

MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
EX D.LGS. N. 231/2001
di Gerit S.r.l.
(Parte B - Parte Speciale)

Approvato dal C.d.A. con delibera del XXX

Sommario

1. Premessa	3
2. Scopo della Parte Speciale	4
CAPITOLO I	
Reati nei rapporti con la Pubblica Amministrazione.....	5
1.1. Premessa.....	5
1.2. Principi Generali di Comportamento	6
1.3. Principi Operativi.....	7
1.3.1. Rapporti diretti con la P.A.....	7
1.3.2. Gestione degli omaggi.....	8
1.3.3. Sponsorizzazioni	9
1.3.4. Partecipazione a gare d'appalto.....	9
1.3.5. Rapporti con le parti terze.....	10
1.3.6. Accessi, ispezioni e verifiche.....	10
1.3.7. Finanziamenti pubblici (o altre agevolazioni)	10
1.4. Controlli dell'Organismo di Vigilanza.....	11
1.5. Rinvio alle Procedure e Istruzioni Operative.....	11
CAPITOLO II	
Reati Societari.....	13
2.1. Premessa.....	13
2.2. Principi Generali di Comportamento.....	13
2.3. Principi Operativi.....	14
2.4. Predisposizione del bilancio e di altri documenti destinati a terzi	14
2.5. Operazioni contabili	15
2.6. Operazioni relative al capitale sociale.....	15
2.7. Controlli dell'Organismo di Vigilanza.....	16
2.8. Rinvio alle Procedure e Istruzioni Operative.....	16
CAPITOLO III	
Reati contro le frodi in commercio e reati patrimoniali.....	17
3.1. Premessa.....	17
3.2. Principi Generali di Comportamento.....	17
3.3. Principi Operativi	18

3.4. Controlli dell'Organismo di Vigilanza.....	19
3.5. Rinvio alle Procedure e Istruzioni Operative.....	20

CAPITOLO IV

Reati in materia di sicurezza sul lavoro	21
4.1. Premessa.....	21
4.2. Principi Generali di Comportamento	21
4.3. Principi Operativi.....	26
4.3.1. Articolazione interna delle funzioni di sicurezza	27
4.3.2. Valutazione dei rischi	27
4.3.3. Gestione delle emergenze e primo soccorso	28
4.3.4. Riunioni periodiche di sicurezza.....	28
4.3.5. Gestione dei lavori in appalto	28
4.4. Controlli dell'Organismo di Vigilanza.....	29
4.5. Rinvio alle Procedure e Istruzioni Operative.....	30

CAPITOLO V

Reati Tributari.....	31
5.1. Premessa.....	31
5.2. Principi Generali di Comportamento.....	31
5.3. Principi Operativi.....	32
5.4. Controlli dell'Organismo di Vigilanza.....	34
5.5. Rinvio alle Procedure e Istruzioni Operative.....	35

CAPITOLO VI

Reati informatici, di trattamento illecito di dati e violazione del diritto d'autore.....	36
6.1. Premessa.....	36
6.2. Principi Generali di Comportamento.....	38
6.3. Principi Operativi.....	38
6.4. Controlli dell'Organismo di Vigilanza.....	40
6.5. Rinvio alle Procedure e Istruzioni Operative.....	41

1. PREMESSA

Dall'analisi dei processi aziendali di Gerit S.r.l., sia tramite intervista diretta alle principali funzioni aziendali, sia tramite analisi della principale documentazione aziendale (Statuto, documenti societari, procedure), sono stati individuati alcuni c.d. "Processi Sensibili", con conseguente identificazione dei Reati di possibile commissione nell'interesse o a vantaggio della Società.

Tali reati sono ascrivibili principalmente ed in via sintetica alle seguenti categorie:

- Reati nei rapporti con la Pubblica Amministrazione e l'Autorità Giudiziaria;
- Reati societari;
- Reati di ricettazione e riciclaggio;
- Reati contro l'industria e il commercio;
- Reati tributari;
- Reati in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (omicidio colposo e lesioni colpose gravi o gravissime);
- Reati informatici e trattamento illecito di dati;
- Reati in materia di violazione del diritto d'autore;
- Reati in materia di assunzione di lavoratori stranieri.

Le altre fattispecie di Reato previste nel Decreto non sembrano presentare profili di rischio tali da rendere ragionevolmente fondata la loro possibile commissione nell'interesse o a vantaggio della Società.

Per tali Reati, pertanto, permane il richiamo ai principi generali contenuti sia nel presente Modello sia nel Codice Etico, i quali vincolano tutti i Destinatari al rispetto dei valori di tutela della personalità individuale, di correttezza, moralità e rispetto delle leggi vigenti.

La Parte Speciale del Modello risulta, pertanto, suddivisa nei Capitoli di seguito intitolati:

1. Reati nei rapporti con la Pubblica Amministrazione;
2. Reati societari;
3. Reati contro le frodi in commercio e reati patrimoniali;
4. Reati in materia di salute e sicurezza sul lavoro;
5. Reati tributari;
6. Reati informatici, di trattamento illecito di dati e di violazione del diritto d'autore.

Con riferimento ai "Reati nei confronti dell'Autorità Giudiziaria" e ai "Reati in materia di assunzione di lavoratori stranieri", agli stessi non risulta dedicata una specifica Sezione di Parte Speciale del Modello in quanto si ritiene che gli stessi risultino adeguatamente contrastati da principi e procedure di controllo già stabiliti per altri Reati.

2. SCOPO DELLA PARTE SPECIALE

La presente Parte Speciale ha lo scopo di:

- i) indicare i Processi Sensibili in relazione ai quali sono astrattamente configurabili i Reati presupposto;
- ii) indicare i principi generali di comportamento e i principi operativi che i Destinatari sono obbligati ad osservare ai fini della corretta applicazione del Modello e, quindi, della prevenzione dei Reati predetti;
- i) fornire all'Organismo di Vigilanza e alle diverse funzioni aziendali interessate dalla possibile commissione dei Reati, gli strumenti per esercitare le attività di controllo, monitoraggio e verifica.

In particolare, i principi generali di comportamento individuano i principi fondamentali e di portata generale, ai quali tutti i Destinatari del Modello devono conformarsi per prevenire la commissione dei Reati. Tali principi si articolano in una serie di protocolli che devono necessariamente essere coerenti sia con i principi del Codice Etico, di cui costituiscono una maggiore specificazione, sia con i risultati della mappatura delle aree a rischio Reato.

I principi operativi, invece, costituiscono una specificazione sul piano operativo dei principi generali di comportamento, in quanto definiscono nel dettaglio i processi e le attività di controllo. I principi operativi identificano i soggetti coinvolti nelle varie fasi del processo e attribuiscono a ciascuno compiti e responsabilità coerentemente con i risultati della mappatura e con i principi generali.

Il sistema di organizzazione di Gerit S.r.l., pertanto, deve rispettare i seguenti principi di portata generale:

- i. chiara descrizione delle linee di riporto gerarchico;
- ii. conoscibilità, trasparenza e pubblicità dei poteri attribuiti (all'interno della Società e nei confronti dei terzi interessati);
- iii. chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione, dei relativi poteri e responsabilità;
- iv. separazione, all'interno di ciascun processo, tra il soggetto che assume la decisione (impulso decisionale), il soggetto che esegue tale decisione e il soggetto cui è affidato il controllo del processo (c.d. "segregazione delle funzioni");
- v. traccia scritta di ciascun passaggio rilevante del processo (c.d. "tracciabilità").

CAPITOLO I

Reati nei rapporti con la Pubblica Amministrazione

1.1. Premessa

Il presente Capitolo prende in considerazione i Reati che possono essere commessi dai Destinatari del Modello nell'ambito dei rapporti tra la Società e la Pubblica Amministrazione, previsti dagli artt. 24 (*"Indebita percezione di erogazioni, truffa in danno dello Stato, 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"*) e 25 (*"Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio"*) del d.lgs. 231/2001.

Di seguito si riportano le fattispecie di reato previste dall'art. 24 del Decreto (*"Indebita percezione di erogazioni, truffa in danno dello Stato, 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. 316 *bis* c.p.: Malversazione di erogazioni pubbliche
- art. 316 *ter* c.p.: Indebita percezione di erogazioni a danno dello Stato
- art. 353 c.p.: Turbata libertà degli incanti
- art. 353 *bis* c.p.: Turbata libertà del procedimento di scelta del contraente
- art. 356 c.p.: Frode nelle pubbliche forniture
- art. 640, comma 2 n. 1), c.p.: Truffa in danno dello Stato o di un altro ente pubblico e della Comunità europee
- art. 640 *bis* c.p.: Truffa aggravata per il conseguimento di erogazioni pubbliche
- art. 640 *ter* c.p.: Frode informatica in danno dello Stato o di altro ente pubblico
- art. 2 L. n. 898/1986: Frode ai danni del fondo agricolo europeo

Di seguito si riportano le fattispecie di reato previste dall'art. 25 (*"Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio"*) del Decreto.

- art. 314, comma 1, c.p.: Peculato
- art. 314 *bis* c.p.: Indebita destinazione di denaro o cose mobili
- art. 316 c.p.: Peculato mediante profitto dell'errore altrui
- art. 317 c.p.: Concussione
- art. 318 c.p.: Corruzione per l'esercizio della funzione
- art. 319 c.p.: Corruzione per un atto contrario ai doveri di ufficio
- art. 319 *bis* c.p.: Circostanze aggravanti
- art. 319 *ter*, comma 1, c.p.: Corruzione in atti giudiziari
- art. 319 *ter*, comma 2, c.p.: Corruzione in atti giudiziari (se taluno è ingiustamente condannato alla detenzione)
- art. 319 *quater* c.p.: Induzione indebita a dare o promettere utilità
- art. 320 c.p.: Corruzione di persona incaricata di un pubblico servizio
- art. 321 c.p.: Pene per il corruttore
- art. 322, commi 1 e 3, c.p.: Istigazione alla corruzione per l'esercizio della funzione
- art. 322, commi 2 e 4, c.p.: Istigazione alla corruzione
- art. 322 *bis* c.p.: Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli Organi delle Comunità europee o di assemblee parlamentari internazionali o organizzazioni internazionali o di funzionari delle Comunità europee e di Stati esteri
- art. 346 *bis* c.p.: Traffico di influenze illecite

In linea generale, i Destinatari del Modello, al fine di prevenire la commissione dei predetti Reati, devono conformarsi alla normativa vigente, al Codice Etico, ai valori e alle politiche della Società e alle regole contenute nel presente Modello.

Inoltre, l'organizzazione della Società deve rispettare i principi fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative, di tracciabilità delle operazioni.

1.2. Principi Generali di Comportamento

I Destinatari del Modello, ovvero amministratori, dipendenti, collaboratori e *partner* commerciali di Gerit S.r.l., devono attenersi ai principi generali di comportamento di seguito enunciati:

- a) osservare tutte le regole e i principi contenuti nel presente Modello, nel Codice Etico, in leggi, regolamenti, protocolli e procedure interne che disciplinano l'operatività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con la Pubblica Amministrazione;
- b) instaurare e gestire qualsiasi rapporto con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza;
- c) astenersi dal porre in essere, collaborare o contribuire alla realizzazione di comportamenti che, in tutto o in parte, possano integrare, direttamente o indirettamente, i reati previsti dagli artt. 24 e 25 o possano semplicemente agevolare la commissione;
- d) effettuare pagamenti o qualsivoglia operazione di carattere finanziario solo in forza di poteri di firma previsti da espresse deleghe di funzione e da specifiche procure o previa autorizzazione espressa e specifica;
- e) ove possibile, evitare di trovarsi in una posizione, potenziale o reale, di conflitto di interessi¹.

In particolare, nello svolgimento della normale attività lavorativa, coerentemente con i principi del Modello e del Codice Etico, vi è il divieto di porre in essere le seguenti condotte:

- f) presentare documentazione e/o dichiarazioni non veritiere o incomplete a funzionari della P.A. (a titolo esemplificativo e non esaustivo: al fine di conseguire erogazioni, contributi o finanziamenti, ovvero ottenere il rilascio/rinnovo di autorizzazioni, licenze, concessioni ovvero ogni attestato e/o documentazione funzionali all'esercizio dell'attività da parte della Società);
- g) destinare le somme ricevute dalla P.A. a scopi diversi da quelli per i quali sono state erogate;
- h) attestare il possesso di requisiti inesistenti, richiesti dalla legge o da atti amministrativi, al fine di partecipare a gare o simili ovvero al fine di risultarne i vincitori;
- i) porre in essere qualsiasi tipo di condotta idonea a indurre in errore organismi pubblici nazionali o esteri;

¹ In particolare, il conflitto di interessi si verifica quando viene affidata una responsabilità decisionale a un soggetto che ha interessi personali o professionali in contrasto con l'imparzialità richiesta da tale responsabilità, che può venire meno a causa degli interessi in causa. Il conflitto di interessi è reale (o attuale) quando l'interesse secondario proprio del dipendente è suscettibile d'influenzare il perseguimento dell'interesse primario di Gerit S.r.l. nel momento in cui il dipendente è chiamato, nell'esercizio delle sue funzioni, ad assumere o concorrere ad assumere una decisione, a svolgere un'attività istruttoria o comunque a contribuire tramite l'espletamento della propria attività lavorativa alla formazione della decisione. L'interferenza potrebbe anche derivare da strette relazioni interpersonali tra il dipendente e soggetti portatori di un proprio interesse secondario in grado di interferire con l'interesse primario.

- j) ricevere o offrire somme di denaro o altre utilità allo scopo di sollecitare od ottenere informazioni riservate utili alla compromissione dell'integrità decisionale delle persone coinvolte nella gestione del rapporto d'affari;
- k) riconoscere a consulenti o collaboratori esterni compensi (economici o prestazioni) che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;
- l) effettuare prestazioni in favore di eventuali *partner* (commerciali od operativi) che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;
- m) ricevere o offrire somme di denaro o altre utilità al fine di falsificare e/o alterare i dati documentali per ottenere il favore o l'approvazione di un progetto non conforme alle normative vigenti in materia;
- n) concedere ai soggetti appartenenti alla P.A., ai loro familiari o a persone a loro collegate e/o da loro segnalate, elargizioni in denaro o altro, ivi inclusi omaggi, doni o regalie, offrire o promettere vantaggi pecuniari o in natura al fine di influenzarne l'autonomia e il giudizio

1.3. Principi Operativi

Ai fini dell'attuazione delle regole e dei divieti sopra elencati, devono essere altresì osservati i principi operativi di seguito descritti, anche in accordo con l'apposita procedura adottata a livello *Corporate*, denominata "*Anti-bribery policy*", alla quale si fa rinvio.

In via generale, il gruppo Gerit è dotato di un apposito *Chief Compliance Officer* (CCO), al quale sono demandate una serie di funzioni, volte, innanzitutto, alla verifica del rispetto della *policy* in questione ed al quale dovranno essere segnalate eventuali condotte corruttive di cui i Destinatari siano venuti a conoscenza.

1.3.1. Rapporti diretti con la P.A.

Ogni soggetto che rappresenta la Società nei rapporti con la Pubblica Amministrazione dovrà essere stato a ciò espressamente delegato, con formale conferimento del relativo potere di rappresentanza.

Le deleghe in tal senso dovranno essere disposte:

- i) con atto del Consiglio di Amministrazione, con riferimento alle figure di vertice della Società (Amministratori);
- ii) con procura specifica, con riferimento ai dipendenti;
- iii) con specifica previsione nel relativo contratto di consulenza o di *partnership*, con riferimento a consulenti e *partners*.

I soggetti che intrattengono, per conto della Società, rapporti con la P.A., anche per una serie di attività ripetitive (ad esempio, i Dipendenti che curano gli adempimenti necessari al rilascio, ottenimento, rinnovo di licenze, concessioni, autorizzazioni, certificati) dovranno essere individuati e ricevere incarico specifico (eventualmente sulla base di apposito Mansionario).

1.3.2. Gestione degli omaggi

All'interno di Gerit S.r.l., è fatto divieto di:

- promettere o offrire denaro, benefici, promesse di favori o altre utilità, anche se indirettamente o per tramite di interposta persona, a soggetti appartenenti alla Pubblica Amministrazione o a soci in affari, a loro parenti o a persone a loro collegate e/o segnalate e/o ai terzi in generale, al fine di ottenere, anche implicitamente, trattamenti di favore per sé o per l'Organizzazione;
- accettare qualsiasi forma di regalo o beneficio, dono, pagamento, omaggio, a qualsivoglia titolo, che possa essere interpretata come eccedente le normali pratiche commerciali o di cortesia, o che sia rivolta ad acquisire trattamenti di favore nell'adozione di decisioni o conduzione di qualsiasi attività legata o inerente all'organizzazione, fatto salvo regali e omaggi di carattere puramente simbolico e, comunque, di modesto valore economico (ad es. omaggi promozionali di esiguo valore);
- le proposte di concessione a favore di terzi di regali, omaggi, ospitalità e liberalità devono essere limitate nel tempo e atte a promuovere iniziative di carattere culturale, sportivo e umanitario o il brand aziendale.

In ogni caso, non è mai ammessa la concessione di regali, omaggi, intrattenimenti o liberalità:

- in denaro contante, prestiti, azioni (di qualsiasi valore);
- per ricevere in cambio una controprestazione analoga (di qualsiasi valore);
- che non abbia un carattere di ragionevolezza in considerazione del luogo, settore dell'attività, donatore e del beneficiario;
- che non rispetti la presenza di divieti o controlli in essere all'interno di luoghi o organizzazioni;
- che comprometta l'integrità e/o la reputazione di una delle parti tali da poter essere interpretati, da un osservatore imparziale, come un obbligo di gratitudine e/o un atto per acquisire vantaggi in modo improprio;
- prima, durante e dopo una gara o la negoziazione di un contratto (di qualsiasi valore).

Per il personale di Gerit S.r.l., non è mai ammissibile accettare regali, omaggi, ospitalità e liberalità, a maggior ragione se in denaro contante, prestiti, azioni (di qualsiasi valore), che possano essere percepiti come atti corruttivi. In particolare, non possono essere accettati da nessun cliente o altro partner commerciale di Gerit:

- gli omaggi di valore superiore ai 100,00 euro;
- liberalità (di qualsiasi valore);
- pranzi, cene ed intrattenimenti di lavoro che non siano ragionevoli e che appaiano eccessivi.

Eventuali donazioni da effettuarsi da parte o per conto di Gerit e che sono consentite in conformità a quanto sopra indicato, devono essere mosse da spirito liberale, al fine di promuovere l'immagine di Gerit S.r.l. in ambito sociale, sportivo, dell'arte, della cultura.

I dirigenti, i funzionari e i dipendenti possono fare una donazione a un ente di beneficenza di loro scelta per conto e/o a nome della Società, a condizione che:

- l'importo della donazione non sia tale da influenzare taluno;
- l'ente di beneficenza sia chiaramente identificabile;
- la donazione sia destinata a scopi caritatevoli appropriati;
- la donazione non sia utilizzata direttamente o indirettamente per benefici personali da una persona associata all'ente;
- non offuschi l'immagine di Gerit come società indipendente;
- non violi leggi, regolamenti o politiche di Gerit.

Lo scopo della donazione, il processo di *due diligence* dell'ente e il pagamento stesso devono essere accuratamente documentati.

1.3.3. Sponsorizzazioni

Le richieste di sponsorizzazioni devono provenire direttamente dalla Società o dall'ente beneficiario e devono essere sottoscritte dal Legale Rappresentante o da altro soggetto delegato e contenere informazioni esaurienti circa la natura della sponsorizzazione.

Tutte le informazioni necessarie sono trasmesse al soggetto a ciò preposto il quale verifica: i) la credibilità, serietà e integrità morale dell'ente beneficiario; ii) la documentabilità dell'iniziativa; iii) la validità dell'oggetto e degli scopi della sponsorizzazione.

Se l'attività di *due diligence* avrà esito positivo o, comunque, non emergeranno particolari rilievi, le richieste saranno sottoposte alla Direzione per l'approvazione. La Direzione, acquisite le necessarie informazioni, valuta le richieste ricevute verificando:

- la coerenza dell'iniziativa;
- la congruità del valore della richiesta rispetto alla destinazione d'uso dichiarata.

1.3.4. Partecipazione a gare d'appalto

Per la partecipazione a gare indette da enti pubblici, Gerit S.r.l. si dota di un'apposita procedura che, oltre a definire in modo chiaro ruoli e responsabilità dei soggetti coinvolti nel processo, si ispira ai seguenti principi:

- definizione delle responsabilità dei soggetti coinvolti nella gestione delle gare pubbliche nel rispetto del principio della segregazione delle funzioni. In particolare, sono individuati i soggetti che intervengono nelle seguenti e distinte fasi: i) decisione di partecipazione alla gara; ii) raccolta e/o predisposizione di documentazione necessaria; iii) verifica della documentazione definitiva; iv) sottoscrizione della documentazione da parte del legale rappresentante/soggetto dotato di potere di firma; v) trasmissione della documentazione; vi) partecipazione alla fase di aggiudicazione;
- obbligo di assoluta riservatezza sulla partecipazione alla gara e sull'*iter* della stessa;
- formalizzazione della fase di verifica del possesso dei requisiti indicati nel bando di gara;
- chiara individuazione del soggetto responsabile del controllo della completezza e correttezza della documentazione da inviarsi all'Ente appaltante per la partecipazione alla gara;
- evidenza dell'approvazione della documentazione;

- controllo formale di conformità delle condizioni e dei termini della delibera di aggiudicazione a quanto previsto in fase di approvazione delle offerte;
- corretta e sistematica archiviazione di tutta la documentazione di cui sopra.

I medesimi principi, in quanto compatibili, dovranno essere scrupolosamente osservati anche in caso di partecipazione a "gare" indette da soggetti privati.

1.3.5. Rapporti con le terze parti

I principi operativi sopra descritti devono essere rispettati anche dalle terze parti con le quali Gerit stipuli un contratto. Le stesse, prima di procedere alla conclusione del contratto medesimo, devono essere sottoposte ad apposita *due diligence*.

Come riportato nella procedura adottata a livello *Corporate*, denominata "*Anti-bribery policy*", esempi di segnali di allarme per quanto riguarda i rapporti con i terzi sono i seguenti:

- la terza parte è collegata ad un funzionario governativo che potrebbe influenzare la decisione di accettare o meno una proposta di Gerit;
- in passato la terza parte ha richiesto fatture false o qualsiasi altro tipo di documentazione falsa;
- la terza parte ha avanzato richieste di sovrappagamento o tutta o parte della commissione è stata pagata in un paese terzo, a una terza parte, in contanti o in fondi non tracciabili;
- la terza parte si rifiuta di collaborare o di accettare per iscritto di seguire misure anticorruzione adeguate;
- la struttura e le operazioni della terza parte indicano il ricorso a pratiche di corruzione.

1.3.6. Accessi, ispezioni e verifiche

Ogni contatto con la Pubblica Amministrazione in fase di accessi, ispezioni e/o verifiche dovrà svolgersi alla presenza di almeno due dipendenti della Società.

Il Responsabile della Funzione interessata all'accesso, ispezione e/o verifica, qualora non sussistano procedure che individuino i soggetti incaricati di intrattenere i rapporti con Pubblici Ufficiali all'interno della Direzione, fornisce di volta in volta indicazioni circa le modalità con cui dovranno avvenire i contatti con i Pubblici Ufficiali, individuando i nominativi dei dipendenti che dovranno interagire con detti Pubblici Ufficiali ed incaricandoli.

Al termine dell'incontro/accesso dovrà essere redatto apposito *report* di sintesi che, nei casi di particolare importanza, sarà trasmesso all'Organismo di Vigilanza.

1.3.7. Finanziamenti pubblici (o altre agevolazioni)

Al fine di scongiurare la commissione dei reati connessi alla richiesta di finanziamenti pubblici e fatta salva l'applicazione delle procedure interne specificamente adottate, in via preliminare sono attuati i seguenti sistemi di controllo:

- dichiarazioni, documentazione ed ogni altro atto fornito ad autorità od organismi pubblici (nazionali o esteri) e/o istituti bancari o finanziari ai fini dell'ottenimento di contributi e/o finanziamenti, mutui ed ogni altra sovvenzione devono: a) essere veritieri e non contenere elementi falsi od alterati; b) essere completi e non omettere alcuna informazione dovuta; c) contenere l'impegno della Società, in caso di ottenimento dei benefici, all'effettiva

utilizzazione delle erogazioni ottenute, secondo le finalità previste dalla specifica normativa di riferimento;

- deve essere previsto l'intervento di operatori diversi nelle seguenti fasi/attività del processo:
a) redazione e presentazione della domanda finalizzata all'erogazione del contributo, del finanziamento o della sovvenzione alla Pubblica Amministrazione competente; b) controllo della correttezza e veridicità della documentazione presentata; c) realizzazione dell'attività oggetto di finanziamento; d) predisposizione dei rendiconti relativi alla gestione dei finanziamenti ottenuti;
- deve essere formalmente identificato il soggetto deputato ad intrattenere rapporti con la Pubblica Amministrazione in relazione a ciascuna operazione relativa alla richiesta e gestione di erogazioni pubbliche;

I sistemi di controllo descritti, in quanto compatibili e con ogni opportuno adattamento, devono essere applicati anche nei processi relativi all'ottenimento di finanziamenti in forma di crediti d'imposta e/o agevolazioni fiscali o contributive di vario tipo.

1.4. Controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività che implicano rapporti con la Pubblica Amministrazione, al fine di verificare il rispetto delle regole di cui alla presente Parte Speciale e delle procedure interne.

Quanto alla reportistica verso l'Organismo di Vigilanza, si segnalano:

A. Reportistica periodica:

Elenco delle comunicazioni inviate /ricevute a/da Autorità pubbliche (con cadenza semestrale)

B. Reportistica specifica/ad evento:

- anomalie specifiche e significative che possano riguardare direttamente o indirettamente la violazione delle procedure e i presidi aziendali;
- modifiche nelle procedure e prassi operative relative alla partecipazione alle gare d'appalto e, in genere, ai rapporti con la P.A.

In caso di accessi, verifiche o ispezioni da parte di Autorità Pubbliche (ASL, VVFF, INPS, INAL, Ispettorato del Lavoro, Guardia di Finanza ecc.), l'O.d.V. deve essere informato, al momento dell'accesso, dell'andamento della verifica/ispezione e gli deve essere consegnato il *report* redatto.

In generale, l'O.d.V. deve essere informato con nota scritta di qualunque criticità o conflitto di interesse che dovesse sorgere nell'ambito dei rapporti con la P.A.

1.5. Rinvio alle Procedure e Istruzioni operative

Di seguito si rinvia alle Procedure e Istruzioni operative aziendali predisposte da Gerit S.r.l. per la prevenzione dei reati nei rapporti con la Pubblica Amministrazione:

- *Gerit's Code of Conduct*;
- *Gerit's Anti-Bribery Policy*;
- Codice Etico;
- Procedura per la gestione dei rapporti con la P.A.;
- Procedura per la gestione delle visite ispettive;
- Procedura per la gestione del personale.

CAPITOLO II

Reati societari

2.1. Premessa

Il presente Capitolo prende in considerazione i Reati che possono essere commessi dai Destinatari del Modello nell'ambito delle attività sensibili, in particolare previsti dall'art. 25 *ter* ("Reati societari") del d.lgs. 231/2001.

Di seguito si riportano le fattispecie di reato previste dall'art. 25 *ter* ("Reati Societari") del Decreto.

- art. 2621 c.c.: False comunicazioni sociali
- art. 2621 *bis* c.c.: Fatti di lieve entità
- art. 2622 c.c.: False comunicazioni sociali delle società quotate
- art. 2625, comma 2, c.c.: Impedito controllo
- art. 2626 c.c.: Indebita restituzione dei conferimenti
- art. 2627 c.c.: Illegale ripartizione degli utili e delle riserve
- art. 2628 c.c.: Illecite operazioni sulle azioni o quote sociali o della società controllante
- art. 2629 c.c.: Operazioni in pregiudizio dei creditori
- art. 2629 *bis* c.c.: Omessa comunicazione del conflitto di interessi
- art. 2632 c.c.: Formazione fittizia del capitale
- art. 2633 c.c.: Indebita ripartizione dei beni sociali da parte dei liquidatori
- art. 2635, comma 3, c.c.: Corruzione tra privati
- art. 2635 *bis*, comma 1, c.c.: Istigazione alla corruzione tra privati
- art. 2636 c.c.: Illecita influenza sull'assemblea
- art. 2637 c.c.: Aggiotaggio
- art. 2638, commi 1 e 2, c.c.: Ostacolo all'esercizio delle autorità pubbliche di vigilanza
- art. 54 d.lgs. 19/2023: False o omesse dichiarazioni per il rilascio del certificato preliminare

In linea generale, i Destinatari del Modello, al fine di prevenire la commissione dei predetti Reati, devono conformarsi alla normativa vigente, al Codice Etico, ai valori e alle politiche della Società e alle regole contenute nel presente Modello.

Inoltre, l'organizzazione della Società deve rispettare i principi fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative, di tracciabilità delle operazioni.

2.2. Principi Generali di Comportamento

I Destinatari del Modello, nello svolgimento di tutte le operazioni relative alla gestione sociale, dovranno attenersi ai seguenti principi generali di comportamento:

- a) osservare tutte le regole e i principi contenuti nel presente Modello, nel Codice Etico, in leggi, regolamenti, protocolli e procedure interne che disciplinano l'operatività aziendale, con particolare riferimento alle attività societarie e di redazione dei bilanci, delle relazioni e delle altre comunicazioni sociali previste dalla legge;
- b) astenersi dal porre in essere, collaborare o contribuire alla realizzazione di comportamenti che, in tutto o in parte, possano integrare, direttamente o indirettamente, le ipotesi di reato

di cui agli artt. 25 *bis-1*, 25 *ter*, 25 *octies* del Decreto o possano semplicemente agevolare la commissione;

- c) con riguardo al bilancio e alle scritture contabili, tenere un comportamento corretto e trasparente, assicurando il pieno rispetto di leggi e regolamenti, nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle scritture contabili periodiche e delle altre comunicazioni sociali, al fine di fornire ai soci ed al pubblico in generale un'informazione veritiera e appropriata sulla situazione economica, patrimoniale e finanziaria della Società;
- d) garantire la veridicità delle informazioni relative alla situazione economica, patrimoniale e finanziaria della società;
- e) con riguardo ai rapporti con creditori o terzi, osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale e agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere. In particolare, è fatto divieto di: i) restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale; ii) ripartire utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve (anche non costituite con utili) che non possono per legge essere distribuite; iii) acquistare o sottoscrivere azioni della Società fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge; iv) effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori; v) procedere in ogni modo a formazione o aumento fittizi del capitale sociale; vi) ripartire i beni sociali tra i soci – in fase di liquidazione – prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli;
- f) assicurare il regolare funzionamento della Società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge nonché la libera e corretta formazione della volontà assembleare;
- g) effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza;
- h) dare notizia agli altri amministratori di ogni interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata; se si tratta dell'Amministratore Delegato, deve altresì astenersi dal compiere tali operazioni, notiziando della questione l'Organismo di Vigilanza della Società;
- i) con riguardo ai rapporti con le Autorità di Vigilanza (ad es. Autorità Garante della concorrenza e del mercato), effettuare con tempestività, correttezza e completezza tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità medesime, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate. In merito è fatto divieto di: i) omettere di effettuare, con la dovuta chiarezza, completezza e tempestività, nei confronti delle Autorità interessate, tutte le comunicazioni, periodiche e non, previste dalla legge e dalla ulteriore normativa di settore, nonché la trasmissione dei dati e documenti previsti dalle norme in vigore e/o specificamente richiesti dalle predette Autorità; ii) esporre in tali comunicazioni e nella documentazione trasmessa fatti non

rispondenti al vero oppure occultare fatti concernenti la situazione economica, patrimoniale o finanziaria della Società;

- j) con riguardo ai rapporti con i terzi, fermo restando quanto espressamente previsto dalle procedure aziendali in materia di omaggi e spese di rappresentanza, è vietato: i) effettuare elargizioni in danaro o sotto forma di omaggi o agevolazioni di qualsiasi tipo a qualsiasi soggetto privato, da intendersi quale qualsiasi soggetto (ad es. amministratori, direttori generali, dirigenti, dipendenti, collaboratori, consulenti, ecc. o loro familiari) facente capo o riconducibile ad enti privati (società, enti, associazioni, ecc.); ii) consegnare, distribuire, promettere o garantire omaggi, ogni forma di regali, sconti, vantaggi ed ogni altra agevolazione a soggetti privati, anche se non finalizzati ad ottenere trattamenti di favore. iii) accordare, promettere o paventare la possibilità di ottenere altri vantaggi di qualsiasi natura in favore di soggetti privati che possano influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda.

In particolare, vi è il divieto di porre in essere le seguenti condotte:

- k) compiere operazioni simulate o diffondere notizie false sulla Società;
- l) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società;
- m) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- n) pubblicare o divulgare notizie false, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento od ingannatorio, aventi ad oggetto la situazione economica, finanziaria, patrimoniale della Società;
- o) porre in essere operazioni in pregiudizio dei soci, creditori o di terzi;
- p) porre in essere operazioni che palesino conflitti di interessi;
- q) ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- r) effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- s) procedere a formazione o aumento fittizio del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale.

2.3. Principi Operativi

Ai fini dell'attuazione delle regole e dei divieti sopra elencati, devono essere altresì osservati i principi operativi di seguito descritti.

2.3.1. Predisposizione del bilancio e di altri documenti destinati a terzi

Tutti i Destinatari coinvolti nelle attività di formazione del bilancio e delle altre scritture contabili, devono attenersi ai seguenti principi comportamentali: i) completezza e chiarezza delle informazioni fornite; ii) accuratezza dei dati e delle elaborazioni; iii) segnalazione di conflitti di interesse.

Le procedure aziendali devono prevedere “meccanismi” di controllo idonei ad assicurare che le comunicazioni periodiche ai terzi siano redatte con il contributo di tutte le funzioni aziendali interessate al fine di assicurare la correttezza del risultato e la condivisione dello stesso. Tali meccanismi garantiscono che le attività relative al processo siano effettuate rispettando la separazione dei ruoli tra chi effettua le registrazioni contabili e chi effettua i controlli sulle stesse; che il sistema contabile permetta la tracciabilità di tutte le operazioni e l'identificazione dell'operatore che le ha effettuate, tracciabilità che può essere garantita anche tramite il sistema informatico.

2.3.2. Operazioni contabili

Nello svolgimento delle attività contabili, nonché nella registrazione delle relative operazioni, devono essere rispettati i principi di correttezza, completezza e veridicità enunciati dal Codice Etico e dal presente Modello, e non devono esser posti in essere comportamenti riconducibili alle seguenti fattispecie: i) mancata contabilizzazione di ricavi, con conseguente sopravvalutazione delle rimanenze a fine esercizio; ii) registrazione di fatture non supportate da riscontri documentali o idonei giustificativi od autorizzazioni al pagamento; iii) realizzazione di sospesi di cassa; iv) gestione e pagamento di note spese prive di documentazione giustificativa.

2.3.3. Operazioni relative al capitale sociale

Al fine di evitare che gli Amministratori possano porre in essere condotte tali da integrare i reati di formazione fittizia del capitale (art. 2632 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.) e operazioni in pregiudizio dei creditori (art. 2629 c.c.), è necessario attenersi a quanto previsto dal presente Modello e dal Codice Etico, oltre che dalle procedure aziendali.

In particolare: i) deve essere garantita la tracciabilità di tutte le attività svolte (es. stime, perizie) e delle decisioni assunte ed i responsabili delle funzioni coinvolte devono controllarne ogni singola fase; ii) l'Organismo di Vigilanza potrà e dovrà ricevere notizia ed in ogni caso accedere a tutta la documentazione relativa a qualsiasi operazione relativa al capitale sociale.

2.4. Operazioni e/o transazioni tra privati

Tutti i Destinatari coinvolti nelle operazioni e/o transazioni tra privati devono attenersi ai seguenti principi comportamentali: i) completezza e chiarezza delle informazioni fornite; ii) accuratezza dei dati e delle elaborazioni; iii) segnalazione di conflitti di interesse.

Inoltre, le operazioni e/o transazioni tra privati devono essere legittime, autorizzate, coerenti, documentate e verificabili in ogni momento.

In particolare, con riferimento alle attività di gestione dei rapporti con i fornitori, la Società si conforma ai seguenti principi di controllo:

- prevedere una fase di preventiva qualifica/*due diligence* dei fornitori, che garantisca la piena conoscibilità della propria controparte contrattuale (si tratta di una fase volta a raccogliere tutte le informazioni anagrafiche, “etiche” e di solidità economico-finanziaria della controparte, improntata alla massima trasparenza);
- verificare periodicamente l'aggiornamento dell'anagrafica dei clienti e dei fornitori, al fine di controllarne l'effettiva esistenza ed operatività;

- definire delle modalità e dei criteri per la valutazione delle offerte ricevute improntati alla trasparenza e, per quanto possibile, alla limitazione di criteri di soggettività;

In particolare, nei rapporti con i fornitori, è espressamente vietato:

- assegnare incarichi di fornitura, consulenza e prestazione professionale a persone o società prive dei necessari requisiti di idoneità tecnico-professionale;
- avvalersi di fornitori che, in relazione ai propri dipendenti: i) li sottopongano a condizioni di sfruttamento e/o approfittino dello stato di bisogno degli stessi; ii) corrispondano agli stessi retribuzioni in modo significativamente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale maggiormente applicati al settore di appartenenza della Società, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato; iii) violino la normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie; iv) violino le norme in materia di salute e sicurezza nei luoghi di lavoro; v) li sottopongano a condizioni di lavoro, metodi di sorveglianza o a situazioni alloggiative degradanti; vi) assumano lavoratori extracomunitari privi del permesso di soggiorno o con permesso di soggiorno scaduto e non rinnovato, revocato, annullato o favoriscano in qualsiasi modo la permanenza, nel territorio nazionale, di soggetti introdotti in violazione delle disposizioni del Testo Unico Immigrazione (d. lgs. 286/1998).

2.5. Controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività sensibili, al fine di verificare il rispetto delle regole di cui alla presente Parte Speciale e delle procedure interne.

Quanto alla reportistica verso l'Organismo di Vigilanza, si segnalano:

A. Reportistica periodica

Trasmissione all'O.d.V. del progetto di bilancio approvato (con cadenza annuale)

B. Reportistica specifica/ad evento:

- mancata approvazione del bilancio nei termini di legge;
- accessi, verifiche, ispezioni da parte di Autorità pubbliche di vigilanza;
- invio della bozza del bilancio e della relazione della società di revisione.

2.6. Rinvio alle Procedure e Istruzioni operative

Di seguito si rinvia alle Procedure e Istruzioni operative aziendali predisposte da Gerit S.r.l. per la prevenzione dei reati trattati nella presente sezione della Parte Speciale:

- *Gerit's Code of Conduct*;
- Codice Etico;
- Procedura per la verifica della gestione degli adempimenti societari generali, formazione del bilancio;
- Procedura per la gestione della crisi d'impresa.

CAPITOLO III

Reati contro le frodi in commercio e reati patrimoniali

3.1. Premessa

Il presente Capitolo prende in considerazione i Reati che possono essere commessi dai Destinatari del Modello nell'ambito delle attività sensibili, in particolare previsti dagli artt. 25 *bis-1* ("*Delitti contro l'industria e il commercio*") e 25 *octies* ("*Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio*") del d.lgs. 231/2001.

Di seguito si riportano le fattispecie di reato previste dall'art. 25 *bis-1* del Decreto ("*Delitti contro l'industria e il commercio*"):

- art. 513 c.p.: Turbata libertà dell'industria o del commercio
- art. 513 *bis* c.p.: Illecita concorrenza con minaccia o violenza
- art. 514 c.p.: Frodi contro le industrie nazionali
- art. 515 c.p.: Frode nell'esercizio del commercio
- art. 516 c.p.: Vendita di sostanze alimentari non genuine come genuine
- art. 517 c.p.: Vendita di prodotti industriali con segni mendaci
- art. 517 *ter* c.p.: Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale
- art. 517 *quater* c.p.: Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari

Di seguito si riportano anche le fattispecie di reato previste dall'art. 25 *octies* ("*Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio*") del Decreto:

- art. 648 c.p.: Ricettazione
- art. 648 *bis* c.p.: Riciclaggio
- art. 648 *ter* c.p.: Impiego di denaro, beni o utilità di provenienza illecita
- art. 648 *ter*. 1 c.p.: Autoriciclaggio

In linea generale, i Destinatari del Modello, al fine di prevenire la commissione dei predetti Reati, devono conformarsi alla normativa vigente, al Codice Etico, ai valori e alle politiche della Società e alle regole contenute nel presente Modello.

Inoltre, l'organizzazione della Società deve rispettare i principi fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative, di tracciabilità delle operazioni.

3.2. Principi Generali di Comportamento

Con particolare riferimento ai reati di cui all'art. 25 *bis-1* ("*Delitti contro l'industria e il commercio*"), ai Destinatari è richiesto di:

- osservare regole e principi del Codice Etico;

- osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività connesse al processo di produzione e/o di erogazione del servizio;
- garantire elevati standard qualitativi nello svolgimento delle attività di competenza, nel rispetto della normativa posta a tutela della concorrenza e del mercato.

È fatto esplicito divieto di:

- porre in essere comportamenti che possano integrare, direttamente o indirettamente, una delle fattispecie di reato *ex artt. 25 bis-1* del d.lgs. 231/2001;
- porre in essere comportamenti in violazione del Codice Etico, delle norme comportamentali e delle procedure aziendali.

Con particolare riferimento ai reati di cui all'art. 25 *octies* ("*Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio*") ai Destinatari è richiesto di:

- osservare regole e principi del Codice Etico;
- osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano la gestione delle risorse e dei flussi finanziari e di tesoreria;

È fatto esplicito divieto di:

- porre in essere comportamenti che possano integrare, direttamente o indirettamente, una delle fattispecie di reato *ex art. 25 octies* del d.lgs. 231/2001;
- porre in essere comportamenti in violazione del Codice Etico, delle norme comportamentali e delle procedure aziendali.

3.3 Principi Operativi

Ai fini dell'attuazione delle regole sopra elencate, devono essere altresì osservati, con riferimento ai reati di cui all'art. 25 *bis-1* ("*Delitti contro l'industria e il commercio*"), i principi operativi di seguito descritti:

- fornire informazioni veritiere, precise ed esaurienti circa l'origine e la qualità dei prodotti posti in vendita;
- garantire che siano definiti i requisiti dei prodotti destinati alla vendita;
- verificare la veridicità e correttezza della documentazione a supporto dei controlli effettuati e garantirne l'archiviazione, anche per il tramite di specifici sistemi informativi.

È fatto esplicito divieto di:

- adoperare violenza sulle cose ovvero utilizzare mezzi fraudolenti per ostacolare l'attività industriale o commerciale altrui;
- perpetrare condotte idonee a cagionare nocumento alle industrie nazionali ponendo in vendita o mettendo in circolazione sui mercati nazionali o esteri, prodotti industriali con nomi, marchi o segni distintivi contraffatti o alterati;

- consegnare all'acquirente, nell'ambito e/o nell'esercizio di un'attività commerciale, una cosa mobile per un'altra ovvero una cosa mobile che per origine, provenienza, qualità o quantità è diversa rispetto a quella dichiarata o pattuita;
- vendere o mettere in circolazione opere d'ingegno o prodotti industriali recanti nomi, marchi o segni distintivi che possano trarre in inganno il compratore sull'origine, provenienza o qualità del prodotto;
- fabbricare o adoperare per fini industriali beni realizzati usurpando o violando il titolo di proprietà industriale, nonché cercare di trarre profitto dai beni stessi introducendoli nel territorio dello Stato, detenendoli e/o ponendoli in vendita o mettendoli comunque in circolazione;
- porre in essere, nell'esercizio di un'attività industriale, commerciale o comunque produttiva, atti di concorrenza sleale anche facendo ricorso alla violenza o alla minaccia.

Con riferimento ai reati di cui all'art. 25 *octies* ("*Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio*") devono essere osservati i principi operativi di seguito descritti:

- instaurare e mantenere qualsiasi rapporto con gli istituti di credito sulla base di criteri di massima correttezza e trasparenza;
- verificare la regolarità formale e sostanziale dei flussi finanziari aziendali, in particolare verso terzi. Tali controlli devono tener conto della sede legale della controparte (per es. paradisi fiscali e Paesi a rischio terrorismo), degli istituti di credito utilizzati e di eventuali strutture fiduciarie coinvolte nella transazione;
- verificare l'esistenza di regole disciplinari in materia di prevenzione dei reati di riciclaggio;
- verificare la trasparenza e tracciabilità degli investimenti;
- predisporre o realizzare adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio;
- attenersi ai principi e alle prescrizioni contenuti nelle istruzioni interne;
- osservare scrupolosamente tutte le norme volte al mantenimento dell'integrità del capitale sociale e agire sempre rispettando le procedure interne che su tali norme si fondano al fine di non ledere gli interessi dei soci, dei creditori e dei terzi;
- redigere per iscritto gli incarichi conferiti a consulenti, indicando le motivazioni alla base del rapporto instaurato e il compenso pattuito;
- effettuare pagamenti o riconoscere compensi a favore di soggetti terzi che operino per conto della Società, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- redigere per iscritto i contratti stipulati con i fornitori e i partners, specificando tanto le motivazioni alla base del rapporto quanto le condizioni economiche accordate.

3.4. Controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività sensibili, al fine di verificare il rispetto delle regole di cui alla presente Parte Speciale e delle procedure interne.

Quanto alla reportistica verso l'Organismo di Vigilanza, si segnala:

A. Reportistica specifica/ad evento:

Trasmissione all'O.d.V. di eventuali segnalazioni di:

- flussi finanziari aziendali anomali;
- condotte in violazione della tutela della concorrenza e del mercato.

3.5. [Rinvio alle Procedure e Istruzioni operative](#)

Di seguito si rinvia alle Procedure e Istruzioni operative aziendali predisposte da Gerit S.r.l. per la prevenzione dei reati trattati nella presente sezione della Parte Speciale:

- Gerit's Code of Conduct;
- Codice Etico;
- Procedura per la verifica della gestione degli adempimenti societari generali, formazione del bilancio.

CAPITOLO IV

Reati in materia di sicurezza sul lavoro

4.1. Premessa

Il presente Capitolo prende in considerazione i Reati che possono essere commessi dai Destinatari del Modello nell'ambito delle attività sensibili, previsti dall'art. 25 *septies* ("*Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro*") del d.lgs. n. 231/2001.

Di seguito si riportano le fattispecie di reato previste dall'art. 25 *septies* del Decreto ("*Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro*"):

- art. 589 c.p.: Omicidio colposo
- art. 590 c.p.: Lesioni personali colpose

Per quanto riguarda la disciplina in materia antinfortunistica, nello specifico, è richiesta l'osservanza delle norme del d.lgs. n. 81/2008 (c.d. Testo Unico Sicurezza Lavoro) e dell'art. 2087 c.c., laddove vengano omesse quelle misure e quegli accorgimenti tali da consentire una più efficace tutela della integrità fisica dei Lavoratori.

Destinatari del Modello, per quanto riguarda la sicurezza nei luoghi di lavoro, sono, in particolare, i soggetti di seguito indicati:

- **Lavoratore:** è la persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione di un Datore di Lavoro, pubblico o privato, anche al solo fine di apprendere un mestiere, un'arte, una professione, esclusi gli addetti ai servizi domestici e familiari;
- **Datore di Lavoro:** è il soggetto titolare del rapporto con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa, o dell'unità produttiva, in quanto esercita i poteri decisionali e di spesa;
- **Dirigente:** è la persona che, in ragione delle competenze professionali e di poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, attua le direttive del Datore di Lavoro organizzando l'attività lavorativa e vigilando su di essa;
- **Preposto:** è la persona che, in ragione delle competenze professionali e nei limiti di poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, sovrintende all'attività lavorativa e garantisce l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa.

4.2. Principi generali di Comportamento

Secondo le previsioni degli artt. 15 e 18 del d.lgs. n. 81/2008, al Datore di Lavoro, ai Dirigenti, ai Preposti e, più in generale, a tutti i Destinatari sui quali incombono specifiche responsabilità ai sensi delle procedure in materia di sicurezza e salute nei luoghi di lavoro adottate dalla Società, è fatto obbligo, nell'ambito delle rispettive attribuzioni e competenze, di:

- promuovere ed attuare ogni ragionevole iniziativa finalizzata a minimizzare i rischi e a rimuovere le cause che possono mettere a repentaglio la sicurezza e la salute dei Dipendenti e dei terzi che prestano la propria attività presso la Società;
- provvedere al costante e tempestivo adeguamento delle norme interne alla legislazione in materia di salute e sicurezza;
- sviluppare programmi di formazione (e di informazione) specifici sulle tematiche della salute e sicurezza;
- effettuare periodiche attività di controllo sull'effettiva applicazione delle procedure adottate in tema di tutela della salute e della sicurezza nei luoghi di lavoro;
- adottare specifiche politiche di selezione delle società esterne cui possono essere affidati appalti di lavori/servizi;
- promuovere e garantire, nella gestione di attività affidate in appalto a terzi, la cooperazione ed il coordinamento tra l'attività propria della Società e quella dell'impresa appaltatrice;
- garantire il rispetto della normativa in materia di organizzazione del lavoro, con particolare riferimento ai tempi di lavoro, di riposo giornaliero e settimanale del personale dipendente.

In particolare, per quanto riguarda, nello specifico, la figura del Datore di lavoro, non sono delegabili, ai sensi dell'art. 17, le seguenti attività: a) la valutazione di tutti i rischi con la conseguente elaborazione del documento ("DVR"); b) la designazione del Responsabile del Servizio di Prevenzione e Protezione dai rischi ("RSPP").

Gli obblighi specifici del Datore di Lavoro e dei Dirigenti, che organizzano e dirigono le stesse attività secondo le attribuzioni e competenze ad essi conferite, in forza di quanto stabilito dall'art. 18 del d.lgs. n. 81/2008, sono:

- nominare il medico competente per l'effettuazione delle attività di sorveglianza sanitaria nei casi previsti dalla legge (*lettera a*);
- designare preventivamente i lavoratori incaricati di attuare le misure di prevenzione incendi e lotta anti-incendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave ed immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza (*lettera b*);
- individuare il preposto o i preposti per l'effettuazione delle attività di vigilanza di cui all'art. 19 (*lettera b-bis*);
- nell'affidare i compiti ai lavoratori, tenere conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute e alla sicurezza (*lettera c*);
- fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale, sentito il responsabile del servizio di prevenzione e protezione e il medico competente, ove presente (*lettera d*);
- prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico (*lettera e*);

- richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione (*lettera f*);
- inviare i lavoratori alla visita medica entro le scadenze previste dal programma di sorveglianza sanitaria e richiedere al medico competente l'osservanza degli obblighi previsti a suo carico (*lettera g*);
- nei casi di sorveglianza sanitaria, comunicare tempestivamente al medico competente la cessazione del rapporto di lavoro (*lettera g bis*);
- adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa (*lettera h*);
- informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione (*lettera i*);
- adempiere agli obblighi di informazione, formazione e addestramento di cui agli artt. 36 e 37 (*lettera l*);
- astenersi, salvo eccezione debitamente motivata da esigenze di tutela della salute e sicurezza, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave e immediato (*lettera m*);
- consentire ai lavoratori di verificare, mediante il rappresentante dei lavoratori per la sicurezza, l'applicazione delle misure di sicurezza e di protezione della salute (*lettera n*);
- consegnare tempestivamente al rappresentante dei lavoratori per la sicurezza, su richiesta di questi e per l'espletamento della sua funzione, copia del documento di valutazione dei rischi (DVR), anche su supporto informatico come previsto, nonché consentire al medesimo rappresentante di accedere ai dati di cui alla lettera r (*lettera o*);
- in caso di appalto o affidamento a terzi di lavori di qualsiasi natura all'interno dell'azienda, procedere alla elaborazione del documento di cui all'art. 26, comma terzo, d.lgs. n. 81/2008, tenendolo a disposizione della/e figura/e di *Rappresentante dei Lavoratori per la Sicurezza* (anche "RLS") e, più in generale, curare tutti gli adempimenti previsti dalla legge in relazione a tale fattispecie (*lettera p*);
- prendere appropriati provvedimenti per evitare che le misure tecniche adottate possano causare rischi per la salute della popolazione o deteriorare l'ambiente esterno verificando periodicamente la perdurante assenza di rischio (*lettera q*);
- eseguire tutte le comunicazioni previste dalla legge, in particolare ad INAIL ed IPSEMA e/o ad eventuali ulteriori enti o autorità pubbliche, anche su richiesta degli stessi (*lettera r*);
- consultare il rappresentante dei lavoratori per la sicurezza nelle ipotesi previste per legge (*lettera s*);

- adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro, nonché per il caso di pericolo grave e immediato, secondo le disposizioni di legge (*lettera f*);
- nell'ambito dello svolgimento di attività in regime di appalto e di subappalto, munire i lavoratori di apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro (*lettera u*);
- nelle unità produttive con più di 15 lavoratori, convocare la riunione periodica di cui all'art. 35 (*lettera v*);
- aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione (*lettera z*);
- comunicare in via telematica all'INAIL e all'IPSEMA, nonché per loro tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro, in caso di nuova elezione o designazione, i nominativi dei rappresentanti dei lavoratori per la sicurezza; in fase di prima applicazione l'obbligo di cui alla presente lettera riguarda i nominativi dei rappresentanti dei lavoratori già eletti o designati (*lettera aa*);
- vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità (*lettera bb*);
- fornire al Servizio di Prevenzione e Protezione ed al Medico Competente informazioni in merito ai seguenti aspetti: i) natura dei rischi; ii) organizzazione del lavoro; programmazione ed attuazione delle misure preventive; descrizione degli impianti e dei processi produttivi; iii) dati di infortunio rilevanti *ex art. 18, comma primo, lettera r*) del d.lgs. n. 81/2008 e dati relativi alle malattie professionali; iv) provvedimenti adottati dagli organi di vigilanza (*comma 1f*);
- vigilare in ordine all'adempimento degli obblighi di cui agli artt. 19 (Obblighi del preposto), 20 (Obblighi dei lavoratori), 22 (Obblighi dei progettisti), 23 (Obblighi dei fabbricanti e dei fornitori), 24 (Obblighi degli installatori) e 25 (Obblighi del medico competente) del d.lgs. n. 81/2008, ferma restando l'esclusiva responsabilità dei soggetti obbligati ai sensi dei medesimi articoli, qualora la mancata attuazione dei predetti obblighi sia addebitabile unicamente agli stessi e non sia riscontrabile un difetto di vigilanza del Datore di Lavoro e dei Dirigenti (*comma 3-bis*).

Con riferimento ai preposti, sono a loro carico, secondo le competenze loro attribuite, i seguenti obblighi (art. 19 d.lgs. 81/2008):

- sovrintendere e vigilare sull'osservanza da parte dei singoli lavoratori dei loro obblighi di legge, nonché delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messi a loro disposizione e, in caso di rilevazione di comportamenti non conformi alle disposizioni e istruzioni impartite dal Datore di lavoro e dai Dirigenti ai fini della protezione collettiva e individuale, intervenire per modificare il comportamento non conforme fornendo le necessarie indicazioni di sicurezza. In caso di mancata attuazione delle disposizioni impartite o di persistenza dell'inosservanza, interrompere l'attività del lavoratore e informare i superiori diretti (*lettera a*);

- verificare affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico (*lettera b*);
- richiedere l'osservanza delle misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato e inevitabile, abbandonino il posto di lavoro o la zona pericolosa (*lettera c*);
- informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione (*lettera d*);
- astenersi, salvo eccezioni debitamente motivate, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave ed immediato (*lettera e*);
- segnalare tempestivamente al datore di lavoro o al dirigente sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro, delle quali venga a conoscenza sulla base della formazione ricevuta (*lettera f*);
- in caso di rilevazione di deficienze dei mezzi e delle attrezzature di lavoro e di ogni condizione di pericolo rilevata durante la vigilanza, se necessario, interrompere temporaneamente l'attività e, comunque, segnalare tempestivamente al datore di lavoro e al dirigente le non conformità rilevate (*lettera f bis*);
- frequentare appositi corsi di formazione secondo quanto previsto dall'art. 37 (*lettera g*).

Quanto ai Lavoratori, ai sensi dell'art. 20 d.lgs. 81/2008, gli stessi devono prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle loro azioni o omissioni, conformemente alla loro formazione, alle istruzioni e ai mezzi forniti dal datore di lavoro.

Nello specifico, i Lavoratori devono:

- contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro (*lettera a*);
- osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale (*lettera b*);
- utilizzare correttamente le attrezzature di lavoro, le sostanze e le miscele pericolose, i mezzi di trasporto, nonché i dispositivi di sicurezza (*lettera c*);
- utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione (*lettera d*);
- segnalare immediatamente al Datore di lavoro, al Dirigente o al Preposto le deficienze dei mezzi e dei dispositivi di cui alle lettere *c*) e *d*), nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla lettera *f*) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al Rappresentante dei lavoratori per la sicurezza (*lettera e*);

- non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo (*lettera f*);
- non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori (*lettera g*);
- partecipare ai programmi di formazione e di addestramento organizzati dal datore di lavoro (*lettera h*);
- sottoporsi ai controlli sanitari previsti dal presente decreto legislativo o comunque disposti dal medico competente (*lettera i*).

Allo scopo di conseguire gli obiettivi prefissati e descritti nel presente paragrafo, la Società, in particolare, assicura:

- un'organizzazione delle risorse umane aziendali in termini di competenze individuali, autonomia decisionale e relative responsabilità;
- risorse necessarie per realizzare gli interventi tecnici, organizzativi e gestionali atti a conseguire l'obiettivo di miglioramento continuo del livello di sicurezza;
- informazione, formazione dei Dipendenti per promuoverne la responsabilizzazione e consapevolezza in materia di sicurezza e salute;
- sensibilizzazione dei fornitori e dei collaboratori esterni in genere, affinché adottino idonei comportamenti in materia di sicurezza e salute coerenti con il presente Modello;
- prevenzione e minimizzazione dei rischi per la salute e la sicurezza personale nei confronti dei Dipendenti, dei Collaboratori e dei clienti;
- sviluppo e continua ottimizzazione dei processi produttivi;
- progettazione o modifica degli impianti in modo da garantirne la compatibilità con la tutela della sicurezza, della salute e dell'ambiente;
- sorveglianza e verifica, al fine di controllare la realizzazione della politica aziendale in materia di sicurezza e salute nei luoghi di lavoro.

4.3. Principi Operativi

Ai sensi dell'art. 30 del d.lgs. n. 81/2008, il Modello di Organizzazione e Gestione idoneo ad avere efficacia esimente della responsabilità da reato dell'ente deve essere adottato ed efficacemente attuato, assicurando un Sistema Aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

- a) al rispetto degli *standard* tecnico-strutturali di legge relativi a: attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- d) alle attività di sorveglianza sanitaria.

4.3.1. Articolazione interna delle funzioni di sicurezza

Gerit S.r.l. adotta un'organizzazione interna ed un riparto di compiti e ruoli al fine di: i) prevenire il verificarsi di eventi dannosi, quali infortuni o malattie professionali, a carico dei Dipendenti, dei Collaboratori e del personale di soggetti terzi che svolgano interventi per conto della Società; ii) identificare e registrare ogni situazione di rischio relativo al servizio ed alle attività svolte, avviare, proporre o fornire delle soluzioni; iii) verificare l'attuazione delle misure di contenimento dei rischi individuati; iv) monitorare l'attività lavorativa al fine di correggere tempestivamente le carenze individuate.

Tale organizzazione per la sicurezza viene attuata mediante:

- un Organigramma Aziendale, che individua le linee di dipendenza gerarchica tra le diverse posizioni organizzative;
- un Mansionario di Sicurezza, che descrive i compiti assegnati al personale responsabile nella conduzione aziendale della sicurezza.

Dall'Organigramma Aziendale risultano le seguenti figure:

- il Datore di Lavoro, coincidente con uno degli amministratori;
- il Responsabile del Servizio di Prevenzione e Protezione ("RSPP");
- il Rappresentante dei lavoratori per la sicurezza;
- dei dipendenti con funzione di addetti al 1^a soccorso e altri con funzione di addetti antincendio
- il Medico Competente per ogni sede.

Non è stata effettuata una delega di funzioni da parte del Datore di Lavoro, delega che, comunque, ai sensi dell'art. 16 del d.lgs. n. 81/2008, non consente di attribuire al delegato: i) la valutazione di tutti i rischi con la conseguente redazione del documento relativo; ii) la designazione del RSPP.

4.3.2. Valutazione dei rischi

Come premesso, il Datore di Lavoro, in collaborazione con RSPP e Medico competente, previa consultazione con il RLS, è tenuto ad effettuare la valutazione dei rischi e ad elaborare il relativo documento ("DVR").

Ai sensi dell'art. 28 del d.lgs. 81/2008, il documento predetto contiene:

- a) una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa;
- b) l'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuali adottati;
- c) il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
- d) l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;

- e) l'indicazione del nominativo del Responsabile del Servizio di Prevenzione e Protezione, del Rappresentante dei Lavoratori per la Sicurezza o di quello territoriale e del Medico Competente che ha partecipato alla valutazione del rischio;
- f) l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

Ai sensi dell'art. 29, la valutazione dei rischi deve essere immediatamente rielaborata al verificarsi anche di una soltanto delle seguenti circostanze, nel termine di trenta giorni:

- in occasione di modifiche del processo produttivo o della organizzazione del lavoro significative ai fini della salute e sicurezza dei lavoratori;
- in relazione al grado di evoluzione della tecnica, della prevenzione o della protezione;
- a seguito di infortuni significativi o quando i risultati della sorveglianza sanitaria ne evidenzino la necessità.

A seguito di tale rielaborazione, le misure di prevenzione debbono essere aggiornate. Anche in caso di rielaborazione della valutazione dei rischi, il datore di lavoro deve comunque dare immediata evidenza, attraverso idonea documentazione, dell'aggiornamento delle misure di prevenzione e immediata comunicazione al Rappresentante dei Lavoratori per la Sicurezza.

4.3.3. Gestione delle emergenze e primo soccorso

La Società ha adottato un apposito Piano di Emergenza, al quale si fa rinvio, che prescrive:

- le azioni che i Lavoratori devono mettere in atto in caso di incendio;
- le procedure per l'evacuazione del luogo di lavoro che devono essere attuate dai Lavoratori e dalle altre persone presenti;
- le disposizioni per chiedere l'intervento dei Vigili del Fuoco e per fornire le necessarie informazioni al loro arrivo;
- le specifiche misure per assistere le persone con esigenze speciali.

Il Piano di Emergenza dovrà essere aggiornato in occasione di ogni modifica che possa alterare le misure di prevenzione e protezione; l'aggiornamento deve prevedere l'informazione dei Lavoratori ed il coinvolgimento degli addetti alla gestione dell'emergenza.

4.3.4. Riunioni periodiche di sicurezza

Ai sensi dell'art. 35 del d.lgs. n. 81/2008, almeno una volta all'anno viene svolta la riunione periodica per la sicurezza cui partecipano Datore di Lavoro, RSPP, Medico competente e RLS.

Nel caso in cui si renda necessario, la riunione può essere convocata anche più volte all'anno.

Nel corso della riunione, vengono esaminati: i) DVR; ii) andamento di infortuni, malattie professionali e sorveglianza sanitaria; iii) criteri di scelta, caratteristiche tecniche, efficacia dei Dispositivi di Protezione Individuali ("DPI").

4.3.5 Gestione dei lavori in appalto

All'interno degli uffici di Gerit S.r.l. possono operare imprese terze/lavoratori autonomi incaricati delle seguenti attività:

- revisione biennale dei mezzi di protezione antincendio installati;
- manutenzione di impianti / attrezzature;
- manutenzione del sistema informativo;
- pulizie.

Per lavori della durata di almeno 5 giorni o che prevedano rischi particolari, il Datore di lavoro, con la collaborazione del RSPP, elabora il Documento Unico di Valutazione dei Rischi Interferenziali (DUVRI).

La sequenza degli obblighi che il Datore di Lavoro, in qualità di committente, segue nel momento in cui intende affidare dei lavori in appalto o mediante contratto d'opera o di somministrazione al fine di ottemperare correttamente all'art. 26 del d.lgs. 2008 n. 81/2008, si può così di seguito riassumere:

- i) effettuazione, prima di affidare i lavori in appalto o mediante contratto d'opera o di somministrazione, di una verifica tecnico-professionale sia delle imprese che dei lavoratori autonomi, in relazione ai lavori da affidare in appalto o mediante contratto d'opera o di somministrazione, mediante l'esibizione e l'esame della documentazione prevista dallo stesso decreto ed indicata nell'Allegato n. XVII (iscrizione alla Camera di Commercio, DVR, elenco dei DPI forniti ai lavoratori, ecc.);
- ii) informazione alla ditta appaltatrice ed ai lavoratori autonomi dei rischi specifici esistenti nell'ambiente in cui sono chiamati ad operare e sulle misure di protezione e di emergenza adottate in relazione alla propria attività;
- iii) acquisizione delle informazioni sui rischi eventualmente apportati dalle ditte appaltatrici e dai lavoratori autonomi al fine di individuare ed eliminare i rischi dovuti alle interferenze fra i lavori delle diverse imprese coinvolte e degli autonomi nella esecuzione dell'opera complessiva;
- iv) elaborazione di un Unico Documento di Valutazione dei Rischi (DUVRI) che indichi le misure da adottare ed eliminazione o, ove ciò non è possibile, riduzione al minimo dei rischi da interferenze, documento da allegare al contratto di appalto o d'opera (in particolare per lavori che hanno durata maggiore di 5 giorni consecutivi o che prevedano rischi particolari);
- v) stipulazione del contratto di appalto o di somministrazione nel quale devono essere specificatamente indicati, a pena di nullità ai sensi dell'art. 1418 c.c., i costi relativi alla sicurezza del lavoro con particolare riferimento a quelli propri connessi allo specifico appalto;
- vi) affidamento dei lavori e promozione della cooperazione nell'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sulla attività lavorativa oggetto dell'appalto, nonché coordinamento degli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori.

4.4. Controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività connesse alla salute e sicurezza nei luoghi di lavoro al fine di verificare il rispetto delle regole di cui alla presente Parte Speciale e delle procedure interne.

In particolare, l'O.d.V. verifica periodicamente, con il supporto delle altre funzioni competenti: i) l'attività di formazione dei Destinatari; ii) il sistema di deleghe e procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative, raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie; iii) il rispetto di protocolli, procedure e disposizioni aziendali.

Quanto alla reportistica verso l'Organismo di Vigilanza, si segnalano:

A. Reportistica periodica:

- verbale della riunione *ex art.* 35 del d.lgs. n. 81/2008;

B. Reportistica specifica/ad evento

- aggiornamento o modifiche del D.V.R.;
- variazioni dell'Organigramma sulla Sicurezza;
- su base trimestrale, comunicazione della registrazione degli infortuni accaduti nel periodo o la dichiarazione di assenza di infortuni;
- su base annuale, trasmissione del *report* di interventi informativi e formativi erogati nel corso dell'anno;
- verbali di verifica del funzionamento delle procedure di gestione per emergenze e primo soccorso;
- DUVRI di particolare importanza;
- relazione del Medico competente relativa alla sorveglianza sanitaria;
- piani di formazione periodica in materia di salute e sicurezza;
- calendario delle verifiche di *audit* (interne e di parte terza) e relativi verbali;
- documento di Riesame della Direzione;
- piano periodico degli investimenti in impianti ed attrezzature, con evidenza degli interventi rilevanti in materia di salute e sicurezza sul lavoro, ivi compresi gli interventi di manutenzione.

4.5. [Rinvio alle Procedure e alle Istruzioni Operative](#)

Di seguito si rinvia alle Procedure e Istruzioni operative aziendali approntate da Gerit S.r.l. per la prevenzione dei reati in materia di sicurezza sul lavoro:

- DVR;
- Piano di Emergenza;
- Procedura per la gestione degli adempimenti *ex art.* 30 d. lgs. 81/2008 e valutazione dei rischi.

CAPITOLO V

Reati tributari

5.1. Premessa

La presente Parte Speciale prende in considerazione i reati di natura tributaria che possono essere commessi dai Destinatari del Modello, previsti dall'art. 25 *quinquiesdecies* del d.lgs. 231/2001 (" *Reati tributari*"), ovvero:

- art. 2 d.lgs. n. 74/2000: Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti
- art. 3 d.lgs. 74/2000: Dichiarazione fraudolenta mediante altri artifici
- art. 4 d.lgs. 74/2000: Dichiarazione infedele
- art. 5 d.lgs. 74/2000: Omessa dichiarazione
- art. 8 d.lgs. 74/2000: Emissione di fatture o altri documenti per operazioni inesistenti
- art. 10 d.lgs. 74/2000: Occultamento o distruzione di documenti contabili
- art. 10 *quater* d.lgs. 74/2000: Indebita compensazione
- art. 11 d.lgs. 74/2000: Sottrazione fraudolenta al pagamento di imposte solo, però, "*se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro*".

Nello specifico, i processi aziendali esposti al rischio fiscale possono essere distinti tra:

- i) processi diretti, che includono attività di natura prettamente fiscale, come la presentazione delle dichiarazioni fiscali e, in genere, delle altre comunicazioni sociali, la liquidazione ed il versamento dei tributi, la regolare tenuta e custodia della documentazione obbligatoria, la gestione delle operazioni di finanziamento;
- ii) processi indiretti, che includono attività non di natura fiscale, ma con riflessi significativi sui processi direttamente correlati alla sfera fiscale, come la selezione dei fornitori di beni, servizi e prestazioni intellettuali, la stipula e la gestione dei relativi contratti, la predisposizione di bandi di gara, il ciclo degli incassi e dei pagamenti, la gestione delle missioni e dei rimborsi spesa, la gestione delle sponsorizzazioni e/o dei contributi.

Tutte le fattispecie di attività sensibili in relazione ai reati della presente sezione, in particolare previsti all'art. 25 *quinquiesdecies* d.lgs. 231/2001, devono essere svolte conformandosi alle leggi vigenti, al Codice Etico, alle procedure aziendali e alle regole contenute nel presente Modello.

Inoltre, anche con riferimento ai reati tributari sono validi i principi generali del sistema di controllo preventivo, relativi alla tracciabilità delle operazioni, alla separazione dei compiti e delle funzioni, alla chiara definizione dei poteri e delle responsabilità, alla oggettivizzazione dei processi decisionali e alla tracciabilità delle attività di controllo.

5.2. Principi generali di comportamento

I Destinatari del Modello sono tenuti ad osservare i seguenti principi generali:

- a) verificare che le attività afferenti alla gestione degli adempimenti fiscali o contabili siano effettuate esclusivamente da soggetti aventi adeguati poteri, nel rispetto di ruoli e responsabilità definiti in appositi documenti organizzativi interni quali *job description* e mansionari;

- b) rispettare il sistema di deleghe e procure con l'indicazione dei poteri e dei limiti di spesa dei soggetti coinvolti;
- c) verificare che i pagamenti effettuati nei confronti di soggetti interni (es. rimborsi) o esterni trovino adeguata giustificazione alla luce del rapporto contrattuale in essere;
- d) verificare che i pagamenti avvengano solo a fronte di beni/servizi effettivamente ricevuti dalla Società nel rispetto delle condizioni contrattuali;
- e) verificare che per ogni trasferimento in denaro (effettuato o ricevuto) vi sia piena coincidenza tra i destinatari/ordinanti i pagamenti e le controparti effettivamente coinvolte nelle transazioni;
- f) verificare che l'importo effettivamente incassato corrisponda a quello fatturato e che non vi siano anomalie al riguardo;
- g) verificare che non siano effettuati bonifici che non rechino l'indicazione della controparte;
- h) non effettuare pagamenti in favore di un soggetto diverso dalla controparte contrattuale. Eventuali eccezioni a tale divieto sono ammesse solo a fronte della presentazione di una regolare documentazione che giustifica e consente il pagamento nei confronti di un terzo (es. in caso di cessione del credito o di pignoramento presso terzi);
- i) verificare che la gestione degli adempimenti fiscali o contabili sia conforme anche alle prassi o procedure interne in tema di eventuale *iter* autorizzativo alla trasferta, natura/tipologia di spese ammesse a rimborso ed eventuali limiti d'importo, ambiti di responsabilità e limiti autorizzativi delle note spese, gestione carte di credito aziendali, regolamentazione delle note spese per soggetti esterni (ad es. fornitori, consulenti, etc.) tramite previsioni contrattuali e modalità di verifica/rimborso;
- j) monitorare la gestione delle note spese, al fine di garantire una maggiore efficienza del processo;
- k) verificare che non siano concessi sconti, premi, note di accredito che non trovino adeguata giustificazione alla luce del rapporto contrattuale costituito e che siano motivati da fattori obiettivi; l'autorizzazione all'emissione della nota di credito deve comunque essere autorizzata da soggetto provvisto di adeguati poteri, in coerenza con le *policy* e le procedure aziendali;
- l) gestire le attività di sponsorizzazione e/o pubblicitarie mediante l'adozione di appositi supporti contrattuali, completi di adeguate clausole volte a garantire idonee dimostrazioni dell'utilizzo delle somme corrisposte;
- m) garantire la tracciabilità dei flussi finanziari, anche mediante la registrazione di: forma del pagamento (es. contante, bonifico, ecc...); contenuto del pagamento (identificazione del soggetto che ha disposto il flusso, da quale disponibilità ha attinto, beneficiario del flusso, causale).

5.3. Principi Operativi

Si riportano di seguito i principi operativi che i Destinatari del Modello sono tenuti a rispettare nelle attività sensibili, ciascuno secondo il proprio ruolo e responsabilità.

Gestione dei rapporti con i fornitori

- prevedere una fase di preventiva qualifica/*due diligence* dei fornitori, che garantisca la piena conoscibilità della propria controparte contrattuale (si tratta di una fase volta a raccogliere tutte le informazioni anagrafiche, "etiche" e di solidità economico-finanziaria della controparte, improntata alla massima trasparenza);
- verificare periodicamente l'aggiornamento dell'anagrafica dei clienti e dei fornitori, al fine di controllarne l'effettiva esistenza ed operatività;
- definire delle modalità e dei criteri per la valutazione delle offerte ricevute improntati alla trasparenza e, per quanto possibile, alla limitazione di criteri di soggettività;
- monitorare costantemente l'effettiva esecuzione del contratto stipulato, al fine di verificare la corrispondenza tra prestazioni effettuate e pattuite e la corrispondenza tra i documenti contabili e la fattura emessa (es. verifica circa la conformità delle caratteristiche dei beni o servizi oggetto di acquisto, rispetto al contenuto dell'ordine/contratto; verifica della coerenza tra il soggetto che ha erogato la prestazione, il soggetto indicato nell'ordine/contratto ed il soggetto che ha emesso la fattura).

Controlli di coerenza amministrativo-contabile nel ciclo attivo/passivo

- verificare che qualsivoglia fattura (di acquisto o di vendita) abbia adeguata giustificazione alla luce di un rapporto contrattuale effettivamente esistente;
- verificare, all'atto di registrazione della fattura, che sussista quantomeno (alternativamente):
i) l'effettiva corrispondenza tra ordine e fattura; ii) un contratto che giustifichi l'esistenza di un rapporto sottostante tra le controparti economiche e la corrispondenza di questo con la fattura; iii) in assenza di contratto formale, della corrispondenza (anche in forma di e-mail) che dia evidenza di trattative o accordi commerciali, dell'oggetto del rapporto tra le parti e del *quantum* di corrispettivo in relazione alla fattura; iv) in caso di acquisto di beni, la corrispondenza tra fattura e DDT e ordine/contratto; v) in caso di prestazioni di servizi, tracciabilità documentale di quanto reso dal professionista che ha emesso la fattura o una dichiarazione sottoscritta (e tenuta in specifico registro) da parte del soggetto interno della Società che ha gestito l'attività con il professionista che ha emesso la fattura in ordine alla veridicità ed esistenza dell'attività resa.

Gestione degli adempimenti fiscali-contabili

- provvedere al regolare adempimento degli obblighi fiscali-tributari cui la Società è tenuta (tributi, contributi, Iva etc.);
- definire le modalità di verifica circa la tempestiva e corretta liquidazione delle imposte (o delle cartelle esattoriali) rispetto alle scadenze di legge e a quanto riportato nelle dichiarazioni presentate, tenendo conto sia dei versamenti in acconto già effettuati che degli acconti dovuti per l'esercizio in corso;
- fornire informazioni e dati veritieri e completi sulla situazione economica, patrimoniale e finanziaria della Società;
- adempiere le prescrizioni di legge in materia contabile, di informazione societaria, di valutazione di cespiti e di redazione del bilancio;

- non occultare in contabilità redditi conseguiti soggetti a tassazione, non rappresentare falsamente spese non reali, non emettere fatture per prestazioni inesistenti, effettuare stime, valutazioni e determinazione di poste di bilancio con modalità e criteri valutativi difformi da quelli richiesti dalla legge;
- non ostacolare l'effettuazione di verifiche, accertamenti ed ispezioni da parte di Autorità di settore, fiscali o giudiziarie.

Gestione della documentazione contabile

- assicurarsi che le scritture contabili e gli altri documenti di cui è obbligatoria la conservazione a fini fiscali, siano custodite, approntando difese fisiche e/o informatiche che impediscano eventuali atti di distruzione o occultamento;
- assicurarsi che sia attuato il principio di segregazione delle funzioni nella gestione della contabilità e nella predisposizione delle dichiarazioni tributarie, anche tramite il ricorso a strumenti informatici che assicurino l'inserimento delle informazioni rilevanti e impediscano qualsiasi modifica senza evidenza di autore, data e registrazione originaria;
- tenere tracciate tutte le fasi di gestione dei flussi finanziari e archiviare in maniera completa i relativi documenti giustificativi;
- prevedere un sistema di *back up* dell'archiviazione dei documenti contabili;
- non occultare o distruggere, in tutto o in parte, documenti contabili, fiscali o di cui è comunque obbligatoria la conservazione.

Gestione delle operazioni straordinarie

- garantire l'esplicita approvazione, da parte del Consiglio di Amministrazione, di ogni attività relativa ad operazioni straordinarie, comprese le cessioni e dismissioni di asset aziendali, nonché in merito alla effettuazione di conferimenti, alla distribuzione di utili o riserve, a operazioni sul capitale sociale, a fusioni e scissioni, qualora per il compimento delle suddette operazioni si renda necessaria od opportuna l'approvazione del Consiglio di Amministrazione;
- garantire l'adeguata informazione e/o il rendiconto in merito alle operazioni di cui sopra qualora queste vengano effettuate da soggetti cui il Consiglio di Amministrazione ha conferito appositi poteri;
- identificare in maniera chiara e precisa i ruoli ed i soggetti competenti alla predisposizione della documentazione destinata agli organi sociali a supporto delle deliberazioni relative ad operazioni straordinarie;

5.4. Controlli dell'Organismo di Vigilanza

In linea generale, sarà opportuno che ogni funzione coinvolta nelle attività sensibili, individuate in relazione ai reati tributari, comunichi all'Organismo di Vigilanza tutte le informazioni rilevanti in materia, mediante la previsione di specifici flussi informativi.

Così, la Funzione Tax/Amministrazione/Controllo dovrà comunicare gli esiti delle verifiche svolte in merito a:

- i) veridicità delle dichiarazioni fiscali rispetto alle scritture contabili e correttezza dei relativi versamenti (con cadenza annuale);

- ii) eventuali accertamenti da parte dell'Autorità Fiscale;
- iii) procedure adottate per garantire la tracciabilità dei flussi contabili e finanziari;
- iv) investimenti di maggiore rilevanza;
- v) operazioni straordinarie che comportino impatti rilevanti in ambito fiscale.

5.5. Rinvio alle Procedure e alle Istruzioni Operative

Di seguito si rinvia alle Procedure e Istruzioni operative aziendali approntate da Gerit S.r.l. per la prevenzione dei reati tributari:

- *Gerit's Expense Policy*;
- Codice Etico;
- Procedura per gli adempimenti societari e la redazione del bilancio;
- Procedura per la gestione della tesoreria.

CAPITOLO VI

Reati informatici, di trattamento illecito di dati e violazione del diritto d'autore

6.1. Premessa

Il presente Capitolo della Parte Speciale prende in considerazione i reati di natura informatica e di trattamento illecito di dati, previsti dall'art. 24 *bis* del d.lgs. 231/2001, nonché di violazione del diritto d'autore, previsto dall'art. 25 *novies* del decreto predetto.

Di seguito si riportano le fattispecie di reato previste dall'art. 24 *bis* del Decreto ("*Delitti informatici e trattamento illecito dei dati*");

- art. 491 *bis* c.p.: Documenti informatici
- art. 615 *ter* c.p.: Accesso abusivo ad un sistema informatico o telematico
- art. 615 *quater* c.p.: Detenzione, diffusione e installazione abusiva di apparecchiature, codice e altri messi all'accesso a sistemi informatici o telematici
- art. 615 *quinquies* c.p.: Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- art. 617 *quater* c.p.: Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- art. 617 *quinquies* c.p.: Detenzione, diffusione e installazione di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche
- art. 635 *bis* c.p.: Danneggiamento di informazioni dati e programmi informatici
- art. 635 *ter* c.p.: Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da un altro ente pubblico o comunque di utilità pubblica
- art. 635 *quater* c.p.: Danneggiamento di sistema informatici o telematici
- art. 635 *quinquies* c.p.: Danneggiamento sistemi informatici o telematici di pubblica utilità
- art. 640 *quinquies* c.p.: Frode informatica del soggetto che presta servizi di certificazione di firma elettronica
- art. 1, comma 11, D.L. 105/2019: Violazione delle norme in materia di perimetro di sicurezza nazionale cibernetica

Di seguito si riportano anche le fattispecie di reato previste dall'art. 25 *novies* ("*Delitti in materia di violazione del diritto d'autore*") del Decreto:

- art. 171, comma 1 lett. a) *bis*), L. 633/1941: Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa
- art. 171, comma 3, L. 633/1941: Reati di cui all'art. 171 L. 633/1941, comma 1 lettera a) *bis*), commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione
- art. 171 *bis*, comma 1, L. 633/1941: Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non

contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori

- art. 171 *bis*, comma 2, L. 633/1941: Riproduzione, trasferimento su altro su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati
- art. 171 *ter*, L. 633/1941: Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa
- art. 171 *septies*, L. 633/1941: Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione
- art. 171 *octies*, L. 633/1941: Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale

Sul piano teorico, le fattispecie di reato richiamate da tali disposizioni potrebbero verificarsi nell'ambito delle attività poste in essere dai Dipendenti operanti nell'area IT, la quale è maggiormente esposta al rischio potenziale di commissione di taluno di tali reati; tuttavia, non si può escludere che anche altre aree aziendali siano esposte al rischio predetto, nella misura in cui in esse si faccia uso di sistemi *hardware*, *software* e telematici.

Pertanto, tali attività sono state individuate con riferimento al complessivo utilizzo dei sistemi informativi di cui la Società fa ricorso mediante l'impiego di sistemi *hardware e software*, di accesso alla rete *internet*, di utilizzo di sistemi di posta elettronica o di altri sistemi di comunicazione telematica.

A questo proposito, la Società considera attività sensibili:

- la gestione degli accessi ai sistemi informatici o telematici (inclusi quelli della P.A.);
- la gestione dei codici di accesso a sistemi informatici o telematici;
- l'utilizzo dei sistemi informatici, informazioni, dati e programmi informatici;
- la redazione e trasmissione di documenti informatici, anche verso la P.A. e anche da parte dell'*outsourcer*;
- l'utilizzo di internet e posta elettronica;
- l'organizzazione dei profili di accesso al sistema contabile;
- la gestione della tracciabilità delle operazioni eseguite tramite sistemi informatici;
- la realizzazione di interventi di tipo organizzativo normativo e tecnologico;
- la gestione ed utilizzo dei sistemi informatici e del patrimonio informativo della Società.

6.2. Principi Generali di Comportamento

I Destinatari del Modello, con riferimento ai reati informatici, di trattamento illecito di dati e di violazione del diritto d'autore, devono attenersi ai principi generali di comportamento di seguito enunciati:

- a) rispettare le norme di legge e le procedure aziendali in tutte le attività finalizzate alla gestione della rete informatica aziendale e dei dati personali, nell'ambito delle attività lavorative svolte, coerentemente con il ruolo assunto all'interno della organizzazione aziendale;
- b) non divulgare informazioni relative ai sistemi informatici aziendali;
- c) non introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso;
- d) non accedere al sistema informatico o telematico, ovvero a banche dati della Società, non possedendo le credenziali di accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati, senza esserne autorizzati;
- e) non utilizzare dispositivi tecnici o strumenti *software* non autorizzati (*virus, worm, trojan, spyware, dialer, keylogger, rootkit*, etc.) atti ad impedire od interrompere le comunicazioni relative al sistema informatico o telematico od intercorrenti tra più sistemi;
- f) non utilizzare illecitamente materiale tutelato dall'altrui diritto d'autore;
- g) non distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui od anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- h) non introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- i) non detenere, procurarsi, riprodurre o diffondere abusivamente codici di accesso o comunque mezzi idonei all'accesso ad un sistema protetto da misure di sicurezza;
- j) non rivelare, divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale o sistemi di terze parti;
- k) non procurare, riprodurre, diffondere, comunicare o mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema od i dati ed i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- l) non lasciare incustodito il *personal computer* affidato;
- m) non accedere a siti *internet* sensibili, potenziali veicoli di diffusione di *virus*, nonché di ogni ulteriore e potenziale pregiudizio per l'attività aziendale.

6.3. Principi Operativi

Oltre ai principi generali sopra descritti, si indicano di seguito ulteriori principi specifici di prevenzione che tutti i soggetti coinvolti devono rispettare, al fine di prevenire e impedire il verificarsi dei reati in oggetto:

- ogni dipendente è tenuto a segnalare agli Amministratori, anche singolarmente intesi, eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di *hacker* esterni), mettendo a disposizione ed archiviando tutta la documentazione relativa all'incidente;
- ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate (es. *personal computer* fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività. Tali risorse devono essere conservate in modo appropriato e la Società dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;
- l'utilizzo di materiale coperto da altrui diritto d'autore deve avvenire solamente in presenza di una specifica licenza da parte dell'autore, ovvero nell'ambito di diritti di utilizzo formalizzati;

Protezione della rete da intrusioni informatiche, virus, etc.

La Società deve garantire la protezione della rete informatica con misure tecnologicamente adeguate. In particolare:

- tutti i *computer* aziendali (fissi e portatili) ed il *server* sono dotati di sistemi *antivirus*, *firewall* e protezioni da eventuali aggressioni esterne;
- i sistemi *antivirus* siano quotidianamente aggiornati secondo un programma di *upgrade* aggiornato;
- ogni supporto che venga istallato e/o utilizzato su *computer* aziendali è preventivamente sottoposto a scansione *antivirus*.

Protezione del materiale informatico da utilizzi impropri

- tutti i computer sono dotati di *username* personale riferibile al singolo utente, nonché di una *password* di protezione;
- tutti i *computer* aziendali devono essere impostati in modo che durante la fase di *standby* l'utilizzo divenga possibile solo previo inserimento della *password*;
- le *password* devono essere periodicamente modificate;
- il *server* aziendale deve essere collocato in un locale protetto e l'accesso al medesimo deve essere consentito solo agli Amministratori e al tecnico esterno autorizzato, che, ove strettamente necessario, possono a loro volta consentire l'accesso, alla loro presenza, di altri dipendenti della Società o di ulteriori tecnici esterni autorizzati.

Tutela del diritto di autore

Al fine di tutelare il diritto d'autore, la Società è tenuta a:

- fornire ai Destinatari un'adeguata informazione circa il corretto utilizzo degli *user-id* e delle *password* per accedere ai principali sottosistemi informatici utilizzati presso la Società;
- regolamentare l'utilizzo dei sistemi informatici e l'accesso agli stessi da parte dei Destinatari sulla base delle finalità connesse agli impieghi da questi ultimi svolti;

- effettuare, per quanto possibile, nel rispetto della normativa sulla *privacy*, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;
- predisporre e mantenere adeguate difese fisiche a protezione dei sistemi informatici aziendali;
- effettuare, per quanto possibile, controlli periodici sui contenuti del sito *internet* aziendale.

A tutti i destinatari del Modello è vietato:

- utilizzare il *computer* aziendale a propria disposizione per scopi esclusivamente personali;
- consentire a soggetti, interni od esterni alla Società, di accedere al proprio computer anche temporaneamente, se non dopo essersi collegati alla rete con il proprio identificativo;
- inserire nel *computer* supporti di memorizzazione esterni, tipo dischi fissi esterni, chiavette USB, DVD o CD, qualora i medesimi supporti non siano di provenienza conosciuta e garantita;
- salvare dati al di fuori del proprio profilo utente in modo che siano visibili da altri che si collegano al computer con un altro identificativo;
- copiare dati aziendali sui computer personali o su dispositivi rimovibili, qualora non sia strettamente necessario per fini lavorativi;
- inviare per posta elettronica dati sensibili;
- configurare l'accesso remoto alla rete informatica aziendale su *computer* diversi da quello in uso senza preventiva autorizzazione;
- installare e utilizzare *software* (programmi) non approvati dalla Società e non correlati con l'attività professionale espletata da parte dei destinatari o degli utilizzatori.

6.4. Controlli dell'Organismo di Vigilanza

In linea generale, sarà opportuno che ogni funzione coinvolta nelle attività sensibili sopra descritte comunichi all'Organismo di Vigilanza tutte le informazioni rilevanti in materia, mediante la previsione di specifici flussi informativi.

Quanto alla reportistica verso l'Organismo di Vigilanza, si segnalano:

A. Reportistica periodica

Relazione annuale circa la verifica dell'adeguatezza delle procedure informatiche, della loro applicazione, di ogni altro aspetto di sicurezza IT rilevante.

B. Reportistica specifica/ad evento

Anomalie specifiche e significative rilevate in esito a verifiche/controlli circa l'adeguatezza delle procedure informatiche e la loro applicazione. In particolare:

- criticità riscontrate nella sicurezza IT;
- errori, ritardi ed omissioni nell'esecuzione delle procedure;
- cambiamenti nelle procedure;
- carenze o disfunzioni riscontrate.

6.5. Rinvio alle Procedure e alle Istruzioni Operative

Di seguito si rinvia alle Procedure e Istruzioni operative aziendali approntate da Gerit S.r.l. per la prevenzione dei reati in questione:

- Codice Etico;
- Gerit's Information Security Policy - GDPR Data Protection Addendum;
- Global Data Protection Policy;
- Guidelines on International Data Transfers, *Adequate vs. Restricted Countries*;
- Guidelines on the Management of Data Protection Impact Assessments;
- Gerit's Document Retention Policy;
- Guidelines on the Management of Vendors Processing PII;
- Guidelines on Personally Identifiable Information (PII), Pseudonymized PII, Sensitive PII and Anonymized Data
- Gerit Information Classification & Data Handling Standard;
- ICEE Operating Manual - IT Security and Processes;
- Information Security Policy & Acceptable Use Agreement.