenti sui controlli svolti nelle aree a rischio.

27.7 CONCLUSIONI

L'ente adotta misure preventive specifiche per garantire il rispetto della personalità individuale, minimizzando i rischi di comportamenti illeciti. L'impegno nella formazione e nell'applicazione dei protocolli contribuisce a un ambiente lavorativo etico e conforme alle normative.

28 PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI

Questa sezione del Modello si applica al reato di pratiche di mutilazione degli organi genitali femminili, disciplinato dall'art. 25-quater.1 del D. Lgs. 231/2001, che introduce la responsabilità amministrativa dell'ente.

28.1 FATTISPECIE DI REATO RILEVANTI

La Legge n. 7 del 9 gennaio 2006, contenente disposizioni per la prevenzione e il divieto delle pratiche di infibulazione, ha introdotto nel Codice penale il reato di pratiche di mutilazione degli organi genitali femminili (art. 583-bis c.p.), successivamente modificato e integrato, estendendo la responsabilità anche alle entità e strutture che, direttamente o indirettamente, favoriscano la realizzazione di tali pratiche. Tale responsabilità si applica in particolare alle strutture sanitarie e organizzazioni di volontariato che potrebbero coinvolgersi in attività illecite di questa natura.

- **Pratiche di mutilazione degli organi genitali femminili** (art. 583-bis c.p.): l'art. 583-bis punisce chiunque, in assenza di necessità terapeutiche, causi una mutilazione degli organi genitali femminili. La

norma include pratiche quali clitoridectomia, escissione, infibulazione e altre azioni che comportino effetti analoghi. Inoltre, è sanzionato chiunque, al fine di menomare le funzioni sessuali, provochi lesioni agli organi genitali femminili che causino una malattia nel corpo o nella mente. La disposizione si applica anche ai reati commessi all'estero da cittadini italiani o da stranieri residenti in Italia, o quando la vittima sia cittadino italiano o residente in Italia.

28.2 ATTIVITA' SENSIBILI

Le attività sensibili e le aree a rischio per la possibile commissione del reato in oggetto includono:

- **Attività clinico-assistenziale**, con particolare riferimento all'erogazione di prestazioni ambulatoriali.

28.3 PRINCIPI GENERALI DI COMPORTAMENTO

Per evitare il verificarsi di pratiche illecite legate alla mutilazione degli organi genitali femminili, tutti i destinatari del Modello sono tenuti a rispettare i seguenti principi:

- È fatto divieto di compiere o partecipare a condotte che possano configurare, anche solo potenzialmente, le fattispecie di reato di cui all'art. 25-quater.1 del D. Lgs. 231/2001.
- È proibito causare mutilazioni ai pazienti in assenza di specifiche esigenze terapeutiche, specialmente sugli organi genitali femminili.
- È vietato utilizzare le strutture o le risorse della Società per finalità che possano essere ricondotte a pratiche mutilanti.

Inoltre, i destinatari devono:

- Assicurare che le attività di diagnosi e cura siano sempre proporzionate e appropriate rispetto alle patologie riscontrate;
- Fornire prestazioni sanitarie in conformità con le finalità istituzionali della Società e il Codice di Deontologia Medica;
- Adottare protocolli e trattamenti clinici che rispettino la dignità e i diritti dei pazienti;
- Gestire la documentazione clinica e diagnostica in conformità alla legge, assicurando tracciabilità, chiarezza, accuratezza e veridicità delle informazioni;
- Rispettare l'integrità fisica, psichica e sessuale della persona, come previsto dalla Costituzione e dalle convenzioni internazionali.

28.4 PROTOCOLLI SPECIFICI DI PREVENZIONE

Per prevenire questo tipo di reato, la Società ha adottato specifici protocolli e presidi generali che comprendono:

- Controlli documentali per assicurare che le attività siano conformi alle norme;
- Monitoraggio delle attività clinico-assistenziali, con particolare attenzione alle pratiche ambulatoriali, per garantire che non vengano eseguiti interventi non autorizzati;
- Rispetto del Codice Etico e dei principi di deontologia medica, per assicurare il massimo rispetto per l'integrità psicofisica delle persone;
- Canali riservati per le segnalazioni di comportamenti anomali, garantendo la confidenzialità delle comunicazioni e la protezione da eventuali ritorsioni.

28.5 SOGGETTI COINVOLTI

I principali soggetti responsabili per la prevenzione e gestione del reato di mutilazione degli organi genitali femminili sono:

Direzione: responsabile dell'implementazione dei protocolli di controllo e supervisione delle attività a rischio.

Preposto: assicura il rispetto delle norme e delle procedure aziendali.

Direzione Sanitaria/Tecnica e Medici: si occupano della corretta applicazione dei protocolli clinico-assistenziali e del rispetto delle normative di settore.

Organismo di Vigilanza (OdV): verifica l'efficacia del Modello 231 e riceve segnalazioni su eventuali violazioni.

28.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

L'Organismo di Vigilanza riceve periodicamente:

- Segnalazioni di eventuali violazioni o comportamenti sospetti;
- Report sulle attività di monitoraggio e formazione in materia di prevenzione;
- Aggiornamenti sui controlli effettuati nelle aree a rischio e sugli eventuali adeguamenti dei protocolli.

La Società si impegna a garantire il rispetto della dignità e dell'integrità della persona, adottando misure preventive mirate per evitare ogni forma di mutilazione degli organi genitali femminili. Le misure di formazione continua e l'implementazione di specifici protocolli di prevenzione contribuiscono a promuovere un ambiente lavorativo sicuro e conforme alle normative vigenti.

29 REATI IN MATERIA AMBIENTALE

La presente Parte Speciale si applica alle tipologie di reati identificati dall'art. 25-undecies del Decreto.

29.1 FATTISPECIE DI REATO RILEVANTI

Il D. Lgs. 121/2011 ha esteso l'ambito di applicazione del D. Lgs. 231/2001 ai reati ambientali, come previsto dalla Legge Delega n. 300/2000. Questa normativa mira a responsabilizzare le società in merito alla protezione ambientale, soprattutto nel contesto di attività possono generare rifiuti speciali e pericolosi.
Il riferimento centrale è il Testo Unico Ambientale (D. Lgs. 152/2006), che definisce il "danno ambientale" come qualsiasi deterioramento significativo e misurabile di una risorsa naturale o dell'utilità assicurata da questa.
I principali reati ambientali rilevanti per la struttura includono:

- **Attività di gestione dei rifiuti non autorizzate** (art. 256, D. Lgs. 152/2006): si configura quando si svolge attività di raccolta, trasporto, smaltimento o gestione di rifiuti pericolosi senza le autorizzazioni prescritte. Nei laboratori di analisi, ciò riguarda principalmente rifiuti biologici, materiali contaminati, reagenti chimici esausti e contenitori utilizzati.
- **False indicazioni su natura e caratteristiche dei rifiuti** (art. 258, D. Lgs. 152/2006): Le violazioni possono includere la falsificazione o l'incompletezza dei dati riportati nei registri di carico e scarico dei rifiuti e nei formulari di identificazione dei rifiuti. Ad esempio, dichiarare una tipologia di rifiuto meno pericolosa rispetto a quella reale o indicare quantitativi differenti.
- **Traffico illecito di rifiuti** (art. 259, D. Lgs. 152/2006): Si configura qualora i rifiuti vengano movimentati o smaltiti in modo non conforme, ad esempio attraverso operatori non autorizzati, o esportati senza rispettare le normative nazionali ed europee.
- **Inquinamento ambientale** (art. 452-bis c.p.): Questo reato si applica se una gestione inadeguata dei rifiuti o di sostanze pericolose causa una compromissione o deterioramento significativo e misurabile dell'ambiente, incluse le risorse idriche, l'aria, il suolo o gli ecosistemi.
- **Delitti colposi contro l'ambiente** (art. 452-quater c.p.): Si applica qualora i reati di inquinamento ambientale vengano commessi per colpa, cioè per negligenza o imprudenza.

29.2 ATTIVITA' SENSIBILI

Le attività identificate come particolarmente sensibili per la possibile commissione di reati ambientali includono:
Gestione dei Rifiuti Sanitari pericolosi:
È fondamentale disporre di contenitori specifici per rifiuti pericolosi e collaborare con fornitori autorizzati per lo smaltimento.
Stoccaggio temporaneo di rifiuti:

- I rifiuti sanitari e altri rifiuti speciali devono essere conservati temporaneamente in spazi dedicati, in modo sicuro e separato, evitando il rischio di dispersione o contaminazione.

- Devono essere adottate procedure che garantiscano la chiusura ermetica dei contenitori e il rispetto dei tempi massimi di stoccaggio.

Uso e Smaltimento di Sostanze Chimiche:

- Nel caso di utilizzo di sostanze chimiche, ad esempio per la manutenzione di apparecchiature o la sanificazione degli ambienti, è necessario verificare che i fornitori e gli operatori esterni incaricati del trasporto e dello smaltimento siano autorizzati e in possesso di tutte le certificazioni previste dalla normativa ambientale.

Gestione di Scarichi e Rifiuti Liquidi:

- Eventuali scarichi prodotti, come acque reflue contenenti detergenti o disinfettanti, devono essere gestiti in conformità alle normative vigenti.
- Il centro deve verificare che gli scarichi siano trattati adeguatamente e non rappresentino un rischio per l'ambiente o per il sistema fognario

29.3 PRINCIPI GENERALI DI COMPORTAMENTO

Al fine di garantire il rispetto delle normative ambientali, il laboratorio si impegna a rispettare i seguenti principi generali di comportamento:

- Divieto di abbandono di rifiuti: tutti i rifiuti devono essere gestiti e conferiti a soggetti autorizzati secondo quanto stabilito dalla normativa.
- Tracciabilità dei rifiuti: la compilazione di registri e formulari deve essere accurata e completa, riportando correttamente la natura, la quantità e la destinazione dei rifiuti.
- Prevenzione delle contaminazioni: i rifiuti e i reagenti devono essere stoccati in contenitori adeguati, etichettati e conservati in aree appositamente designate.
- Conformità alle autorizzazioni: ogni attività legata a scarichi, emissioni o smaltimento deve essere effettuata nel rispetto dei limiti e delle prescrizioni previste dalle autorizzazioni rilasciate.
- Formazione del personale: tutto il personale coinvolto nella gestione di sostanze pericolose e rifiuti deve ricevere una formazione adeguata.

29.4 PROTOCOLLI SPECIFICI DI PREVENZIONE E CONTROLLO

I protocolli specifici di prevenzione e controllo per la struttura includono:

Procedure per la gestione dei rifiuti sanitari:

- Raccolta, separazione e smaltimento secondo le categorie di pericolosità, con un'attenzione particolare ai rifiuti biologici e chimici.

Monitoraggio dei registri di tracciabilità:

- Controllo regolare della correttezza dei registri e dei formulari relativi ai rifiuti.

Manutenzione delle infrastrutture:

- Verifica periodica delle aree di stoccaggio e delle apparecchiature per prevenire perdite o dispersioni.

Selezione dei fornitori:

- Definizione di criteri stringenti per la scelta degli operatori incaricati del trasporto e dello smaltimento dei rifiuti.

Controllo sugli scarichi:

- Campionamenti periodici per verificare la conformità delle acque reflue agli standard previsti.

29.5 I SOGGETTI COINVOLTI

I principali soggetti coinvolti nella gestione e prevenzione dei reati ambientali sono:

- **Direzione**: responsabile della supervisione delle attività sensibili e dell'implementazione dei protocolli ambientali;
- **Direzione Sanitaria/Tecnica**: assicurano la corretta gestione dei rifiuti e il rispetto delle normative;
- **Organismo di Vigilanza (OdV)**: monitora l'efficacia del Modello 231 e riceve eventuali segnalazioni di non conformità;
- **Fornitori e Consulenti esterni**: devono possedere adeguate qualifiche e rispettare le normative ambientali.

29.6 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA (ODV)

L'OdV deve ricevere regolarmente:

- Segnalazioni di possibili violazioni o anomalie nella gestione dei rifiuti;
- Report di monitoraggio sui dati delle emissioni, dei rifiuti radioattivi e sugli aggiornamenti delle autorizzazioni;
- Documentazione relativa alla conformità delle attività di smaltimento e gestione dei rifiuti sanitari pericolosi.

29.7 CONCLUSIONI

La struttura si impegna a garantire la massima attenzione e conformità alle normative ambientali, adottando misure rigorose per la gestione dei rifiuti, la tracciabilità delle attività sensibili e la formazione del personale. L'obiettivo è assicurare la tutela dell'ambiente e prevenire ogni rischio legato a comportamenti illeciti o negligenti.

30 MISURAZIONE E ANALISI DI MIGLIORAMENTO

30.1 PIANIFICAZIONE E ATTUAZIONE

3d srl, per pianificare ed attuare i processi di analisi e di miglioramento necessari a:

- Dimostrare la conformità ai requisiti del SGRA
- Assicurare la conformità del SGRA alla legislazione vigente
- Migliorare in continuo il SGRA

ha formalizzato le seguenti azioni:

- Attuazione del Programma di *Audit* finalizzata alla promozione di Azioni Correttive e Preventive;
- Gestione delle non Conformità;
- Riesame della Direzione.

30.2 MONITORAGGIO E MISURAZIONE DEI PROCESSI

Il monitoraggio e misurazione dei processi è effettuato mediante i seguenti strumenti di controllo:

PROCESSO	STRUMENTO DI CONTROLLO
Monitoraggio del livello delle prestazioni e per il raggiungimento degli obiettivi definiti	Audit finalizzato alla promozione di Azioni Correttive e Preventive Riesame della Direzione
Monitoraggio dell'attività lavorativa rispetto al MMO	Numero di Non Conformità
Monitoraggio della percezione e grado di coinvolgimento delle parti interessate	Riunioni con il personale
Misure reattive per violazioni gravi	Sistema disciplinare e Sanzionatorio
Verifica della necessità di ulteriori azioni correttive e preventive	Sufficiente Numero di registrazioni dei dati e dei risultati dei controlli
Valutazione della conformità legislativa	Controllo Periodico

30.3 L'ANALISI DEI DATI

L'analisi dei dati del Monitoraggio e Misurazione dei processi permette di dimostrare l'adeguatezza e l'efficacia del SGRA e valutazione delle aree dove possa essere realizzato il Miglioramento Continuo e fornisce informazioni in merito a:

- Percezione e grado di coinvolgimento delle parti interessate
- Conformità alle prescrizioni legali
- Caratteristiche e tendenze dei processi, comprese opportunità per azioni preventive