Modello di organizzazione e gestione ex D.Lgs. 8 giugno 2001, n. 231

Informatica Alto Adige S.p.A.

Approvato da:	Consiglio di Amministrazione
Data di approvazione:	24.09.2021
N.ro versione:	8.0
N.ro pagine:	80
Distribuzione:	Sito Intranet della Società
Nomefile:	Modello_di_Organizzazione_e_Gestione_231_SIAG_0.3.docx 5.0

Attenzione

Il presente documento è disponibile in copia originale sul server della rete *intranet*.

Ogni copia cartacea si ritiene copia di lavoro **non controllata**.

È responsabilità di chi utilizza copie non controllate verificarne il livello di aggiornamento.

AGGIORNAMENTI DELLA VERSIONE

Versione	Data	Motivo	Modifiche
1.0	20/03/2012	Nuova emissione	Nuova emissione
2.0	29/11/2012	Nuova emissione	Aggiornamento Reati
3.0	24/04/2014	Nuova emissione	Aggiornamento Reati
4.0	22/12/2016	Revisione complessiva del documento	▪ Aggiornamento complessivo conseguente all'inserimento, da parte del Legislatore, di nuovi reati nell'area di applicazione del D.Lgs. 231/01 (es.: alcune fattispecie di reati societari, l'autoriciclaggio, alcune fattispecie di reati ambientali). ▪ Razionalizzazione della struttura del Modello, con inserimento di Principi di comportamento di valenza generale e di valenza specifica, per tipologia di reato. ▪ Incrementata la frequenza dei flussi informativi periodici verso l'Organismo di Vigilanza.
5.0	14/06/2018	Nuova emissione	Aggiornamento dei reati • L. 17 ottobre 2017, n. 161 (in G.U. serie generale 4/11/2017, n. 258) • D.Lgs. 15 marzo 2017, n. 38 (in G.U. serie generale 30/3/2017, n. 75)
6.0	29/01/2019	Nuova emissione	Inserimento riferimento alla procedura aziendale in tema di Whistleblowing di cui alla legge 30 novembre 2017, n. 179 "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato"

7.0	…….	Nuova emissione	Aggiornamento dei reati • DL 14 dicembre 2018, n. 135 (“Semplificazioni”), convertito con Legge n. 12/2019 • Legge 9 gennaio 2019, n. 3 (“Spazzacorrotti”) • Legge 3 maggio 2019, n. 39 • DL 26 ottobre 2019, n. 124, convertito con modificazioni con Legge 157”2019 • Cooridnamento con il PTPC
8.0	……	Nuova emissione	Aggiornamento dei reati • D.lgs. 14 luglio 2020 n. 75

Sommario

1. SEZIONE GENERALE

Il Decreto Legislativo n. 231/2001

Il Decreto Legislativo 231/01 ("*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica…*", dell'8 giugno 2001) sancisce il principio per cui alcuni enti collettivi (di seguito anche "*Enti*") rispondono, nelle modalità e nei termini indicati, dei reati commessi da Personale interno alla struttura della Società, reati specificatamente indicati dal Decreto stesso.

In un'assoluta ottica di responsabilizzazione dell'Ente per una corretta organizzazione gestionale, un valido fattore di difesa che il soggetto giuridico può spendere in caso di commissione di un reato che vede la struttura perseguire un illecito interesse o beneficiare di un indebito vantaggio, è dato dalla possibilità di dimostrare la sua assoluta estraneità istituzionale ai fatti criminosi, con conseguente emersione di responsabilità e/o interesse esclusivamente in capo al soggetto agente che ha commesso l'illecito.

La suddetta estraneità va comprovata attraverso la funzionalità di un'organizzazione interna attenta, in chiave di prevenzione, sia alla formazione della corretta volontà decisionale della struttura sia alla vigilanza circa il corretto utilizzo delle risorse finanziarie della Società.

Con il D.Lgs. 231/2001 è stato quindi recepito nel nostro ordinamento il principio per cui anche le persone giuridiche rispondono in modo diretto dei reati commessi, nel loro interesse o a loro vantaggio, da chi opera professionalmente al loro interno.

La sanzionabilità dell'Ente e la correlata funzionalità complessiva del sistema preventivo, atto a scongiurare l'addebito di responsabilità, sono concetti legati alla capacità di lettura dell'organizzazione interna della persona giuridica e della conseguente corretta costituzione sia di norme etiche preventive che delle regole di sorveglianza "difensiva" sui fatti (quali per l'appunto, quelle contenute nei "*Modelli di organizzazione e di gestione*"), che gli amministratori hanno l'obbligo civilistico di precostituire anche nell'interesse del patrimonio sociale.

La suddetta verifica passa anche attraverso:

- le misure di vigilanza interna sui "modelli di organizzazione e gestione" istituiti;
- la costituzione di appositi organi dotati di adeguati poteri;
- il riscontro della sussistenza o meno di caratteri elusivi specifici verso le suddette misure, nei fatti occorsi, da parte di coloro che, nonostante le misure preventive, hanno commesso i reati.
-

L'essenza della normativa in oggetto comporta che se il reato è commesso da persone "*appartenenti*", nei termini appositamente stabiliti dal Decreto, alla persona giuridica, la commissione di quel reato comporta anche direttamente, in aggiunta alle conseguenze "tipiche" che procurerà a carico del reo, l'applicabilità consequenziale di diverse e gravi sanzioni direttamente a carico della Società.

L'effetto pratico primario del decreto è, quindi, l'ampliamento dello spettro di responsabilità per la commissione di certi reati.

L'aver beneficiato, anche economicamente, di un illecito è presupposto valido per scontare le responsabilità consequenziali previste dalla legge, che affiancano e non sostituiscono le eventuali conseguenze di tipo civilistico, ovvero quelle basate su impatti di danno verso terzi.

Tale riverbero di responsabilità sorge allorché certe persone appartenenti professionalmente all'Ente si rendono autrici di certi specifici reati, in seguito detti anche "*reati-presupposto*".

Dunque la tematica implica a monte un'analisi selettiva sia sui Soggetti che determinano la responsabilità sia sugli illeciti che comportano l'insorgenza della stessa.

Quanto ai predetti Soggetti "interni", la legge dispone che si tratta dei seguenti:

1. persone che rivestono funzioni di rappresentanza;
2. persone che rivestono funzioni di amministrazione;
3. persone che rivestono funzioni di direzione dell'Ente o di una sua unità organizzativa autonoma (una sede secondaria, ad esempio, ma anche uno stabilimento o una rappresentanza);

4. persone che esercitano anche di fatto la gestione o il controllo dell'Ente stesso;
5. persone sottoposte alla direzione o alla vigilanza di qualunque Soggetto menzionato nei punti precedenti (il che corrisponde ad un'estensione cospicua dell'ambito soggettivo in parola).

Il Decreto dispone che la responsabilità dell'Ente non scatta se risulta dimostrato processualmente che le persone fisiche sopra elencate hanno commesso il reato che ha determinato l'implicazione derivata della persona giuridica operando esclusivamente nell'interesse proprio o di terzi estranei.

Due le tipologie soggettive dei Soggetti interni rilevanti: apicali e sottoposti.

La posizione apicale è in sostanza quella che dà luogo alle ipotesi che più sopra abbiamo incluso nei punti da 1 a 4. È infatti a quei Soggetti che, nell'ambito del decreto, è destinata con priorità la disciplina della capacità esimente di quello che chiamiamo, più avanti, con termine già in voga nella prassi, lo "scudo protettivo" (cioè il compendio di misure volte a prevenire la "trasmissione" di responsabilità che è il punto nodale del Decreto). Per ciò che attiene al rapporto tra Soggetti "apicali" e "scudo", è importante sottolineare come, perché lo "scudo" risulti efficace, in caso di reati commessi da questi Soggetti, è necessario dimostrare in giudizio che nel commettere il reato costoro hanno agito con dolo anche verso lo *scudo*, cioè si sono volontariamente e fraudolentemente sottratti alle prescrizioni e ai contenuti del "*Modello di organizzazione e gestione*".

Va altresì dimostrato, oltre a ciò che attiene all'azione dei "trasgressori", che non vi è stata omessa o insufficiente sorveglianza da parte dell'apposito "Organismo di Vigilanza" in ordine al funzionamento, all'osservanza ed all'aggiornamento del Modello.

Per i Soggetti sottoposti alla direzione di altri (i Dipendenti o i Collaboratori non apicali), fermo che anche essi non trasmettono all'Ente responsabilità se agiscono, col reato, nell'interesse esclusivo proprio o di terzi, la responsabilità è ascrivibile all'Ente solo se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza, cosa che è esclusa presuntivamente, dall'adozione ed efficace attuazione, prima della commissione del reato, di un modello *idoneo a prevenire reati della stessa specie di quello verificatosi*.

Per quanto riguarda i "*reati-presupposto*" da cui discende la responsabilità degli Enti, il decreto legislativo 231/2001 individua le seguenti tipologie omogenee:

a) 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 fronde nelle pubbliche forniture
b) reati informatici e trattamento illecito di dati
c) delitti di criminalità organizzata
d) peculato, concussione, induzione indebita a dare o promettere altra utilità, corruzione e abuso d'ufficio falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento
e) delitti contro l'industria e il commercio
f) reati societari
g) delitti con finalità di terrorismo o di eversione dell'ordine democratico
h) pratiche di mutilazione degli organi genitali femminili
i) delitti contro la personalità individuale
j) abusi di mercato
k) omicidio colposo o lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro
l) ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio
m) delitti in materia di violazione del diritto d'autore
n) induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
o) reati ambientali
p) impiego di cittadini di paesi terzi il cui soggiorno è irregolare
q) razzismo e xenofobia
r) frode in competizioni sportive, esercizio abusivo di gioco o di scomessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati
s) reati tributari

t) contrabbando
u) reati transnazionali (favoreggiamento personale, contrabbando di tabacchi lavorati esteri, immigrazioni clandestine.)

Si segnala infine che, nella generalità dei casi e ad eventuale integrazione di sanzioni di altro tipo, l'Ente ritenuto responsabile per la commissione di un determinato reato può essere soggetto ad una o più delle seguenti *sanzioni interdittive*:

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

Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo *unico* o *prevalente* di consentire o agevolare la commissione di reati in relazione ai quali è prevista la sua responsabilità, è sempre disposta l'interdizione definitiva dall'esercizio dell'attività.

Il collegamento con le Misure integrative di prevenzione della corruzione

Informatica Alto Adige S.p.A. è una società in controllo pubblico come definita dal D.lgs. 175/2016 e meglio descritta nel paragrafo che segue.

Ai sensi dell'art. 1, co. 2bis, L 190/2012 (come modificato dall'art. 41, D.lgs. 97/2016, recante "Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 06.11.2012, n. 190 e del D.lgs. 14.03.2013, n. 33, ai sensi dell'articolo 7 della legge 07.08.2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche") le società in controllo pubblico non sono tenute ad adottare un vero e proprio PTPC, ma devono adottare Misure integrative di quelle adottate ai sensi del D.lgs. 231/2001, idonee a prevenire anche i fenomeni di corruzione e di illegalità in coerenza con le finalità della L. 190/2012.

In particolare, con riferimento alla tipologia dei reati da prevenire, il D.lgs. 231/2001 ha riguardo ai reati commessi nell'interesse o a vantaggio della società o che comunque siano stati commessi anche nell'interesse di questa, mentre la L. n. 190/2012 è volta a prevenire anche reati commessi in danno alla società.

Le Misure integrative di prevenzione della corruzione adottate da Informatica Alto Adige S.p.A. (da ultimo approvate con delibera del CdA dd. 24.01.2020 per il triennio 2020-2022) costituiscono, pertanto, parte integrante ed essenziale del presente Modello organizzativo.

La Società Informatica Alto Adige S.p.A.

Informatica Alto Adige S.p.A. (di seguito, per brevità, anche "*SIAG*", "*Società*" o "*Azienda*") da oltre venti anni rappresenta il partner IT dell'Amministrazione pubblica in provincia di Bolzano: Provincia Autonoma di Bolzano ("*PAB*"), Consorzio dei Comuni, Regione Trentino Alto Adige Südtirol.

Trattandosi di una Società "*in house*" (come recita l'art. 4-BIS dello Statuto di *Informatica Alto Adige*), SIAG eroga i propri servizi in ambito IT (*Information Technology*), servizi previsti da specifico "*Catalogo*", ad esclusivo beneficio dei suoi Azionisti (i tre Enti citati) e degli Enti ad essi collegati.

Al centro del proprio interesse la Società ha da sempre l'ottimizzazione dei processi amministrativi, così da favorire una sempre maggiore vicinanza fra Amministrazione e Cittadino, con vantaggi per entrambi.

Oltre a fornire specifiche soluzioni IT per l' *e-Government* dell'Amministrazione, SIAG eroga servizi IT, attività di consulenza ed assistenza a beneficio dei propri Clienti.

Una specifica menzione merita la gestione di un efficiente Datacenter, così come la disponibilità di una sala corsi opportunamente attrezzata per lo svolgimento di attività formativa.

Sistema di Governance

Informatica Alto Adige S.p.A. ha adottato, come sistema di amministrazione e controllo, un modello di *Amministrazione tradizionale*, che prevede, come descritto da proprio statuto, un Consiglio di Amministrazione (composto da tre membri) ed un Collegio sindacale (composto da tre membri effettivi).

Struttura organizzativa

Al Consiglio di Amministrazione risponde il *Management* di *Informatica Alto Adige S.p.A.*

Il Direttore sottoscrive i contratti di assunzione di nuovi Dipendenti, con esclusione dei Quadri e (da Statuto SIAG) dei Dirigenti, per i quali la responsabilità della loro assunzione è attribuita, collegialmente, al CdA in base all'articolo 25 dello statuto societario.

Per quanto riguarda l'attività di formazione destinata a settori dell'Azienda, eventuali esigenze in tal senso vengono programmate dal Responsabile Risorse Umane che li propone, per autorizzazione, al Direttore.

Eventuali sanzioni disciplinari, normalmente proposte dal Superiore gerarchico del Dipendente o dall'*Organismo di Vigilanza* (vedasi successivamente "L'Organismo di Vigilanza"), vengono comminate dal Direttore.

La gestione degli acquisti (nei suoi vari aspetti: contrattuali, amministrativi ed operativi) è supervisionata dal Responsabile della Funzione Supply e (in funzione della natura dell'acquisto) dal RUP ([1]). Nella fase autorizzativa del processo possono intervenire altri ulteriori Responsabili: Responsabile Finance, Direttore, ecc.

In posizione di staff al Direttore è collocata l'U.O. "Internal Audit – Certification", che comprende la funzione di *Internal Auditing*. Il principale compito di tale funzione è quello di attuare un controllo sul rispetto dei protocolli previsti dal presente *Modello* da parte delle varie UU.OO., al fine di garantire:

- l'affidabilità e l'integrità delle informazioni contabili, finanziarie ed operative;
- l'efficacia e l'efficienza delle operazioni;
- la salvaguardia del patrimonio;
- la conformità a leggi, regolamenti e contratti.

L'*Internal Auditing* è anche tenuto a riportare le principali evidenze e criticità emerse sia all'attenzione del Top Management della Società, che agli organi di controllo e vigilanza: *Collegio sindacale* e *Organismo di Vigilanza*.

Company Profile

Fondata nel 1992, la società *Informatica Alto Adige S.p.A.* è controllata dalla *Provincia Autonoma di Bolzano ("PAB")*, che detiene il 78,04% del capitale sociale di SIAG. Il rimanente è posseduto dal *Consorzio dei Comuni dell'Alto Adige* (circa il 20,88%) e dalla *Regione Trentino Alto Adige* (circa il 1,08%). Lo Statuto prevede che la partecipazione al capitale sociale della Società sia *interamente pubblica*.

Si ritiene opportuno evidenziare che fra i Soci della Società è stato stabilito un *Patto parasociale* che fra l'altro garantisce, in tema di scelte societarie di natura strategica, una totale trasparenza reciproca fra gli Azionisti.

La Società opera nei vari settori dell'IT, in linea con gli obiettivi strategici della Proprietà.

([1]) "*Per ogni singola procedura per l'affidamento di un appalto o di una concessione le stazioni appaltanti nominano, nel primo atto relativo ad ogni singolo intervento, un responsabile unico del procedimento (RUP) per le fasi della programmazione, della progettazione, dell'affidamento, dell'esecuzione.*" (art. 31 del D.Lgs. 50/2016)

La Società ha acquisito le seguenti certificazioni:

- ISO 9001: certifica il Sistema per la gestione della Qualità adottato in SIAG;
- ISO 27001: certifica il Sistema di gestione della sicurezza delle informazioni, in particolare di quelle gestite su supporto elettronico.

Inoltre, i Collaboratori di SIAG hanno conseguito, fra le altre, le seguenti certificazioni:

- Microsoft® – Tecnologie Server
- Cisco®
- RedHat®
- ITIL v3

Per una descrizione aggiornata e più dettagliata della società SIAG si rimanda al sito internet (**www.siag.it**).

La società *Informatica Alto Adige S.p.A.* non è mai stata sottoposta a procedimento ai sensi del D.Lgs. 231/01.

Il Codice Etico di Informatica Alto Adige

Il *Codice Etico* di *Informatica Alto Adige*, partendo da un patrimonio di valori condiviso, detta le norme di comportamento che tutti coloro che, direttamente o indirettamente, stabilmente o temporaneamente, instaurino a qualsiasi titolo rapporti di collaborazione od operino nell'interesse della Società, devono applicare nella conduzione degli affari e nella gestione delle attività.

Il *Codice Etico* di *Informatica Alto Adige* è da intendersi, quindi, vincolante per Amministratori, Dirigenti e Dipendenti tutti, Membri del *Collegio sindacale*, Membri dell'Organismo di Vigilanza, Collaboratori esterni temporanei o continuativi, Partners, Fornitori e Clienti.

Il *Codice Etico* di *Informatica Alto Adige* è da considerare, ad ogni effetto, parte integrante e sostanziale del presente *Modello di Organizzazione e Gestione*. Pertanto violazioni delle disposizioni in esso contenute rappresentano vere e proprie violazioni del *Modello*, con tutte le conseguenze da ciò derivanti in tema di applicabilità delle sanzioni disciplinari.

Il Modello di organizzazione e gestione ex D.Lgs 231/01 della Società

Un sistema di controlli preventivi ritenuto idoneo a garantire che i rischi di commissione dei reati previsti dal D.Lgs 231/01 siano ridotti ad un "livello *accettabile*" è quel sistema che costringe, per il suo aggiramento, ad un *comportamento fraudolento* da parte di chi compie l'atto illecito.

Il sistema suddetto si articola in specifici protocolli settoriali (*procedure*) costituiti da un insieme di controlli preventivi e successivi, parte integrante del *Modello di organizzazione e gestione* e indispensabile strumento destinato a guidare le attività dei Soggetti "sensibili".

Si ritiene che il presente *Modello di organizzazione e gestione* si connoti come un efficace sistema di controllo preventivo, contraddistinto, com'è, dall'esistenza delle seguenti caratteristiche, che integrano fondamentali *princìpi di controllo*:

- sistema organizzativo sufficientemente formalizzato con specifico riferimento alle attribuzioni di funzioni, responsabilità e linee di dipendenza gerarchica;
- separazione, indipendenza ed integrazione fra funzioni aziendali: le varie fasi di uno stesso processo (esecuzione, controllo operativo, contabilizzazione, supervisione, autorizzazione, ecc.) non possono essere lasciate all'autonoma gestione di una singola persona;
- poteri autorizzativi e di firma formalizzati e coerenti con le funzioni e le responsabilità aziendali ricoperte dai Soggetti apicali

- punti di controllo manuali ed informatici;
- verificabilità, documentabilità e congruità di ogni processo aziendale, in particolare delle transazioni e delle operazioni più significative
- verificabilità, documentabilità delle attività di controllo: *operativo* (previsto nell'ambito del processo) o *di supervisione* (di primo e secondo livello, dove previsto)
- comunicazione continuativa all'Organismo di Vigilanza delle informazioni concernenti le operazioni a rischio e tempestiva informativa allo stesso Organismo di anomalie o violazioni del Modello organizzativo
- monitoraggio da parte dell'Organismo di Vigilanza sull'attuazione del Modello organizzativo.

Documenti della Società integrati nel Modello

Vanno considerate parti integranti e sostanziali del presente *Modello di organizzazione e gestione*, anche in relazione alle conseguenze in tema di applicazione delle sanzioni disciplinari conseguenti all'eventuale violazioni delle disposizioni in essi contenute, i seguenti documenti della Società:

- il *Codice Etico* di *Informatica Alto Adige* (già precedentemente richiamato)
- i documenti (manuali, procedure, regolamenti, ecc.) richiamati nel presente *Modello* ed, in particolare, nella sua *Sezione Speciale*, in quanto *di riferimento* nella descrizione dei protocolli e dei controlli prescritti.
- Piano Triennale per la Prevenzione della Corruzione e le misure integrative di prevenzione della corruzione ex art. 1, co. 2bis della Legge 1902/2012

Il *Codice Etico* di *Informatica Alto Adige* risulta reperibile nel portale internet della Società (**www.siag.it**), mentre gli altri documenti referenziati sono accessibili, a tutti i Dipendenti, presso apposite sezioni della rete *intranet* di SIAG.

Metodologia di definizione e revisione del Modello

Di seguito si fornisce una descrizione sintetica delle fasi operative svolte per la definizione del primo impianto del *Modello di organizzazione e gestione*, con un accenno anche alle successive fasi di revisione. In particolare ci si concentra nella descrizione dei passi seguiti per la stesura della seconda Sezione del presente *Modello*, la *Sezione speciale*, che descrive, contestualizzandolo nell'Azienda, ciascun reato-presupposto, fornendo riferimenti alle norme, ai protocolli ed ai controlli posti a presidio del rischio di commissione del reato.

1.5.2.1. Analisi del reato-presupposto ed individuazione della possibile modalità di commissione

Il Decreto Legislativo 231/2001 disciplina la responsabilità di un *Ente* (persone giuridiche, società e associazioni anche prive di personalità giuridica) a fronte di illeciti amministrativi dipendenti dalla commissione di specifici reati. I "*reati-presupposto*" elencati dal Decreto, fin dalla sua emanazione, sono vari e sono stati successivamente integrati, a più riprese, con l'aggiunta, da parte del Legislatore, di ulteriori nuove fattispecie.

Nell'approccio seguito per la definizione del *Modello di organizzazione e gestione* il primo obiettivo che ci si è posti è stato quello di identificare i rischi effettivi di commissione del reato a cui la Società era esposta.

Ciò ha richiesto innanzitutto, un'attenta analisi *tecnico-giuridica* dei reati richiamati dal Decreto. Tale processo è stato infatti valutato come indispensabile presupposto per la concreta identificazione dei rischi effettivamente rilevabili in Azienda, essendo questo, come sopra accennato, il nostro primo obiettivo.

Il passo successivo alla concreta identificazione del comportamento delittuoso evocato dal Decreto è stato quello di riconoscere quali potessero essere, anche *in astratto*, le modalità e le circostanze con le quali una o più Persone, operative nell'ambito dell'organizzazione dell'Azienda, potessero fare *proprio* il comportamento delittuoso.

1.5.2.2. Individuazione dei processi, dei Soggetti e delle UU.OO. sensibili

A partire dall'identificazione (a volte anche *astratta*) delle modalità di commissione di uno specifico reato-presupposto, esito della fase precedente, si è passati al riconoscimento, sostanzialmente concomitante:

- dei processi e dei sotto-processi aziendali in cui più facilmente può trovare modo di concretizzarsi il comportamento delittuoso;
- dei Soggetti e/o delle UU.OO. più esposte o "sensibili" al rischio di commissione del reato.

Questa fase, sostanzialmente finalizzata alla *mappatura* dei rischi, da una parte, e dei processi e delle UU.OO. sensibili, dall'altra, s'è rivelata assai efficace anche in quanto ha fornito elementi ad integrazione ed arricchimento della fase precedente. Spesso infatti, da un'analisi più dettagliata dei processi svolti presso singole funzioni aziendali è venuta evidenziandosi una nuova modalità di possibile commissione di un reato, precedentemente non rilevata, e, a partire da questa, sono emersi nuovi processi e nuove UU.OO. *sensibili*, precedentemente sfuggiti all'analisi.

L'iterazione ciclica fra queste due prime fasi ha così consentito di raggiungere una mappatura sufficientemente accurata, risultato difficilmente raggiungibile laddove tali fasi fossero state eseguite, in sequenza, una sola volta.

1.5.2.3. L'analisi e la valutazione del rischio – Metodo FMEA

La valutazione del rischio, cioè dell'esposizione a pericolo che la società commetta o agevoli la commissione di un reato presupposto è stata condotta mediante la verifica degli standard di controllo individuati dalla *best practice*, ovvero:

1) Esistenza di procedure di regolamentazione interne;
2) Tracciabilità delle operazioni;
3) Segregazione delle funzioni e dei compiti;
4) Presenza di poteri autorizzativi formalmente conferiti.

La classificazione degli standard di controllo è stata eseguita indicando il rischio come Alto, Medio o Basso, in relazione all'esistenza ed all'adeguatezza degli standard di controllo adottati da Informatica Alto Adige S.p.A. e attutati:

- Rischio Alto = gli standard di controllo non sono rispettati
- Rischio Medio = gli standard sono rispettati solo in parte
- Rischio Basso = gli standard sono rispettati

La misurazione del "rischio netto" ossia la determinazione del livello di esposizione a pericolo di commissione dei reati presupposto rilevanti e del livello di accettabilità del rischio è stata eseguita utilizzando la metodologia FMEA (*Failure Mode and Effect Analysis*), utilizzata per analizzare le modalità di guasto o di difetto di un processo, prodotto o sistema.

Si noti che il termine "guasto" qui non è utilizzato nel suo significato corrente di "rotto", ma denota un'anomalia che non permette al componente di svolgere correttamente la sua funzione e di conseguenza ha delle ripercussioni più o meno gravi sul funzionamento del sistema di cui fa parte.

Il *failure mode* è l'espressione di come il guasto o difetto si manifesta nel processo, mentre per *effect* si intende l'impatto del guasto o difetto sul processo.

Attraverso l'applicazione della metodologia FMEA è possibile:

- individuare preventivamente i potenziali modi di guasto che possono verificarsi durante l'applicazione del processo;
- determinare le cause dei modi di guasto riferite al processo;
- valutare gli effetti dei modi di guasto in ottica del rischio della commissione di reati 231;
- quantificare il gli indici di rischio e stabilire le priorità di intervento per eliminare alla radice le cause dei modi di guasto individuati e/o migliorare i sistemi di controllo;
- identificare le opportune azioni correttive/preventive e valutarne l'impatto complessivo sugli indici di rischio.

L'applicazione sistematica e completa della metodologia FMEA consente anche di:

- disporre di una mappatura sempre aggiornata delle parti/elementi del processo e della loro criticità dal punto di vista della idoneità a prevenire reati, dei relativi modi di guasto e delle fasi del processo dove intervenire per eliminare le cause dei modi di guasto e/o per migliorare i sistemi di controllo;
- documentare e storicizzare i miglioramenti attuati contribuendo alla costruzione di una «memoria tecnica» (*knowledge data base*).

Il primo passo consiste nella scomposizione del processo nelle sue attività elementari. A questo punto, nell'analisi dei "guasti" di ogni attività, occorre:

- Individuare tutti i possibili modi di guasto, e per ciascuno:
  - individuare tutte le possibili cause (p.es. mancanza adeguati controlli preventivi, anomalie nella prassi applicativa, etc.)
  - individuare tutti i possibili effetti (rischio commissione reati 231)
  - individuare tutti i controlli in essere (a prevenzione o a rilevamento del modo di guasto – classificazione degli standard di controllo)

Per tutte le combinazioni modo di guasto - causa si devono valutare tre fattori:

- P – probabilità di accadimento (1-10)
- G – gravità dell'effetto (1-10)
- R – possibilità di rilevamento da parte dei controlli (10-1)

Per le voci "P" e "G" 1 rappresenta la condizione di minimo rischio e 10 quella di massimo rischio. Per la voce "R" minore è il punteggio (ad esempio 1) maggiore è la possibilità di rilevamento del modo di guasto.

Probabilità (P)		**Gravità (G)**		**Rilevabilità (R)**	
1	remota	1	irrilevante (sanzione pecuniaria < 100 quote)	1	molto alta
2-3	bassa	2-3	danno lieve (sanzione pecuniaria tra 100 e 200 quote)	2-3	alta
4-6	media/ moderata	4-6	danno moderato, impatto lieve (sanzione pecuniaria tra 200 e 500 quote)	4-6	media/ moderata
7-8	Alta	7-8	danno grave (sanzione pecuniaria tra 200 e 500 quote + sanzione interdittiva)	7-8	bassa
9-10	molto alta	9-10	danno gravissimo permanente (sanzione pecuniaria > 500 quote + sanzione interdittiva)	9-10	remota

L'analisi sopra descritta permette di individuare i modi di guasto più critici mediante l'Indice di Priorità del Rischio (IPR):

IPR = P × G × R

Le azioni di miglioramento del processo o sistema dovranno essere orientate principalmente sui modi di guasto che presentano i più alti valori di IPR.

IPR	**Rischio**	**Priorità di intervento**	**Azioni di miglioramento/correttive**
1 a 50	accettabile/ trascurabile	interventi di monitoraggio	mantenere lo standard di controllo / misure di miglioramento possono essere attuate

51 a 100	medio	interventi di programmazione	gli standard di controllo devono essere modificate/implementate
101 a 1000	elevato	interventi di urgenza	gli standard di controllo devono essere immediatamente attuate

1.5.2.4. Verifica del livello di presidio dei processi a rischio

Raggiunta una visione sufficientemente completa:

- dei rischi effettivi (di commissione di un reato-presupposto) a cui l'Azienda risulta esposta,
- dei processi, dei Soggetti e delle UU.OO. *sensibili* a tali rischi

si è infine passati ad analizzare quale livello di "protezione dai rischi" venisse offerto dalle norme e dalle *procedure* aziendali esistenti ([2]).

Va detto che, data la natura dei reati richiamati dal Decreto, per molti di loro è risultato del tutto appropriato richiamare, in primo luogo, i *princìpi*, le *norme di comportamento* ed i *valori* espressi nel *Codice Etico* di *Informatica Alto Adige*, per alcuni reati-presupposto, "scudo" di per sé sufficiente a scongiurare la commissione di reati particolarmente esecrabili, connotati da un elevato disvalore sociale.

Al termine della succitata ricognizione circa il livello di protezione dai rischi offerto dall'insieme del *Codice Etico* e delle procedure esistenti, nei casi in cui tale protezione è stata ritenuta insufficiente, si è proceduto, a seconda delle circostanze:

- ad emettere nuove versioni aggiornate delle procedure esistenti, così da renderle idonee a proteggere rispetto ad un rischio specifico;

oppure

- ad emettere, *ex-novo*, nuove procedure, così da creare una protezione rispetto ad un rischio specifico;
- in alternativa alle due ipotesi precedenti, nei casi in cui, in carenza di protezione, non s'è tuttavia ritenuto opportuno procedere come sopra descritto, le norme ed i controlli necessari a proteggere dal rischio di commissione di un determinato reato sono stati direttamente inseriti, con pari efficacia prescrittiva, nella *Sezione speciale* del presente *Modello di organizzazione e gestione*.

Al termine di tali attività, s'è provveduto a consolidare il presente *Modello di organizzazione e gestione*, recependo in esso:

- i protocolli e le norme
- i controlli

ritenuti indispensabili al raggiungimento di un'efficace protezione dal rischio di commissione di uno qualunque dei reati-presupposto previsti dal D. Lgs. 231/01.

In conclusione, nella *Sezione speciale* del *Modello*, sono stati quindi riportati, per ciascun reato-presupposto:

- la *descrizione sintetica del reato* e, laddove necessario, alcune esemplificazioni dello stesso
- la *contestualizzazione aziendale*: processi/UU.OO. sensibili e possibili modalità di commissione
- la *descrizione del comportamento prescritto,* delle norme e dei protocolli

([2]) Di seguito, nel presente *Modello*, per semplicità si farà riferimento a documenti aziendali contenenti norme e prescrizioni utilizzando il termine "*procedura*". Con tale termine, tuttavia, si farà implicito riferimento anche a tipologie di documenti (come "*regolamenti*", "*circolari*", ecc.) che formalmente non si presentano come *procedure*, pur avendone lo stesso valore prescrittivo in relazioni a specifiche attività o a determinati processi aziendali.

- la *descrizione sintetica dei controlli applicati*
- *i riferimenti ai documenti aziendali* contenenti le norme ed i protocolli.

1.5.2.5. Revisione del Modello

Il presente *Modello di organizzazione e gestione* è soggetto a periodiche verifiche, soprattutto in ottica di efficacia rispetto agli obiettivi per i quali è stato predisposto e di garanzia di effettiva attuazione di quanto previsto dal *Modello* stesso. In questa attività di verifica il ruolo principale è svolto dall'*Organismo di Vigilanza* (istituto di seguito dettagliatamente descritto), che potrà avvalersi, in proposito, dell'apporto informativo a lui fornito dalla funzione di *Internal Auditing*.

Eventi che possono determinare la revisione del *Modello* sono i seguenti:

- il manifestarsi di significative violazioni delle prescrizioni contenute nel *Modello* (o nelle procedure da esso richiamate), tali da evidenziare, anche indirettamente, una vulnerabilità rispetto al rischio di commissione di un determinato reato;
- variazioni intervenute nell'organizzazione dell'Azienda o nei processi aziendali, laddove le une e/o le altre richiedano un aggiornamento della "mappatura" delle tre entità: rischio da reato – Soggetti o UU.OO. sensibili – processi/sottoprocessi sensibili e, conseguentemente, una verifica delle norme, dei protocolli e dei controlli da prevedere a protezione del rischio;
- modifiche o integrazioni al D.Lgs. 231/01 attuate dal Legislatore, con introduzione di nuovi reati-presupposto (precedentemente non compresi nell'ambito) o con interventi di modifica rispetto a reati già previsti dal Decreto.

In tutti i casi, a prescindere dalla motivazione che ha innescato il processo di revisione del *Modello*, vengono replicate le tre fasi operative che hanno portato alla stesura della prima versione del presente *Modello*, già precedentemente descritte.

Ogni intervento di revisione del *Modello* sarà ovviamente seguito dalle fasi di approvazione e pubblicazione di seguito trattate.

Si precisa che *non* costituisce "*revisione del Modello*" la semplice modifica di uno o più dei documenti dallo stesso richiamati (referenziati nella *Sezione speciale* del presente documento). Coloro che, nell'applicazione di quanto previsto dal presente Modello, si trovano a dover far riferimento ai citati documenti, sono tenuti ad accedere all'ultima versione degli stessi disponibile all'interno della rete *intranet*.

Approvazione del Modello e sua pubblicazione

Ai fini della sua promulgazione, il presente *Modello di organizzazione e gestione* è soggetto all'approvazione del Consiglio di Amministrazione della Società ("*CdA*").

In occasione di una revisione del *Modello*, laddove le modifiche apportate non rivestano caratteristiche di particolare urgenza, tale approvazione interverrà in occasione del primo *CdA* utile. Diversamente il Presidente, eventualmente su sollecitazione dell'*Organismo di Vigilanza*, convocherà anticipatamente un apposito *CdA* per l'approvazione della nuova versione del Modello.

Una volta approvato, il *Modello di organizzazione e gestione* viene pubblicato all'interno della rete intranet aziendale.

La promulgazione di una nuova versione del *Modello* viene sempre accompagnata da una contestuale comunicazione interna, via e-mail, destinata a tutti i Dipendenti, con la quale si segnala la disponibilità, nella intranet, della nuova versione e si precisano, sinteticamente, le ragioni che hanno motivato l'aggiornamento.

Destinatari e ambito d'applicazione del Modello

Il Decreto sancisce che l'Ente è ritenuto responsabile nel caso di reati commessi nel suo interesse o a suo vantaggio dai seguenti Soggetti:

- Persone che rivestono funzioni di rappresentanza o di amministrazione;

- Persone che rivestono funzioni di direzione dell'Ente o di una sua Unità Organizzativa autonoma (ad esempio, di una sede secondaria);
- Persone che esercitano, anche di fatto, la gestione o il controllo dell'Azienda;
- Persone sottoposte alla direzione o alla vigilanza di qualunque Soggetto menzionato nei punti precedenti.

Oltre a tali Destinatari, prevalentemente, ma non *necessariamente* Dipendenti della Società, tutti comunque operanti nell'ambito delle attività svolte dall'organizzazione aziendale, sono tenuti a conformarsi alle norme ed ai princìpi richiamati dal presente *Modello* tutti coloro che instaurano relazioni con *Informatica Alto Adige* (regolate o meno da un rapporto contrattuale): Clienti, Partner e Fornitori.

L'Organismo di Vigilanza

Presupposti alla sua istituzione

Il D.Lgs. 231/2001 prevede che l'adozione di un modello di organizzazione e gestione sia accompagnata dalla individuazione ed istituzione di un apposito *Organismo di Vigilanza* (di seguito anche "*OdV*").

Più precisamente, tale organismo è disciplinato dall'articolo 6 del decreto in questione, ai sensi del quale l'Ente non risponde dei reati eventualmente compiuti anche o solo nell'interesse o a vantaggio dell'Ente stesso, qualora quest'ultimo dia prova, tra l'altro, (a) che è stato preventivamente adottato un valido modello di organizzazione; (b) che "*il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato a un organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo*".

In sostanza, in base al citato articolo 6, il c.d. "*scudo protettivo*" che dovrebbe mettere l'Ente al riparo dalle conseguenze derivanti dalla commissione di un reato da parte di un Soggetto che riveste al suo interno una posizione *apicale* (così come definita dal Decreto), risulta realizzato, oltre che da un valido modello di organizzazione e gestione, anche dalla istituzione di un idoneo *Organismo di Vigilanza*.

Per quanto, invece, riguarda i reati compiuti dai c.d. Soggetti *non apicali* (così come definiti dall'articolo 5, comma 1, lett. b, del D.Lgs 231/01), si deve segnalare che non è richiesta con altrettanta chiarezza l'individuazione o l'istituzione di tale organismo di controllo. In realtà, però, si deve rilevare che l'articolo 7 del medesimo decreto, che appunto disciplina i reati compiuti dai Soggetti non apicali, prevede che il modello, per poter validamente proteggere l'Ente, debba essere efficacemente attuato, precisando poi che l'efficace attuazione del modello richiede, tra l'altro, "*una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività*". È chiaro, quindi, che tale periodica verifica non potrà che essere svolta da un idoneo Organismo di Vigilanza.

Requisiti dell'OdV e dei singoli Membri, cause di ineleggibilità e di decadenza

Di seguito si descrivono i requisiti che, sulla base dell'interpretazione del art. 6 del D.Lgs. 231/01, devono caratterizzare un Organismo di Vigilanza:

a) **Autonomia ed indipendenza**: l'Organismo deve essere dotato di autonomia ed indipendenza rispetto agli organi direttivi dell'Ente, in modo da poter svolgere al meglio il suo ruolo. Tale autonomia ed indipendenza non richiedono soltanto l'assenza di ogni forma di subordinazione gerarchica, ma anche il mancato conferimento di poteri operativi e decisionali. Infatti, la presenza di tali poteri in capo all'organismo potrebbe, in alcuni casi, pregiudicare e compromettere i citati requisiti di autonomia ed indipendenza, comportando un'intollerabile coincidenza tra Soggetto controllore e controllato.

b) **Natura interna all'Ente**: come si ricava dall'art. 6 del D.Lgs. 231/01, le funzioni di vigilanza rimesse all'Organismo non possono essere integralmente affidate all'esterno, neppure attraverso dinamiche di *outsourcing*. Ciò, però, non significa, come di seguito verrà meglio precisato, che non possa farsi ricorso a consulenti esterni, la cui presenza garantisce invero in modo significativo l'autonomia e l'indipendenza dal Vertice della Società.

c) **Professionalità**: l'Organismo deve essere dotato di adeguati poteri e di competenze professionali appropriate al fine di garantire uno svolgimento efficace dei compiti di vigilanza previsti dal D.Lgs. 231/01. Ciò comporta, in caso di organo di controllo di natura collegiale, la scelta di membri aventi le conoscenze e le professionalità richieste per l'espletamento delle funzioni, quali la conoscenza della struttura interna dell'Ente, le competenze in materie aziendalistiche, organizzative e quelle prettamente giuridico-penalistiche. Tale necessaria professionalità, sempre nel caso di organismo di controllo di natura collegiale, può essere realizzata anche attraverso il ricorso ad uno o più consulenti esterni.

d) **Continuità di azione**: la costante attività di vigilanza e controllo richiesta dal D.Lgs. 231/01 impone che l'organismo in questione sia in grado di garantire una sufficiente continuità della sua azione. Ciò significa, pertanto, che tale organismo deve garantire una continua operatività, nonché, ove necessario, una costante presenza nell'azienda.

Possono essere nominati membri dell'OdV i Soggetti in possesso delle professionalità necessarie per l'espletamento delle funzioni e/o che abbiano maturato specifica esperienza in ambito aziendale. In particolare, le competenze richieste afferiscono alle materie giuridiche, economiche, finanziarie e alle scienze organizzative e aziendalistiche.

I membri dell'Organismo possono ricoprire funzioni o cariche in ambito aziendale, purché queste non comportino a titolo individuale poteri gestionali di amministrazione attiva incompatibili con l'esercizio delle funzioni dell'Organismo.

Costituiscono cause di ineleggibilità dei componenti dell'OdV:

- la condanna, anche in primo grado, o l'applicazione della pena su richiesta ex artt. 444 e ss. c.p.p. per uno dei reati previsti dal D. Lgs. 231/2001;
- la condanna, anche in primo grado, a pena che comporta l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea, dagli uffici direttivi delle persone giuridiche e delle imprese;
- la condanna anche in primo grado o l'applicazione della pena su richiesta ex artt. 444 e ss. c.p.p. per reati contro la pubblica amministrazione, per reati finanziari, o per reati che comunque incidano sull'affidabilità morale e professionale del Soggetto;
- la condizione giuridica di interdetto, inabilitato o fallito;
- l'esercizio o il potenziale esercizio di attività in concorrenza o in conflitto di interessi con quella svolta dalla Società;
- l'irrogazione di una sanzione da parte della Consob per aver commesso in Società quotate, uno degli abusi di mercato di cui al D.Lgs. n. 58/1998.

I membri dell'Organismo di Vigilanza devono dichiarare, sotto la propria responsabilità, di non trovarsi in alcuna delle situazioni di ineleggibilità o in altra situazione di conflitto d'interessi, con riguardo alle funzioni/compiti dell'Organismo di Vigilanza, impegnandosi, nel caso in cui si verificasse una delle predette situazioni (e fermo restando, in tale evenienza, l'assoluto e inderogabile obbligo di astensione), a darne immediata comunicazione al Consiglio di Amministrazione, onde consentire la sostituzione nell'incarico.

Costituiscono cause di decadenza dei componenti dell'OdV:

- la condanna in secondo grado o l'applicazione della pena su richiesta ex artt.444 e ss. c.p.p. per uno dei reati previsti dal D.Lgs. 231/2001;
- la condanna in secondo grado a pena che comporta l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea, dagli uffici direttivi delle persone giuridiche e delle imprese;
- la condanna in secondo grado o l'applicazione della pena su richiesta ex artt.444 e ss. c.p.p. per reati contro la pubblica amministrazione, per reati finanziari, o per reati che comunque incidano sull'affidabilità morale e professionale del Soggetto;
- la condizione giuridica di interdetto, inabilitato o fallito;
- l'esercizio o il potenziale esercizio di attività in concorrenza o in conflitto di interessi con quella svolta dalla Società;
- l'irrogazione di una sanzione da parte della Consob per aver commesso in Società quotate, uno degli abusi di mercato di cui al D.Lgs. n. 58/1998;
- l'omessa comunicazione di una situazione di incompatibilità o di conflitto di interessi con riguardo alle funzioni/compiti dell'Organismo di Vigilanza o la violazione, in tali ipotesi, dell'obbligo di astensione.

Durata in carica e cessazione

All'atto dell'istituzione dell'*Organismo di Vigilanza*, il CdA di *Informatica Alto Adige* stabilisce, a sua discrezione, che i Componenti dell'OdV restano in carica fino a loro revoca (deliberata dallo stesso CdA) ovvero fino allo scadere di un precisato periodo di tempo. Lo stesso vale per i successivi *rinnovi* dell'OdV.

La cessazione dalla carica dei componenti dell'OdV è determinata - oltre che dalla revoca - da rinuncia, decadenza, impedimento permanente e, per quanto riguarda i membri interni alla Società nominati in ragione della funzione aziendale ricoperta, dal venir meno della titolarità di tale funzione.

La rinuncia da parte dei membri dell'OdV può essere esercitata in qualsiasi momento e deve essere comunicata al Consiglio di Amministrazione per iscritto, unitamente alle motivazioni che l'hanno determinata. La rinuncia ha effetto immediato, se rimane in carica la maggioranza dei membri dell'Organismo o, in caso contrario, dal momento in cui la maggioranza dell'Organismo si è ricostituita, in seguito all'accettazione dei nuovi membri.

La revoca dell'incarico conferito a uno o più membri dell'Organismo di Vigilanza può essere deliberata dal Consiglio di Amministrazione, sentito il parere non vincolante del *Collegio sindacale*, per giusta causa.

Per giusta causa di revoca deve intendersi:

- un grave inadempimento ai propri doveri/funzioni, così come definiti nel Modello;
- la condanna della Società, ai sensi del Decreto, anche con provvedimento non ancora passato in giudicato, motivato sulla base della "omessa o insufficiente vigilanza" da parte dell'Organismo;
- il verificarsi di una delle cause di decadenza;
- la violazione del divieto di comunicazione e diffusione delle informazioni.

In caso di cessazione per qualunque causa di un membro dell'Organismo, il Consiglio di Amministrazione provvede senza ritardo alla sua sostituzione con un'apposita delibera. In tal caso, il componente sostituto dura in carica fino alla scadenza degli altri membri dell'OdV.

In caso di cessazione del Presidente, le relative funzioni sono assunte, fino all'accettazione del nuovo Presidente, dal membro più anziano.

L'OdV e ciascuno dei suoi membri, nonché coloro dei quali l'OdV si avvarrà per l'espletamento delle proprie funzioni (siano questi Soggetti interni che esterni alla Società), non potranno subire conseguenze ritorsive di alcun tipo per effetto dell'attività svolta.

Convocazione, voto e delibere

Le riunioni dell'OdV sono convocate dal Presidente, ovvero su richiesta congiunta degli altri membri e sono valide con la presenza della maggioranza dei membri.

Le delibere dell'Organismo sono adottate a maggioranza assoluta e motivate con espressa indicazione dell'eventuale posizione minoritaria.

È fatto obbligo a ciascun membro dell'Organismo di dare notizia agli altri membri di ogni interesse in conflitto, per conto proprio o di terzi, con un'attività dell'Organismo, precisandone in particolare la natura, i termini, l'origine e la portata, astenendosi in ogni caso dal partecipare alle deliberazioni riguardanti l'attività stessa. Nel caso in cui al membro sia stata delegata un'attività, lo stesso deve astenersi dal compierla e investire della questione l'intero Organismo.

Conservazione delle informazioni e divieto di comunicare

Presso l'Organismo è conservata, per un periodo minimo di dieci anni, copia cartacea e/o informatica di tutto il materiale relativo all'attività svolta.

A tal fine, la Società dota l'Organismo di strutture idonee alla conservazione del materiale su indicato.

L'accesso all'archivio da parte di Soggetti terzi deve essere preventivamente autorizzato dall'Organismo e svolgersi secondo modalità dallo stesso stabilite.

Su nomina del Titolare del trattamento, i membri dell'Organismo assumono, per quanto attiene alla gestione della casella e-mail e degli archivi cartaceo e informatico, la qualifica di Responsabili del trattamento dei dati personali ai sensi del D.Lgs. n.196/2003, e adottano ogni cautela idonea a preservare i dati stessi, garantendo un backup dei dati con cadenza trimestrale.

I Componenti dell'OdV, i Componenti delle strutture aziendali e i Consulenti di cui esso dovesse avvalersi, non possono comunicare o diffondere notizie, informazioni, dati, atti e documenti acquisiti nell'esercizio delle proprie attività, fatti salvi gli obblighi di comunicazione previsti dal *Modello* e dalle disposizioni vigenti.

Regolamento dell'OdV e relazioni al Vertice della Società

L'Organismo di Vigilanza approva un proprio regolamento che ne disciplina il funzionamento.

L'Organismo di Vigilanza riporta i risultati della propria attività secondo le seguenti modalità:

- rapporto scritto semestrale Presidente;
- rapporto scritto annuale al Collegio sindacale.

L'Organismo di Vigilanza per la esecuzione di specifiche attività di controllo si avvale della funzione di *Internal Auditing*, la quale, ad inizio anno, predispone il piano annuale degli interventi interni all'Azienda.

Funzioni e poteri dell'OdV

In conformità a quanto previsto dal D.Lgs. 231/01, all'Organismo di Vigilanza sono affidate le seguenti funzioni:

a) vigilare sulla reale efficacia ed effettività del *Modello di organizzazione e gestione*, relativamente alla prevenzione dei reati richiamati dal D.Lgs. 231/01;

b) vigilare sul rispetto del *Modello di organizzazione e gestione* e del *Codice etico*;

c) vigilare sulla continua adeguatezza del *Modello di organizzazione e gestione* relativamente alla eventuale intervenuta modifica della struttura aziendale e/o del quadro normativo e curarne l'eventuale aggiornamento.

Per l'effettivo ed efficace svolgimento delle predette funzioni, nonché in conformità a quanto previsto dall'articolo 6, comma 1, lett. b), del D.Lgs. 231/01, all'Organismo di Vigilanza sono riconosciuti i seguenti poteri:

- emanare le disposizioni ritenute necessarie per le attività di vigilanza e controllo, nonché per l'attivazione dei canali informativi di cui ai successivi paragrafi;
- raccogliere e conservare ogni informazione e/o notizia ritenuta utile e rilevante ai fini del decreto in oggetto;
- effettuare, eventualmente anche secondo metodi a campione, ogni opportuna verifica o indagine su operazioni, atti o condotte poste in essere all'interno della Società;
- ricorrere a consulenti esterni di comprovata professionalità;
- elaborare le informazioni e le notizie raccolte, quelle ugualmente pervenute attraverso i canali informativi di cui ai successivi paragrafi, nonché i risultati delle indagini e delle verifiche condotte;
- elaborare le proposte di modifica, aggiornamento e/o implementazione del Modello di organizzazione e gestione e del Codice Etico che dovessero risultare opportune;
- compiere quanto ritenuto opportuno per la diffusione della conoscenza del Modello di organizzazione e gestione all'interno della Società, nonché tra i Soggetti esterni (Collaboratori esterni, Fornitori e Partner) che dovessero entrare in contatto con la Società;
- comunicare per iscritto, al Consiglio di Amministrazione ed al Collegio sindacale la rilevazione di violazioni del *Modello*;
- elaborare, in coordinamento con il Direttore, adeguati metodi per la formazione del personale relativamente al decreto in oggetto (ferma restando la competenza esclusiva dei citati Responsabili per la concreta attuazione degli elaborati metodi);
- elaborare, in coordinamento con la Funzione Finance ed, in particolare, con l'Ufficio Legale, le adeguate clausole contrattuali per una migliore regolamentazione, ai sensi del decreto in oggetto, dei rapporti con Soggetti terzi (ferma restando la competenza esclusiva delle citate Strutture per la concreta attuazione delle elaborate clausole contrattuali);
- accedere liberamente alla documentazione utile per le finalità istituzionali dell'Organismo di Vigilanza in possesso delle diverse Direzioni della Società, degli Amministratori e del Collegio sindacale;
- ricevere periodicamente, dai Soggetti individuati nel presente Modello, le informazioni indicate nel paragrafo "*Flussi informativi*"

- promuovere, ferma la competenza del vertice della Società per l'irrogazione delle sanzioni e del relativo procedimento disciplinare, l'applicazione di eventuali sanzioni disciplinari, anche nel caso di omesso invio all'OdV dei *Flussi informativi* richiesti;
- coordinare il monitoraggio delle attività in relazione ai princìpi stabiliti dal *Modello*, anche con il supporto delle diverse funzioni aziendali indicendo, quando opportuno, apposite riunioni.

L'OdV è chiamato ad assolvere i seguenti ulteriori compiti in materia di anticorruzione e trasparenza, meglio individuate e specificate nel documento "Misure integrative di prevenzione della corruzione":

- verificare, unitamente al Responsabile della Prevenzione della Corruzione e Trasparenza, che le Misure integrative di prevenzione della corruzione rispettino i protocolli di prevenzione dei reati ex D.lgs. 231/2001 definiti dal Modello di Organizzazione;
- collaborare con il Responsabile della Prevenzione della Corruzione e Trasparenza al fine di assicurare la copertura di tutti i processi aziendali a rischio corruzione attiva e passiva con gli opportuni protocolli di prevenzione;
- condividere con il Responsabile della Prevenzione della Corruzione e della Trasparenza il probramma di vigilanza al fine di integrare e coordinare i controlli effettuati da ciascun organismo di controllo nei propri ambiti di competenza.

Al fine di assicurare l'autonomia e l'indipendenza dell'OdV, annualmente lo stesso viene dotato dal Consiglio di Amministrazione di un budget da utilizzare per l'espletamento dei propri compiti. L'Organismo non è tenuto a fornire alcun rendiconto delle somme utilizzate, se non su esplicita richiesta del Consiglio di Amministrazione.

Linee di reporting verso l'Organo Amministrativo

L'OdV provvede a riferire periodicamente all'organo amministrativo attraverso la predisposizione di un apposito rapporto scritto avente ad oggetto l'attività svolta e le eventuali criticità emerse nello svolgimento delle proprie funzioni.

L'Organismo di Vigilanza riferisce in merito all'attuazione del Modello Organizzativo ed all'emersione di eventuali criticità.

Sono previste le seguenti linee di reporting dell'OdV:

- con cadenza almeno annuale, un rapporto scritto relativo all'attività svolta (indicando in particolare i controlli e le verifiche specifiche effettuati e l'esito degli stessi, l'eventuale aggiornamento della mappa delle aree e dei processi sensibili, ecc.) e ad eventuali criticità emerse nello svolgimento delle proprie mansioni;
- tempestivamente, una segnalazione relativa al verificarsi di situazioni straordinarie quali ipotesi di violazione dei principi di attuazione del Modello Organizzativo ovvero ipotesi di violazione riscontrate nell'ambito di operazioni o atti specifici posti in essere da aree aziendali a rischio-reato, o di modifiche legislative in materia di responsabilità amministrativa degli enti e di operazioni di finanza straordinaria che attengano al perimetro di attuazione del Modello Organizzativo;
- tempestivamente, in merito alle violazioni accertate del Modello Organizzativo, nei casi in cui tali violazioni possano comportare l'insorgere di una responsabilità in capo alla Società.

L'organo amministrativo ha la facoltà di convocare in qualsiasi momento l'OdV. Ogni tipo di rapporto/riunione disciplinato al presente paragrafo dovrà trovare riscontro in forma scritta che dovrà essere idoneamente archiviata.

Flussi informativi verso l'Organismo di Vigilanza

L'Organismo di Vigilanza è destinatario dei flussi informativi relativi all'attuazione del *Modello di organizzazione e gestione* e del *Codice Etico*, secondo i canali di informazione attivati in conformità a quanto previsto dall'articolo 6, comma 2, lett. d), del D.Lgs. 231/01.

Il Presidente nomina i *Responsabili flussi informativi 231*, che vengono individuati all'interno del *Management* della Società (Responsabili di Direzione e/o di Reparto).

I Dipendenti della Società ed, in particolare, i "*Responsabili interni della fornitura dei flussi informativi ex D.Lgs. 231/01*" (per brevità: "*Responsabili flussi informativi 231*")) hanno l'obbligo di trasmettere all'Organismo di Vigilanza quanto segue:

- i provvedimenti e/o le notizie provenienti dalla Pubblica Amministrazione dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti (cfr. articolo 8 del D.Lgs. 231/01), per uno o più dei reati previsti dal medesimo decreto;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti relativamente ad un procedimento giudiziario per uno o più dei reati previsti dal D.Lgs. 231/01;
- i rapporti redatti dai Responsabili di ogni Direzione della Società, dai quali possano emergere fatti, atti e condotte, anche omissive, potenzialmente rilevanti ai sensi del D.Lgs. 231/01;
- le notizie relative all'instaurazione ed alla conclusione di procedimenti disciplinari, ivi comprese le sanzioni irrogate ed i provvedimenti di archiviazione, relativi alla violazione del *Modello di organizzazione e gestione*;
- adozione di sistemi organizzativi di gestione;
- le decisioni relative alla richiesta, erogazione ed impiego di finanziamenti e contributi pubblici;
- il sistema di deleghe e procure adottate dalla Società ed ogni loro successiva modifica;
- cambiamenti organizzativi aziendali;
- modifiche nell'assetto societario o nell'operatività dell'impresa.

Tutte le comunicazioni inviate all'*Organismo di Vigilanza* della Società devono avere forma scritta e possono essere inoltrate, , tramite e-mail, all'indirizzo **231@siag.it** messo a disposizione dall'Organismo.

-

Formazione e informazione del Personale e dei Contraenti esterni

Ai fini del buon funzionamento del *Modello di organizzazione e gestione* è necessario che tutti i suoi protocolli siano oggetto di una diffusione capillare, efficace ed autorevole.

È inoltre opportuno che tale processo di comunicazione sia accompagnato da un adeguato programma di formazione rivolto al personale delle aree a rischio, allo scopo di illustrare le ragioni di opportunità, a fianco a quelle giuridiche, che ispirano le regole e la loro portata concreta. Detto processo di formazione e informazione dei lavoratori deve avvenire mediante un sistema che preveda una comunicazione adeguata, chiara, dettagliata e periodicamente ripetuta.

Il Responsabile della Funzione HR cura, sulla base delle indicazioni e proposte provenienti dall'Organismo di Vigilanza, la formazione del personale relativamente al contenuto del D.Lgs. 231/01, del *Modello di organizzazione e gestione* e del *Codice Etico* della Società.

L'Organismo di Vigilanza promuove l'informazione e la formazione del personale sui contenuti del *Modello*, in collaborazione ed in coordinamento con i Responsabili delle strutture aziendali che si ritiene più opportuno coinvolgere.

Quanto alla formazione del personale:

1) per i neo-assunti: al momento dell'assunzione viene fornito loro un documento di autoformazione sui contenuti del D.Lgs. 231/01;

2) per tutto il personale (Soggetti in posizione *apicale* e non):

- tutto il Personale è destinatario di un corso di formazione/aggiornamento sui contenuti del *Codice Etico* e del *Modello di Organizzazione e Gestione ex D.Lgs. 231/01*,
- ciascuna verifica condotta dalla funzione di *Internal Auditing* presso una determinata Unità Organizzativa prevede una specifica sessione formativa rivolta ai Referenti della stessa, finalizzata a richiamare l'importanza di un rigoroso rispetto dei princìpi e delle norme contenute nel *Codice Etico* e nel *Modello di Organizzazione e Gestione ex D.Lgs. 231/01*, nonché a richiamare la tipologia di reati a cui l'Unità Organizzativa risulta particolarmente esposta;
- l'adozione del *Modello* e, successivamente, l'emissione dei suoi aggiornamenti, è comunicata a tutte le Risorse operanti in Azienda, previa pubblicazione della nuova versione all'interno della rete *intranet*, con l'invio di una e-mail illustrativa ed esplicativa.

Il Management della Società può, sulla base delle indicazioni e proposte provenienti dall'Organismo di Vigilanza, introdurre nuovi ed ulteriori criteri di selezione dei terzi contraenti con la Società (Collaboratori esterni, Fornitori, Partner, etc.) che garantiscano in misura ancora maggiore la Società rispetto alla commissione di reati.

Il Management cura, anche sulla base delle indicazioni e proposte provenienti dall'Organismo di Vigilanza, l'informativa ai terzi contraenti con la Società (Collaboratori esterni, Fornitori, Partner, etc.) relativamente al Decreto Legislativo 231/2001 ed alle misure di prevenzione adottate dalla Società.

I Collaboratori esterni, i Fornitori e i Partner vengono informati, mediante specifiche clausole contrattuali, del loro obbligo di rispettare i princìpi contenuti nel *Codice Etico* di *Informatica Alto Adige*, nonché del loro obbligo di non commettere reati di cui al D.Lgs. 231/01, pena il profilarsi di responsabilità a livello contrattuale.

Whistleblowing

I destinatari del presente Modello organizzativo sono tenuti, a tutela dell'integrità dell'ente, al suo rispetto in ogni sua parte ed al contempo alla vigilanza sul suo rispetto da parte di tutti gli altri destinatari e dipendenti a qualsiasi livello.

A tale fine Informatica Alto Adige S.p.A. ha attivato una procedura di reporting e controllo diffuso sul rispetto della legalità delle operazioni ed attività aziendali, nonché sul rispetto del Modello Organizzativo integrato dalle Misure di Prevenzione della Corruzione e Trasparenza, in base alla quale ogni dipendente può segnalare in buona fede i casi di eventuali illeciti da chiunque commessi all'interno della Società, anche a prescindere dai vincoli gerarchici.

Ogni destinatario del Modello organizzativo, ad ogni livello, ha così il dovere/potere di segnalare alle risorse aziendali individuate e/o all'Organismo di Vigilanza oppure al Responsabile della Prevenzione della Corruzione e Trasparenza, condotte illecite rilevanti ai sensi del D.lgs. 231/2001 o di violazioni del Modello della Società, nonché condotte illecite rilevanti ai sensi della L. 190/2012, e fondate su elementi di fatto precisi e concordanti, di cui siano venuti a conoscenza in ragione delle funzioni svolte.

La società ha adottato, nelle forme e con le garanzie di cui all'art. 6, co. 2bis, D.lgs. 231/2001 e all'art. 54bis, D.lgs. 165/2001, più canali, che consentono ai dipendenti e collaboratori interni di presentare segnalazioni circostanziate di condotte illecite, garantendo, anche con modalità informatica, la riservatezza dell'identità del segnalante. La procedura di segnalazione è meglio descritta nella sezione II del presente Modello, nonché nel documento "Misure integrative di prevenzione della corruzione".

Le sanzioni a tutela del sistema di controllo diffuso e le tutele del segnalante sono descritte nell'apposito documento "Meccanismi di segnalazione di violazioni delle regole aziendali (Whisleblowing).

[redacted]Il Sistema disciplinare

[redacted]Introduzione

Ai sensi dell'articolo 6, comma 2, lett. e), del D.Lgs. 231/01, il *Modello di organizzazione e gestione* deve prevedere un idoneo sistema disciplinare in grado di sanzionare il mancato rispetto del *Modello* stesso.

Si tratta di un elemento imprescindibile, in assenza del quale difficilmente potrebbe operare con pieno effetto, a favore della Società, il c.d. "scudo protettivo" contro le conseguenze previste dal D.Lgs. 231/01.

Un siffatto apparato sanzionatorio deve essere efficace, ma al tempo stesso pienamente conforme alla disciplina giuslavoristica vigente nel nostro ordinamento (in particolare: articoli 2104 e ss. del codice civile; articolo 7 della legge n. 300/1970; articolo "*Provvedimenti disciplinari*" del *Contratto Collettivo Nazionale di Lavoro del Terziario* e analogamente, per il Personale in comando, per quanto attiene al *Contratto Collettivo Provinciale*).

A tale scopo, in conformità a quanto prescritto dall'articolo 7 della legge n. 300/1970 (c.d. Statuto dei Lavoratori) il Presidente ed il Direttore, in coordinamento con l'Organismo di Vigilanza, provvedono ad assicurare la piena conoscenza del *Modello di organizzazione e gestione*, anche attraverso la disponibilità del medesimo in *luoghi* accessibili a tutti i Dipendenti. La suddetta disponibilità ha, in particolare, lo scopo di assicurare che i Dipendenti abbiano la piena conoscenza dell'*impianto sanzionatorio* previsto dal *Modello di organizzazione e gestione*. In ossequio alla citata prescrizione contenuta nella L. 300/70, la Società provvede a pubblicare il *Codice Etico* nel portale internet (**www.siag.it**), ed il *Modello di Organizzazione e Gestione ex D.Lgs. 231/01* in apposita sezione del sito intranet aziendale.

L'applicazione delle sanzioni disciplinari è indipendente ed autonoma rispetto all'esito di un eventuale procedimento penale.

[redacted]Il sistema sanzionatorio per il Personale non dirigente

Per i *Dipendenti* l'osservanza delle norme del *Codice Etico* e del *Modello di Organizzazione e Gestione ex D.Lgs. 231/01* deve considerarsi parte essenziale degli obblighi contrattuali dagli stessi assunti ai sensi e per gli effetti dell'art. 2104 del Codice Civile; pertanto, i comportamenti tenuti in violazione del *Codice Etico* o del *Modello di Organizzazione e Gestione 231/01* sono considerati inadempimento degli obblighi primari del rapporto di lavoro ed hanno rilevanza disciplinare. Il procedimento disciplinare, l'irrogazione della sanzione, l'esecuzione, la contestazione e l'impugnazione della stessa sono disciplinati in conformità a quanto previsto dallo *Statuto dei Lavoratori*, dal *Contratto Collettivo Nazionale di Lavoro* del Terziario e dal *Contratto Collettivo Provinciale* (per il Personale in comando).

In coerenza con le richiamate regolamentazioni legislative e contrattuali, l'inosservanza delle norme del *Codice Etico* e del *Modello di Organizzazione e Gestione ex D.Lgs. 231/01* espone il Personale a sanzioni disciplinari che saranno decise ed applicate dal Direttore, che valuterà tipologia ed entità dell'inosservanza, tenendo conto:

- dell'intenzionalità del comportamento o del grado di negligenza, imprudenza o imperizia evidenziata;
- del comportamento complessivo del Dipendente, con particolare riguardo alla sussistenza o meno di precedenti sanzioni disciplinari;
- della posizione funzionale e delle mansioni del Dipendente coinvolto;
- di eventuali altre circostanze collegate alla violazione, in particolare del fatto che essa attenga a reati "*di particolare rilevanza*", fra i quali vengono ricompresi, oltre ai reati inerenti la mancata tutela della salute e della sicurezza sul lavoro, anche i seguenti (in virtù della tipologia delle attività svolte in Azienda):
  - reati inerenti i rapporti con la P.A.,
  - reati informatici.

A tal proposito, le seguenti possono essere considerate indicazioni a cui far riferimento (da valutare nell'ordine con cui vengono esposte):

- si considera applicabile il *rimprovero verbale* nei casi in cui siano tutte vere le seguenti circostanze:

- non risulta evidente l'intenzionalità del comportamento o lo stesso evidenzia un grado lieve di negligenza, imprudenza o imperizia;
- nel passato al Dipendente responsabile del comportamento sanzionato non furono mai comminati provvedimenti disciplinari per reati ex D.Lgs 231/01;
- il comportamento non attiene a reati "*di particolare rilevanza*" (come sopra identificati);

➢ si considera applicabile una sanzione non più lieve del *licenziamento* nei casi in cui siano tutte vere le seguenti circostanze:

- risulta evidente l'intenzionalità del comportamento e lo stesso evidenzia un grado elevato di negligenza, imprudenza o imperizia;
- nel passato al Dipendente responsabile del comportamento sanzionato furono già comminati provvedimenti disciplinari, diversi dal *rimprovero verbale*, per reati ex D.Lgs 231/01;
- il comportamento attiene a reati "*di particolare rilevanza*";

➢ si considera applicabile una sanzione non più lieve del rimprovero scritto e/o della multa e/o della sospensione nei casi che non rientrano nelle casistiche sopra descritte.

È compito dell'Organismo di Vigilanza monitorare il sistema sanzionatorio contenuto nel *Modello di organizzazione e gestione*, nonché elaborare le eventuali proposte di modifica da inoltrare al Consiglio di Amministrazione.

Il sistema sanzionatorio per il Personale dirigente

Laddove i Dirigenti, qualora presenti nell'organico della Società, si rendessero responsabili di violazioni delle norme e delle prescrizioni contenute nel *Codice Etico* o nel *Modello di Organizzazione e Gestione ex D.Lgs. 231/01*, ovvero nel caso in cui avessero violato lo specifico obbligo di vigilanza sui sottoposti, saranno applicabili nei confronti dei medesimi Dirigenti le misure più idonee, in conformità a quanto previsto dalla legge, dal *Contratto Collettivo Nazionale di Lavoro per i Dirigenti delle aziende del Terziario* e dal *Contratto Collettivo Provinciale* (nel caso di Dirigente in comando), nel rispetto del criterio di proporzionalità di cui all'art. 2106 del codice civile.

Altre misure di tutela

Qualora gli Amministratori o i Sindaci della Società si rendessero responsabili di violazione delle procedure previste dal *Modello di organizzazione e gestione* o dell'adozione di un comportamento non conforme a quanto prescritto dal medesimo *Modello* o dal *Codice Etico* della Società, l'Organismo di Vigilanza informerà senza indugio il *Consiglio di Amministrazione* ed il *Collegio sindacale* affinché sia adottato ogni provvedimento ritenuto opportuno e previsto dalla vigente normativa.

A fronte di specifiche clausole presenti all'interno dei contratti stipulati dalla Società con Soggetti terzi (Collaboratori esterni, Fornitori, Partner, etc.), l'eventuale violazione da parte di questi ultimi di quanto previsto dal *Modello di organizzazione e gestione* della Società potrà comportare le conseguenze previste dalle medesime clausole, ivi comprese, a titolo esemplificativo, la risoluzione, il recesso ed il risarcimento dei danni.

Sanzioni a tutela del sistema di controllo diffuso – whistleblowing

In conformità all'art. 6 comma 2bis, D.lgs. 231/01 e dell'art. 54bis, D.lgs. 165/2001 (come modificato dalla L. 179/2017) ed a tutela dell'efficace e corretta applicazione del sistema di controllo diffuso la società ha previsto specifiche sanzioni nei confronti dei soggetti che effettuano segnalazioni con dolo o colpa grave che si rivelano infondate, nonché di chi viola le misure di tutela del segnalante. Le sanzioni sono indicate nella procedura "Whistleblowing" alla quale si rinvia.

2. SEZIONE SPECIALE

Note preliminari

Note sull'approccio adottato nella stesura della Sezione Speciale

Nella presente sezione vengono trattati i reati-presupposto ricompresi nel perimetro del D.Lgs. 231/01. Per ciascuna tipologia di reato:

- viene descritta la fattispecie di riferimento;
- ne viene fornita una contestualizzazione aziendale, dove la descrizione della "*modalità di commissione"* del reato-presupposto scaturisce dall'analisi effettuata del rischio di effettiva commissione del reato;
- vengono descritti sinteticamente norme di comportamento, protocolli e controlli applicati in Azienda a presidio del rischio di commissione del reato-presupposto a cui ci si riferisce, così come vengono forniti i nomi dei documenti aziendali di riferimento. Ciascuna descrizione viene identificata dal codice "*Id. Protoc.*".

La sequenza logica adottata, nei successivi paragrafi, per la trattazione dei vari reati è coerente con la sequenza degli articoli del D.Lgs. 231/01 che richiamano i reati-presupposto.

Nella parte finale verranno trattati i cosiddetti "*reati transnazionali*", non fisicamente *compresi* nel D.Lgs. 231/01, ma introdotti dalla Legge n. 146/2006 che riconosce, per i reati richiamati, la *responsabilità amministrativa degli Enti*, facendo riferimento, per le sanzioni da applicare, a specifici articoli del D.Lgs. 231/01.

Un'ultima considerazione. È stato già precedentemente chiarito che, in linea del tutto generale, *Informatica Alto Adige S.p.A.* eroga i suoi servizi a favore di Clienti appartenenti alla Pubblica Amministrazione. Ciò richiamato, si precisa che il presente *Modello*, dovendo stabilire principi, norme e protocolli di generale applicazione, farà di seguito riferimento a "Clienti" intesi nella più ampia accezione del termine, referenziando, dove il contesto specifico lo richieda, particolari tipologie di Clienti quali: *Stato*, *Ente Pubblico*, *Ente Comunitario*, ecc. Data la natura giuridica delle Società Clienti di SIAG, appare evidente come, nel seguito del presente Modello, l'evocazione di "*eventuali*" rapporti con tale tipologia di Clienti e, specificatamente, con un Ente Pubblico, andrà letta come il richiamo di una situazione che per SIAG è costantemente verificata.

Nota generale relativa al rischio di commissione di reati nei rapporti con la P.A

Da quanto già descritto nel presente documento, emerge che la società *Informatica Alto Adige* risulta completamente controllata, a livello di azionariato, da quelli che sono, oltre che *Soci*, i suoi *esclusivi* Clienti. Va aggiunto che, sulla base di quanto riportato dall'art. 4-BIS dello Statuto di SIAG, "*gli enti titolari del capitale sociale esercitano sulla società un controllo analogo a quello esercitato sui propri servizi*".

A tutto ciò va aggiunta la seguente osservazione: durante la fase di *risk assessment* (come sempre in questi casi) sono stati particolarmente investigati i processi di business attuati da SIAG, ovvero quelli inerenti, anche indirettamente, all'erogazione di forniture di servizi a beneficio dei propri Clienti: quelli del ciclo attivo e passivo (contrattualizzazione, la rendicontazione, la fatturazione, ecc.).

Alla luce delle precedenti considerazioni emerge come il rischio, ancorché astratto, di commissione di reati nei rapporti con la Pubblica Amministrazione risulti, per SIAG, particolarmente modesto. Infatti l'eventuale commissione di un reato ([3]), in presenza di una tale *intrinseca immedesimazione* fra SIAG ed il proprio

([3]) Almeno nell'ambito dei propri processi di business.

"Cliente", determinerebbe una paradossale coincidenza di ruoli: SIAG risulterebbe, contemporaneamente, "reo" e "vittima" dello stesso reato.

Protocolli di particolare rilievo nell'ambito dei Cicli passivo ed attivo.

Procedura di *autorizzazione interna* degli acquisti

In SIAG, ogni acquisto, di qualunque tipologia:

- economale,
- finalizzato all'erogazione di una fornitura (ad esempio un servizio) da parte di SIAG al proprio Cliente, ecc.,

deve puntualmente rispettare una procedura interna dettagliata nel documento "*Regolamento degli acquisti*" (e suoi allegati) a cui qui si rimanda.

Tale *Regolamento* descrive, fra l'altro, le varie fasi del processo di acquisizione, che vanno dalla formulazione (interna) di una richiesta di acquisto, all'autorizzazione interna, fino alla sottoscrizione dell'Ordine/Contratto verso il Fornitore.

Per ogni fase, sono indicati i Soggetti/Responsabili coinvolti ed i limiti di potere:

- autorizzativo interno
- di sottoscrizione di impegni formali verso Terzi (Ordini/Contratti)

che sono riconosciuti ai singoli Soggetti.

Una norma di valenza generale che, essendo indispensabile al fine di prevenire alcuni rischi, è riscontrabile all'interno nel citato Regolamento, è la seguente: un singolo processo di acquisto, dalla richiesta di autorizzazione interna fino al pagamento, non può svolgersi senza il coinvolgimento di almeno due diversi Soggetti.

In SIAG non può essere formalmente emesso (verso Terzi) alcun Ordine/Contratto d'acquisto se i passi preliminari a tale formalizzazione (descritti nel "Regolamento degli acquisti") non sono stati correttamente completati. Naturalmente i citati documenti formali potranno essere sottoscritti solo da specifici Responsabili di SIAG, dotati di adeguati poteri di firma.

Procedura di *autorizzazione interna* delle forniture

Per quanto riguarda il Ciclo attivo e, più precisamente l'autorizzazione del preventivo Costi/Ricavi di una fornitura, SIAG adotta un processo di valutazione, tecnica ed economica, che trova la sua naturale conclusione nell'autorizzazione formale dei valori economici determinati.

La procedura autorizzativa, almeno per quanto riguarda gli aspetti economici, prevede preliminarmente l'identificazione, la valorizzazione e la documentazione (ad esempio, in un foglio di calcolo) delle componenti dettagliate dei costi che si prevede di dover sostenere per l'erogazione della fornitura.

Le valorizzazioni economiche, effettuate sulla base dei documenti disponibili (requisiti condivisi con il Cliente), avranno spesso, almeno per i costi, il significato di *stime*.

Tali valori economici vengono sintetizzati in un documento standard, "*Autorizzazione Preventivo commessa*", che prevede, *a titolo esemplificativo*, le seguenti informazioni:

A) informazioni generali (obbligatorie) di identificazione della fornitura e del suo oggetto: nome del Cliente, oggetto della fornitura, identificativi dei documenti di riferimento (es.: Richiesta d'offerta, Offerta, ecc.), date previste di inizio/fine attività, ecc.;

B) elenco delle varie componenti che possono riscontrarsi nelle forniture di SIAG (da compilare dove applicabili):
   - ✓ gg/u di effort per attività di sviluppo (per tipologia di skill/tariffa),

- ✓ gg/u di effort per attività di servizi di manutenzione a canone,
- ✓ licenze Hw/Sw,
- ✓ impegno del datacenter,
- ✓ costi di subfornitura;
- ✓ costi di sicurezza,
- ✓ costi di trasferte e viaggi,
- ✓ ecc;

C) elenco delle voci finali, di generale applicazione:

- ✓ Totali parziali, Costi e Ricavi, aggregati per tipologia
- ✓ Sconto al Cliente
- ✓ Costi di gestione
- ✓ Importi totali
- ✓ *Contributo di copertura* (valore assoluto e percentuale)
- ✓ IVA

Successivamente a tali informazioni, il modello standard "*Autorizzazione Preventivo commessa*" riporta la seguente dichiarazione:

****

Ai sensi e per gli effetti dell'art. 47 del DPR 445/2000, ciascuno dei Firmatari della presente *Autorizzazione di preventivo*

DICHIARA

che sulla base delle informazioni a sua disposizione:

1) nell'ambito degli ordinari contatti con il Cliente e/o con i Fornitori e nel corso delle attività di valutazione dell'offerta o di allestimento dei documenti correlati (riunioni formali e informali, contatti, conversazioni telefoniche, definizione di ipotesi di accordo, informative, ecc.) NON SI SONO VERIFICATI, da parte di chicchessia, episodi che, anche ipoteticamente, appaiano riconducibili o comunque diretti ad atti rilevanti ai sensi del D.Lgs. 231/2001, in qualunque forma finalizzati a favorire l'acquisizione del Contratto da parte di *Informatica Alto Adige S.p.A.* o, comunque, atti finalizzati a compensare, anche in futuro o indirettamente, il responsabile di illeciti comportamenti volti a produrre un vantaggio per la Società;
2) nelle fasi successive alla sottoscrizione della presente Dichiarazione e fino al completo espletamento della fornitura, qualora si evidenziassero tentativi, episodi o atti anche ipoteticamente inquadrabili fra quelli illeciti sopra richiamati, i Firmatari della presente SI IMPEGNANO formalmente ad inviare immediatamente un'informativa adeguata, fornendo tutti i dettagli noti, all'Organismo di Vigilanza della Società, oltre a comunicare l'evento al proprio Diretto Superiore Gerarchico.

La presente Dichiarazione viene rilasciata nella piena consapevolezza delle Responsabilità che i Firmatari assumono a tutti gli effetti, con particolare riferimento all'obbligo di osservanza del *Modello di Organizzazione e Gestione ex D.Lgs. 231/2001.*

****

Una volta compilato nei campi di cui ai precedenti punti A), B) e C), al di sotto della dichiarazione sopra riportata, il documento standard "*Autorizzazione Preventivo commessa*" andrà sottoscritto per approvazione dal/dai vari Responsabili di Reparto coinvolti nella specifica fornitura.

A tali "*firme*" vanno quindi aggiunte:

- la firma per autorizzazione del Responsabile della Funzione Finance;
- la firma per autorizzazione del Direttore;
- l'ulteriore firma per autorizzazione del Presidente, se l'importo totale del Ricavo supera la *soglia comunitaria* (attualmente: 207.000,00 euro).

Variazioni in corso d'opera. Nel caso di commesse "*chiavi in mano*" di *Importo totale di Ricavo* (inizialmente previsto) maggiore di 5.000 euro: a fronte di una qualunque variazione del Ricavo contrattuale o a fronte di un incremento dei Costi totali (ri)stimati, rispetto a quelli "autorizzati", per una percentuale superiore al 10%, il processo autorizzativo del *Preventivo commessa* va obbligatoriamente ripetuto.

Con l'approvazione ed autorizzazione del preventivo della commessa i citati Responsabili SIAG, ciascuno per le parti di sua competenza, attestano che:

- i requisiti della fornitura, così come noti alla data, sono sufficientemente definiti e descritti nella documentazione di riferimento,
- SIAG ha la capacità di soddisfare i requisiti della fornitura,
- è possibile dar corso alle attività inerenti la fornitura descritta nei documenti di riferimento, nel rispetto dei valori economici indicati.

In SIAG non può essere formalmente emessa alcuna Offerta o sottoscritto alcun Contratto se il processo descritto non è giunto alla sua positiva conclusione, ottenendo le autorizzazioni previste. Naturalmente i citati documenti formali potranno essere sottoscritti solo da Responsabili di SIAG dotati di adeguati poteri di firma.

Principi generali di comportamento

- Con riferimento ai reati-presupposto qui considerati, devono essere rispettati, come indicazioni cogenti, i principi, i valori e le norme contenuti nel Codice Etico di *Informatica Alto Adige*, da considerare, ad ogni effetto, parte integrante del Modello di Organizzazione e Gestione ex D.Lgs. 231/01; entrambi devono essere pubblicati nella rete intranet aziendale e, per quanto riguarda il Codice Etico, nel sito internet di *Informatica Alto Adige*. Il loro contenuto deve essere oggetto di formazione periodica rivolta ai Dipendenti.
- È assolutamente vietato, per chiunque operi in nome o per conto della Società, porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da configurare il compimento di uno dei reati qui considerati.
- È indispensabile che tutte le attività e le operazioni svolte per conto della Società siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza e trasparenza.
- È indispensabile che sia garantito il rispetto della normativa vigente, nonché delle procedure e dei protocolli aziendali, sia relativi al Ciclo attivo che a quello passivo, nonché quelli in materia di gestione ed impiego delle risorse e dei beni aziendali, in particolare per quelli di provenienza estera.
- È indispensabile che sia mantenuto un contegno chiaro, trasparente, diligente e collaborativo con le Pubbliche Autorità, con particolare riguardo alle Autorità Giudicanti ed Inquirenti, mediante la comunicazione di tutte le informazioni, i dati e le notizie eventualmente richieste.
- Chiunque in Azienda venga a conoscenza di comportamenti tenuti da Dipendenti/Collaboratori che integrano uno dei reati-presupposto considerati nel presente documento è tenuto ad informare il proprio Responsabile diretto e l'Organismo di Vigilanza.

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 fronde nelle pubbliche forniture (Art. 24, D.Lgs. n. 231/2001) [articolo modificato dal D.Lgs. n. 75/2020]

Reati richiamati dal D.Lgs. 231/01

L'articolo 24 del Decreto richiama specificatamente i seguenti reati.

- Malversazione a danno dello Stato o di altro ente pubblico
- Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico o delle Comunità europee;
- Frode nelle pubbliche forniture
- Truffa in danno dello Stato o di altro ente pubblico
- Truffa aggravata per il conseguimento di erogazioni da parte dello Stato, di enti pubblici o delle Comunità europee
- Frode informatica in danno dello Stato o di altro ente pubblico
- Indebita percezione di aiuti comunitari nel settore agricolo

Esemplificazioni delle fattispecie di reato richiamate sono le seguenti.

- Destinazione di contributi, di sovvenzioni o di finanziamenti a fini diversi da quelli fissati dall'Ente pubblico che li ha concessi
- Fornitura di false informazioni od omissioni di informazioni dovute (ad es.: in sede di Offerta) allo scopo di ottenere indebitamente da un Ente pubblico, contributi, finanziamenti, decontribuzioni o analoghi benefici
- Mediante artifici o raggiri, inducendo taluno in errore, ci si procura, a danno dello Stato o di altro Ente pubblico, un ingiusto profitto, contributi, finanziamenti o analoghi benefici
- In danno dello Stato o di altro ente pubblico, procurando all'Azienda o ad altri un ingiusto profitto, si altera il funzionamento di un sistema informatico/telematico o si interviene senza diritto, con qualsiasi modalità, su dati, informazioni o programmi contenuti in un sistema informatico o ad esso pertinenti
- Fraudolenta esecuzione di un contratto di somministrazione, contratto di vendita o contratto di appalto

Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società è significativa, soprattutto con riferimento ai seguenti **Soggetti/UU.OO. sensibili**:

- Responsabili di Reparto/ Service Area Manager ("SAM")
- Responsabile della Funzione Finance
- Direttore e Vice-Direttore
- Presidente

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Gestione di procedimenti volti a conseguire erogazioni contributi, sovvenzioni e finanziamenti pubblici
  - Erogazione di forniture che godono di finanziamenti o rimborsi da parte di Enti Pubblici o Comunitari
  - Assunzione di Personale: conseguimento di agevolazioni fiscali/contributive (es. per l'assunzione di Personale appartenente a categorie protette)
- Negoziazione, stipula ed esecuzione di contratti con clienti
  - Stesura Offerta-Contratto nei confronti di un Ente Pubblico
  - Processo di approvazione/autorizzazione preventivo fornitura di servizi
  - Project Management: controllo e verifica, in corso d'opera, del rispetto dei requisiti contrattuali

- Gestione ed utilizzo del sistema informatico aziendale, della rete internet e delle singole apparecchiature; protezione e conservazione dei dati informatici raccolti dalle diverse funzioni aziendali;
- Gestione ed utilizzo di sistemi informatici che si interconnettono e/o utilizzano software della PA
  - Utilizzo del portale Sistema Informativo Contratti Pubblici della PAB in qualità di stazione appaltante;
- Realizzazione e gestione dei sistemi informatici (hardware e software) dei propri clienti.

Le **modalità di commissione del reato** che si possono astrattamente ipotizzare sono le seguenti.

- Allo scopo di non pregiudicare o non ritardare l'assegnazione di una commessa, il preventivo della fornitura viene redatto, approvato ed autorizzato non evidenziando una o più criticità (es.: carenza di know-how specifico) che, se evidenziate, avrebbero potuto portare a diverse valutazioni da parte del Committente.
- Allo stesso scopo di cui al punto precedente, l'Offerta viene predisposta in modo incompleto o non del tutto veritiero, facendo ricorso a imprecisioni, omissioni, falsità o analoghi artifici.
- Acquisita, direttamente o tramite un Socio, una commessa che usufruisce di contributi o finanziamenti da parte di Enti pubblici o Comunitari, in corso d'opera si realizza la fornitura derogando volontariamente dai requisiti contrattuali, eventualmente compilando in modo non corretto o non completo documenti ufficiali correlati al contratto.
- I risultati dell'attività di definizione dei costi preventivati, di quelli sostenuti o degli Stati d'Avanzamento Lavori non scaturiscono da processi trasparenti e documentabili.
- Nel processo di assunzione di Personale appartenente a categorie che danno diritto a finanziamenti o decontribuzioni, i rapporti con gli enti preposti (es.: l'Ufficio del Lavoro) vengono gestiti fornendo informazioni incomplete o non vere.
- Nell'ambito dell'erogazione di una fornitura allo Stato, ad un Ente Pubblico o Comunitario, si interviene in modo illecito su informazioni e programmi pertinenti al suo Sistema Informativo.
- Documenti di valenza contrattuale (Offerta-Contratto) vengono sottoscritti da Responsabili SIAG privi di adeguati poteri al riguardo.
- Impiego dei contributi pubblici ricevuti (p.es. per formazione, innovazione e sviluppo) per scopi diversi dall'erogazione.
- Conseguimento di contributi pubblici utilizzando o presentando dichiarazioni o documenti falsi ovvero attestando cose non vere ovvero omettendo informazioni dovute.
- Conseguimento di contributi o altre erogazioni pubbliche ovvero un altro ingiusto profitto a danno dello Stato di un altro ente pubblico, utilizzando artifizi o raggiri per indurre taluno in errore.
- Comportamento non conforme ai doveri di lealtà e moralità commerciale e di buona fede contrattuale, malafede contrattuale, presenza di un espediente malizioso o di un inganno, tali da far apparire l'esecuzione del contratto conforme agli obblighi assunti.
- Intervento sul funzionamento di un sistema informatico o telematico, dati, informazioni o programmi contenuti in un sistema informatico o telematico per procurarsi un ingiusto profitto con danno altrui.

Si segnala infine che la Società ha deciso di connotare come reati "*di particolare rilevanza*" gli eventuali reati commessi nell'ambito dei rapporti (preliminari o successivi alla formalizzazione contrattuale) instaurati con una Pubblica Amministrazione, *Centrale* o *Locale*, o con Istituzioni Comunitarie e di sanzionarli con maggior severità nell'ambito del *sistema disciplinare* descritto nel presente Modello.

Presidio del rischio attuato dalla Società

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.5.2.1. Principi specifici di comportamento

- Allo scopo di avere totale garanzia che nell'ambito di una fornitura a favore di qualunque Cliente, sia chiara la volontà della Società di rifuggire da qualsiasi comportamento di carattere corruttivo o, comunque, illecito (ancorché condotto nell'interesse o a vantaggio della Società), i Soggetti aziendali obbligatoriamente tenuti ad autorizzare la fornitura, anche con riferimento ad aspetti legati a fasi del "ciclo passivo" (quali, ad esempio, acquisizioni esterne finalizzate all'erogazione della fornitura) sono tenuti a sottoscrivere una dichiarazione con la quale si attesta:
  - che, sulla base delle informazioni a loro disposizione e fino alla data di sottoscrizione della dichiarazione in questione, in nessuna fase della trattativa commerciale o della formalizzazione contrattuale si sono verificati episodi che, anche ipoteticamente, appaiano riconducibili o comunque diretti ad atti RILEVANTI ai sensi del D.Lgs. 231/01;
  - l'impegno a comunicare immediatamente all'Organismo di Vigilanza ex D.Lgs. 231/01 eventuali tentativi, episodi o atti anche ipoteticamente inquadrabili fra gli illeciti sopra menzionati, laddove gli stessi si verificassero successivamente alla sottoscrizione della dichiarazione in questione, fino al completo espletamento della fornitura.

- In tutti i casi in cui l'assunzione di personale determini l'erogazione pubblica di finanziamenti e/o decontribuzioni, la Funzione Finance si rapporta agli Uffici competenti, in primis, con l'Ufficio del Lavoro, in termini di totale trasparenza, fornendo informazioni complete e veritiere.
- Nell'ambito di una fornitura a beneficio di una Pubblica Amministrazione o di un Concessionario di pubblici finanziamenti, va garantita la tracciabilità dei flussi finanziari, nel rispetto di quanto previsto dalla L. 136/10.
- Internamente all'Azienda, per ciascuna commessa, va assegnato il ruolo di Responsabile della commessa/Capo Progetto/SAM.
  In sede di approvazione dei consuntivi, facendo ricorso all'applicativo SW "Work Manager", ciascun Responsabile di un Reparto coinvolto nella fornitura a beneficio di un Ente Pubblico è tenuto a verificare la coerenza dei giorni consuntivati dalle singole Risorse del suo Reparto rispetto ai requisiti delle forniture in cui le stesse Risorse sono impegnate.
- I rapporti e gli adempimenti nei confronti della PA devono essere effettuati con la massima trasparenza, diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere.

- Qualora venisse previsto per l'espletamento dell'attività il coinvolgimento di collaboratori o consulenti esterni questo dovrà essere formalizzato per iscritto ed il relativo contratto dovrà contenere apposita dichiarazione di conoscenza della normativa di cui al Decreto nonché condivisione dei principi di cui al Codice Etico. Il relativo contratto dovrà essere stipulato in conformità ai principi ed alle procedure aziendali in tema di conferimento di incarichi esterni. Non è consentito riconoscere compensi in favore di tali collaboratori o consulenti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto. Il corrispettivo deve essere congruo ed il servizio reso documentato o documentabile.

- L'intero processo in ogni sua fase deve essere tracciato, sia a livello informatico che documentale, così che le attività svolte siano documentate coerenti e congrue. La funzione responsabile archivierà e conserverà la relativa documentazione in adempimento alla relativa procedura aziendale.

2.5.2.2. Protocolli aziendali e controlli relativi ai processi

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
01 – 01	Alla stesura dell'Offerta partecipano, con ruoli diversi, diversi Attori. Nel rispetto della procedura aziendale referenziata, vanno osservate obbligatoriamente fasi di approvazione formale dei preventivi dei costi e dei ricavi, approvazioni demandate a Responsabili appartenenti a strutture diverse dell'organizzazione aziendale. La versione finale dell'Offerta, compresi i relativi allegati, devono essere verificati, in termini formali e sostanziali, prima della trasmissione all'Ente pubblico. In particolare va verificato che l'Offerta soddisfi i requisiti, soggettivi ed oggettivi, richiesti, che non contenga omissioni, imprecisioni o informazioni non vere.	**→ Vedasi "Procedura di autorizzazione interna delle forniture" descritta nel presente documento.** **→ Order management; Service Catalouge Management; Operative Financial Management; Request for Change; Needs analysis Technical Solution definition; Development; Validation an Testing; Information Security Management; Operative Financial Management for IT-Billing; Manuale operativo contabilità SAP**
01 – 02	Le sottoscrizioni, da parte di un Rappresentante della Società: - di un'Offerta o di un Contratto, verso un Cliente (ciclo attivo), ovvero - di un Contratto o di un Ordine, verso un Fornitore (ciclo passivo) sono atti formali che impegnano la Società verso l'esterno; in quanto tali, non possono essere effettuati se non da chi è intestatario di apposita adeguata procura. La titolarità di procure non esime il detentore delle stesse dal rispetto degli adempimenti aziendali prescritti per quanto concerne il processo autorizzativo interno.	**→ Vedasi "Procedura di autorizzazione interna degli acquisti" descritta nel presente documento.** **→ Vedasi "Procedura di autorizzazione interna delle forniture" descritta nel presente documento.**
01 – 03	Nell'ambito: → di una fornitura a beneficio di un Ente Pubblico, oppure → di una fornitura che preveda finanziamenti, sovvenzioni o contributi erogati da un Ente pubblico la stima dei costi preventivati (costi che devono risultare riconciliabili con l'Offerta, anche in termini di profili professionali impiegati nella fornitura), deve scaturire da un processo documentato, durante il quale vengono applicati criteri coerenti con i requisiti della fornitura.	**→ Vedasi "Procedura di autorizzazione interna delle forniture" descritta nel presente documento.** **→ Order management; Service Catalouge Management; Operative Financial Management; Request for Change; Needs analysis Technical Solution definition; Development; Validation an Testing; Information Security Management; Operative Financial Management for IT-Billing; Manuale operativo contabilità SAP**
01 – 04	Nell'ambito dell'erogazione di una fornitura allo Stato, ad altro Ente Pubblico o Comunitario, vanno adottati, laddove il contesto li renda applicabili, i protocolli previsti per i reati-presupposto di cui all'art. 24-bis (commi 1, 2 e 3) del D.Lgs 231/01 (Delitti informatici e trattamento illecito di dati). In particolare vanno applicate (se ne ricorrono le circostanze) le disposizioni illustrate al paragrafo "Interscambio di dati da e verso terzi in forma regolare" del documento aziendale referenziato.	**→ Policies - *Workplace Policy*** **→ Information Security Management.**
01 – 05	Nell'ambito dei rapporti con la PA inerenti la richiesta di finanziamenti, contributi o l'utilizzo di agevolazioni o sgravi fiscali, la società ed i suoi dipendenti dovranno attenersi ai suddetti principi specifici di comportamento ed inoltre è fatto divieto di:	

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
	• predisporre e inviare, così come accettare documenti consapevolmente incompleti e/o comunicare dati falsi o alterati; • tenere una condotta ingannevole che possa indurre la PA, gli enti eroganti e/o di controllo in errore; • richiedere o indurre i soggetti appartenenti alla PA a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare illecitamente atti o comportamenti della PA stessa; • utilizzare contributi, sovvenzioni, finanziamenti, agevolazioni per finalità diverse da quelle per le quali sono stati concessi al fine di procurare un vantaggio alla società; • non porre in essere, in tutto o in parte le attività per le quali finanziamenti contributi, sovvenzioni, finanziamenti, agevolazioni sono state erogate; • promettere o corrispondere utilità e/o vantaggi, siano esse somme di denaro, doni, prestazioni al di fuori di quanto di prassi, al fine di promuovere o favorire gli interessi della società o influenzare illecitamente atti o comportamenti della PA stessa o degli enti eroganti e/o di controllo; affidare incarichi a collaboratori o consulenti esterni eludendo i criteri di cui alle policies e procedure aziendali.	

Delitti informatici e trattamento illecito di dati (Art. 24-bis del D.Lgs. 231/01)

Reati richiamati dal D.Lgs. 231/01

Il primo comma dell'art. 24-bis del Decreto richiama specificatamente i seguenti reati.

- Accesso abusivo ad un sistema informatico o telematico
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
- Danneggiamento di informazioni, dati e programmi informatici
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
- Danneggiamento di sistemi informatici o telematici
- Danneggiamento di sistemi informatici o telematici di pubblica utilità

Il secondo comma dell'art. 24-bis del Decreto richiama specificatamente i seguenti reati:

- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.

Il terzo comma dell'art. 24-bis del Decreto richiama specificatamente i seguenti reati.

- Falsità in un documento informatico pubblico o avente efficacia probatoria
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica.

Esemplificazioni delle fattispecie di reato richiamate sono le seguenti:

- con riferimento alle fattispecie di cui al **primo comma** dell'art. 24 bis del D. Lgs. 231/2001:
  - Introduzione in un sistema informatico, interno e/o esterno all'Azienda, violandone il sistema di sicurezza, ovvero operare al suo interno contro la volontà, espressa o tacita, di chi ha il diritto di escluderlo
  - Intercettazione, impedimento o interruzione fraudolenta di comunicazioni informatiche/telematiche (interne od esterne all'Azienda); diffusione pubblica, anche solo parziale, mediante qualsiasi mezzo di informazione, del contenuto delle comunicazioni
  - Installazione, fuori dai casi previsti (da leggi, procedure o contratti) di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche/telematiche (interne od esterne all'Azienda)
  - Distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui; ovvero commissione di tali atti su informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.
- Con riferimento al **secondo comma** dell'articolo in commento:
  - Reperimento, riproduzione, diffusione, comunicazione o consegna abusiva di codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, interno od esterno all'Azienda, protetto da misure di sicurezza; dare indicazioni o istruzioni idonee al predetto scopo, al fine di procurare a sé o ad altri un profitto o arrecare ad altri un danno
  - Reperimento, produzione, riproduzione, importazione, diffusione, comunicazione, consegna o, comunque, messa a disposizione di altri di apparecchiature, dispositivi o programmi informatici (anche prodotti da altri), con lo scopo di danneggiare un sistema informatico o telematico (interno od esterno all'Azienda), le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero per provocare l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.
- Con riferimento al **terzo comma** dell'articolo in commento:
  - in relazione ad un documento informatico pubblico: falsificazione di documenti informatici o, comunque, uso di documenti informatici falsi.
  - nell'ambito della fornitura di un servizio di certificazione di firma elettronica: violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato, con lo scopo di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno.

 Nota: per *documento informatico* si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

Contestualizzazione aziendale e modalità di commissione

L'art. 24-bis del D.Lgs. 231/01 elenca, nei 3 commi che lo compongono, 11 distinti reati previsti dal Codice Penale, tutti attinenti al settore informatico.

Data la natura del *core business* di *Informatica Alto Adige*, appare evidente la particolare esposizione che la Società presenta rispetto all'ipotesi di commissione dei reati qui trattati.

Ciò, in particolare, tenendo conto delle seguenti due circostanze, astrattamente in grado di "agevolare" la commissione di atti illeciti:

- le competenze tecniche indispensabili per la commissione dei reati qui considerati sono possedute dalla maggior parte delle persone che lavorano per Informatica Alto Adige;
- nell'ambito delle attività inerenti una fornitura, spesso il personale Informatica Alto Adige opera "all'interno" dell'infrastruttura informatica del proprio Cliente, avendo frequentemente la possibilità/necessità (regolamentata dal contratto) di accedere ad apparecchiature e dati del Cliente stesso.

Le gravi sanzioni che la legge infliggerebbe alla SIAG nell'ipotetica eventualità di commissione di uno dei reati informatici qui considerati, sarebbero sempre di due tipi:

- sanzioni pecuniarie
- sanzioni interdittive; queste potranno andare, ad esempio, dal divieto di pubblicizzare beni o servizi, al divieto di contrattare con la Pubblica Amministrazione, fino all'interdizione dall'esercizio dell'attività.

Va sottolineato che la legge prevede l'applicazione, nei confronti dell'Ente, di aggravanti, anche in termini sanzionatori, nelle seguenti due specifiche circostanze:

- se l'infrazione è posta in essere da personale che agisce nel ruolo di operatore/gestore del sistema
- se le informazioni, i dati o i sistemi informatici oggetto di interventi illeciti sono utilizzati dallo Stato o da altro Ente pubblico o comunque di pubblica utilità.

Alla luce delle precedenti considerazioni, *Informatica Alto Adige* ha ritenuto di considerare i reati informatici "*reati di particolare rilevanza*" e di sanzionarli con maggior severità nell'ambito del *sistema disciplinare* descritto nel presente Modello.

Va osservato che, ancorché il presupposto dell'*interesse e vantaggio* ottenuto dall'Azienda a seguito della commissione del reato (presupposto che caratterizza l'imputabilità di un Ente ex D.Lgs. 231/01) porti (implicitamente) ad identificare, come parte offesa, il Cliente di *Informatica Alto Adige* (in particolare: il suo Sistema Informatico, le infrastrutture, le informazioni ed i dati gestiti), il presente *Modello*, come ulteriore misura volta a minimizzare il rischio di commissione del reato, applica le norme, i protocolli ed i controlli di seguito riportati anche con riferimento al proprio Sistema Informatico, alle infrastrutture, alle informazioni ed ai dati gestiti da SIAG. Infatti le risorse HW e/o le applicazioni SW disponibili in *Informatica Alto Adige* potrebbero teoricamente essere utilizzate in quanto *funzionali* all'accesso a Sistemi Informatici di Terzi.

Da tutto quanto precede scaturisce la considerazione che, rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società è difficilmente circoscrivibile. Volendo tuttavia indicare specifici **Soggetti/UU.OO**. **sensibili**, si possono citare i settori RUN e PRODUCTION.

Analogamente per quanto riguarda i **processi/sottoprocessi sensibili**: il rischio di commissione del reato-presupposto qui considerato è piuttosto esteso e difficilmente confinabile, a priori, a specifici processi. Volendo fare stretto riferimento al *Sistema Informatico* ("*S.I.*") del Cliente, processi sensibili sono generalmente tutti quelli che prevedono, nell'esecuzione di un rapporto contrattuale di fornitura, l'accesso a risorse informatiche del Cliente.

In particolare, per quanto riguarda il reato di "*Falsità in un documento informatico pubblico o privato avente efficacia probatoria*":

- Gestione ed utilizzo del sistema informatico aziendale, della rete internet e delle singole apparecchiature; protezione e conservazione dei dati informatici raccolti dalle diverse funzioni aziendali;
- Gestione ed utilizzo di sistemi informatici che si interconnettono e /o utilizzano software della PA
    - Utilizzo del portale Sistema Informativo Contratti Pubblici della PAB in qualità di stazione appaltante
- Realizzazione e gestione dei sistemi informatici (Hardware e software) dei propri clienti pubblici
    - Intervento sulle informazioni che concorrono alla formazione di un documento informatico prodotto sotto la responsabilità del Cliente
- Rapporti con l'Amministrazione dello Stato, di un Ente Pubblico o Comunitario/ Trasmissione di informazioni registrate in un documento informatico.

Le **modalità di commissione del reato** che si possono astrattamente ipotizzare sono le seguenti.

- Ci si introduce nel Sistema Informatico ("S.I.") di Informatica Alto Adige, di un Cliente o di un Fornitore, sistema protetto da misure di sicurezza, con modalità e per finalità non autorizzate da chi ha inteso proteggere il sistema.

- Si interviene illecitamente, eventualmente mediante l'installazione di apposite apparecchiature, sul flusso di comunicazione fra sistemi di Informatica Alto Adige, Clienti o Terze Parti, intercettando, impedendo o interrompendo tale flusso. Eventualmente l'intervento di cui sopra viene seguito dalla diffusione, anche parziale, del contenuto delle comunicazioni.
- Si interviene illecitamente modificando, cancellando o, comunque, danneggiando dati, informazioni o programmi informatici:
  - presenti nei sistemi di Clienti o Terze Parti,
  - utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.
- Ci si introduce nel S.I. di Informatica Alto Adige, di un Cliente o di un Fornitore, allo scopo di acquisire illecitamente codici personali (user-id e password o "parola chiave" o "parola d'ordine") che consentono di accedere a sistemi e/o a funzioni per i quali non si è autorizzati.
- Si duplicano e/o si diffondono, in qualunque modo, codici personali acquisiti abusivamente.
- Si forniscono informazioni e/o strumenti idonei all'acquisizione e/o duplicazione abusiva di codici personali.
- Si interviene illecitamente, eventualmente mediante l'installazione di apposite apparecchiature, di programmi o di virus informatici, sul S.I. di Informatica Alto Adige, di Clienti o di Terze Parti, impedendone o alterandone il funzionamento o danneggiando le informazioni o i programmi del sistema.
- Un Collaboratore impegnato nell'erogazione di una fornitura a favore di un Ente Pubblico, sfruttando la detenzione di abilitazioni giustificate dalle attività previste dalla tipologia di fornitura, interviene sulle informazioni contenute/elaborate dal Sistema Informatico del Cliente, con lo scopo di far sì che venga prodotto un documento informatico dal contenuto totalmente o parzialmente falso.
- Nei rapporti intrattenuti dalla Società con una Pubblica Amministrazione si predispongono documenti informatici falsi.

Presidio del rischio attuato dalla Società

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.6.3.1. Principi specifici di comportamento

- I Soggetti indicati come "sensibili al rischio" sono tenuti a rispettare scrupolosamente tutte le norme vigenti, ed in particolare:
  - utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
  - custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
  - garantire la tracciabilità delle operazioni di inserimento/modifica effettuate in relazione al sistema delle abilitazioni/deleghe interne utilizzato in Azienda;
  - assicurare meccanismi di protezione dei file, quali, ad esempio, password da aggiornare periodicamente, secondo le prescrizioni comportamentali della Società;
  - utilizzare beni protetti dalla normativa sul diritto d'autore nel rispetto delle regole ivi previste.

- Ai Destinatari del Modello è fatto divieto di:
  - utilizzare le risorse informatiche (es. personal computer fissi o portatili) assegnate dalla Società in violazione delle norme aziendali in vigore;
  - effettuare download illegali o trasmettere a soggetti terzi contenuti protetti dal diritto d'autore;
  - alterare documenti elettronici, pubblici o privati, con finalità probatoria;
  - accedere, senza averne l'autorizzazione, ad un sistema informatico o telematico o trattenersi contro la volontà espressa o tacita di chi ha diritto di escluderlo (il divieto include sia l'accesso ai

sistemi informativi interni che l'accesso ai sistemi informativi di enti concorrenti, pubblici o privati, allo scopo di ottenere informazioni su sviluppi commerciali o industriali);

- procurarsi, riprodurre, diffondere, comunicare, ovvero portare a conoscenza di terzi: codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico altrui protetto da misure di sicurezza, oppure fornire indicazioni o istruzioni idonee a consentire ad un terzo di accedere ad un sistema informatico altrui, protetto da misure di sicurezza;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- aggirare o tentare di aggirare i sistemi di sicurezza aziendali (es: Antivirus, Firewall, Proxy server, etc.);
- lasciare il proprio computer incustodito, acceso e senza blocco con protezione password.

➢ In qualunque contesto, ma in particolar modo nell'ambito dell'erogazione di una fornitura ad un Ente Pubblico, anche avendo la possibilità di accedere lecitamente al Sistema Informatico ("S.I.") del Cliente, ovvero all'infrastruttura tecnologica, alle applicazioni, ai programmi, ai dati ed alle informazioni pertinenti a tale S.I., è assolutamente vietato intervenire, in qualunque modo, allo scopo ultimo di falsificare un documento informatico pubblico o avente efficacia probatoria. E' altresì vietato utilizzare documenti informatici falsi.

2.6.3.2. Protocolli aziendali e controlli relativi ai processi

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
02 – 01	Un Sistema Informatico ("*S.I.*"), con ciò intendendo la sua infrastruttura tecnologica, le sue applicazioni, i suoi programmi, i dati e le informazioni ad esso pertinenti, indipendentemente dal fatto che si tratti del S.I. della Società, di un Cliente o di una Terza Parte, può essere *acceduto* effettuando *intercettazioni*, *consultazioni, duplicazioni* o *modifiche* (intervenendo, in qualunque modo, su di esso) ***solo ed esclusivamente*** previa legittima acquisizione delle previste autorizzazioni ed esclusivamente con modalità e per finalità che risultino coerenti con il ruolo svolto e, in ambito contrattuale, con quanto previsto dal contratto.	→ **Codice Etico di Informatica Alto Adige**
02 – 02	Chiunque operi in nome o per conto della Società è direttamente responsabile, civilmente e penalmente, a norma delle leggi vigenti, per l'uso fatto della rete aziendale, del servizio internet e della posta elettronica. Tale responsabilità si estende anche alla violazione degli accessi protetti, del copyright e delle licenze d'uso.	→ **Policies - *Workplace Policy***
02 – 03	Per ciascun specifico sistema (o area applicativa) gestito dal S.I. (ad esempio: SAP), solo una persona può disporre delle credenziali per modificare i profili di abilitazione degli Utenti che possono accedere a tale sistema. Inoltre vengono creati e conservati per un congruo periodo di tempo: - i log che tengono traccia delle modifiche ai vari DBMS; - i log che, per tutti i sistemi/applicativi più sensibili, tengono traccia degli accessi effettuati: Utente, data e ora di accesso, tipo di intervento, esito del tentativo di accesso, laddove non fosse riuscito.	→ **Policies - *Workplace Policy***

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
02 – 04	Vanno rigorosamente osservate tutte le norme previste dal documento referenziato, in particolare quelle contenute nei capitoli: - *La politica aziendale* - *Utilizzo delle risorse interne all'azienda* - *Servizi internet*. A titolo non esaustivo si richiamano, oltre alle disposizioni illustrate al paragrafo "Interscambio di dati da e verso terzi in forma regolare", le seguenti norme: - il Collaboratore si fa obbligo di considerare ed elaborare quale confidenziale ogni dato e qualsiasi informazione con la quale sia posto in contatto durante lo svolgimento della sua mansione - alla rete aziendale possono essere collegati solo i PC ed i portatili assegnati dal Settore "Run". In particolare è fatto divieto di collegare alla rete o installare apparati e/o componenti personali o esterni.	→ **Policies - *Workplace Policy*** → **Information Security Management** **Certificazione: ISO/IEC 27001:2013 Information Security Management Systems**
02 – 05	Nello svolgimento di un intervento sul S.I. del Cliente, al termine dello stesso, il responsabile SIAG dell'intervento è tenuto a far verificare da un Utente del Cliente che il sistema non abbia subìto peggioramenti in termini di prestazioni e/o di funzionalità. Il Responsabile del Reparto coinvolto può chiedere al proprio Collaboratore, laddove le circostanze lo suggeriscano, evidenza di tale positiva verifica da parte del Cliente, ovvero la motivazione per cui la stessa non abbia avuto luogo.	→ **Policies - *Workplace Policy*** → **Information Security Management** **Certificazione: ISO/IEC 27001:2013 Information Security Management Systems**
02 – 06	Nello svolgimento di un intervento sul S.I. del Cliente, se un Dipendente SIAG rilevasse una vulnerabilità di tale sistema rispetto a possibili accessi (anche da parte dello stesso personale SIAG) non esplicitamente autorizzati, è tenuto ad informarne riservatamente il Cliente, mettendolo così in condizioni di adottare gli interventi che riterrà più opportuni.	→ **Policies - *Workplace Policy*** → **Information Security Management** **Certificazione: ISO/IEC 27001:2013 Information Security Management Systems**
02 – 07	Ogni accesso (in ingresso ed in uscita) via internet viene registrato. A fronte di valide motivazioni (ad esempio per consentire all'Autorità Giudiziaria di effettuare indagini su eventuali reati) anche il traffico di rete può essere tracciato su file di log, i quali vengono conservati a termini di legge, nel rispetto della normativa vigente e a tutela dei diritti dei Lavoratori. Personale tecnico SIAG, che deve essere debitamente ed opportunamente autorizzato dall'Azienda, può avere accesso ai dati di traffico al fine di garantire il corretto ed ottimale funzionamento della rete e dei servizi.	→ **Policies - *Workplace Policy*** → **Information Security Management** **Certificazione: ISO/IEC 27001:2013 Information Security Management Systems**
02 – 08	E' vietato, in qualunque ambito, agire allo scopo di venire illecitamente a conoscenza dei codici personali (user-id e password) di un altro Utente e/o allo scopo di diffondere gli stessi. Se si venisse a conoscenza, per cause fortuite, di codici personali altrui, oltre al divieto assoluto di utilizzarli, v'è l'obbligo di informare immediatamente di tale circostanza l'Utente titolare dei codici stessi, che provvederà all'immediata modifica (almeno) della propria password.	→ **Policies - *Workplace Policy*** → **Information Security Management** **Certificazione: ISO/IEC 27001:2013 Information Security Management Systems**

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
02 – 09	Chiunque in SIAG deve applicare con il massimo rigore tutte le norme ed i controlli descritti nel paragrafo "Account e parole d'ordine" del documento referenziato. In particolare, va rispettata la seguente norma (vedasi sotto-paragrafo "*Accounts di utenti/Parole d'ordine*"): *ogni Collaboratore è responsabile in proprio dell'amministrazione della parola d'ordine assegnata e solo a lui/lei nota. In nessun caso il Collaboratore ha da comunicare la propria password ad altri o permettere ad altri l'accesso e/o l'uso del proprio account di rete. Non vi è alcuna ragione tecnica od organizzativa che giustifichi la comunicazione ad altri della propria password.*	→ **Policies - *Workplace Policy*** → **Information Security Management** **Certificazione: ISO/IEC 27001:2013 Information Security Management Systems**
02 – 10	A) Il Dipendente non può installare di sua iniziativa sulla postazione di lavoro software non autorizzato senza prima interpellare il reparto Reti e Sistemi. B) A fronte di specifiche esigenze, l'Azienda può effettuare lo scan da remoto dei dischi fissi dei PC dei Collaboratori, al fine di rilevare i file eseguibili presenti, i software installati e le licenze utilizzate.	→ **Policies - *Workplace Policy*** → **Information Security Management** **Certificazione: ISO/IEC 27001:2013 Information Security Management Systems**
02 – 11	Le componenti software di base non possono essere disinstallate, modificate o manipolate in nessuna maniera. In particolare è fatto divieto di disattivare componenti software collegate con la sicurezza. È espressamente vietato effettuare consapevolmente installazioni ed attivazioni di parti di codice virulenti di ogni tipo (virus informatici)	→ **Policies - *Workplace Policy*** → **Information Security Management** **Certificazione: ISO/IEC 27001:2013 Information Security Management Systems**

Delitti di criminalità organizzata (Art. 24-ter del D.Lgs. 231/01)

Reati richiamati dal D.Lgs. 231/01

L'articolo 24-ter del Decreto richiama specificatamente i seguenti articoli del Codice Penale.

- Associazione per delinquere
- Associazioni di tipo mafioso anche straniere
- Scambio elettorale politico-mafioso
- Sequestro di persona a scopo di rapina o di estorsione
- Associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope

Esemplificazioni delle fattispecie di reato richiamate sono le seguenti.

- Ci si associa allo scopo di commettere più reati
- Si fa parte di un'associazione di tipo mafioso
- Si ottiene la promessa di voti in cambio della erogazione di denaro
- Si sequestra una persona allo scopo di conseguire, per sé o per altri, un ingiusto profitto
- Si fa parte di un'associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope

L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere reati, per acquisire la gestione o il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri. Le disposizioni del presente articolo si applicano anche alla camorra e alle altre associazioni, comunque localmente denominate, anche straniere, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso.

Contestualizzazione aziendale e modalità di commissione

Da un'analisi delle attività nel cui ambito possono essere commessi i reati elencati, è emersa l'inapplicabilità alla Società delle fattispecie delittuose di cui agli artt. 416 comma 6, 416-ter, 630 c.p., 74 D.P.R. n. 309/1990, 407 comma 2 lett. a) n. 5 c.p.p. Si tratta, infatti, di fattispecie penali da considerare del tutto estranee alle attività svolte dalla Società, nonché assolutamente contrarie ai valori e principi che ne hanno da sempre ispirato l'agire, rispetto alle quali non è, pertanto, necessario predisporre alcuna misura preventiva o richiamare specifici principi generali di comportamento.

Un discorso in parte differente va fatto per quel che riguarda l'associazione per delinquere di cui all'art. 416 c.p., i cui elementi costitutivi tipici si fondano sulla stabilità del vincolo associativo, desumibile da un certo livello di organizzazione dell'associazione e dal perseguimento di una finalità associativa consistente nella realizzazione di un programma delittuoso generico, di commettere cioè una serie indeterminata di delitti.

Sullo specifico punto, è intervenuta la Suprema Corte circoscrivendo l'operatività dell'art. 24 ter, negando la possibilità di recuperare indirettamente i delitti-scopo del reato associativo; a ragionare diversamente, infatti, "*la norma incriminatrice di cui all'art. 416 c.p. si trasformerebbe, in violazione del principio di tassatività del sistema sanzionatorio contemplato dal D.Lgs. n. 231 del 2001, in una disposizione "aperta", dal contenuto elastico, potenzialmente idoneo a ricomprendere nel novero dei reati-presupposto qualsiasi fattispecie di reato, con il pericolo di un'ingiustificata dilatazione dell'area di potenziale responsabilità dell'ente collettivo, i cui organi direttivi, peraltro, verrebbero in tal modo costretti ad adottare su basi di assoluta incertezza e nella totale assenza di oggettivi criteri di riferimento, i modelli di organizzazione e di gestione previsti dal citato D.Lgs., art. 6, scomparendone, di fatto, ogni efficacia in relazione agli auspicati fini di prevenzione*" (Cassazione penale, Sez. VI, 20 dicembre 2013, n. 3635).

Ebbene, esclusa la possibilità di immaginare nel caso della Società e, più in generale, di ogni organizzazione lecita, la realizzazione della condotta di costituzione di una associazione a ciò finalizzata, si tratta di vagliare il rischio che la struttura organizzativa societaria sia utilizzata da più persone al fine di realizzare una serie di delitti nell'interesse o a vantaggio della Società stessa; ipotesi che la giurisprudenza spesso riconduce alla figura dell'art. 416 c.p., piuttosto che al mero concorso di persone in più reati.

In quest'ottica, è evidente come il rischio che ciò accada non sia individuabile ex ante da parte della Società, ma si leghi ad un fenomeno di devianza dipendente dalla determinazioni di alcuni suoi membri, nel caso in cui decidano di sfruttare l'organizzazione di persone e di mezzi, tipica di ogni società, per fini criminali.

Le misure preventive immaginabili sono legate, in primo luogo, alla diffusione più ampia possibile dell'etica della Società, ribadendo a chiunque operi al suo interno che il perseguimento di vantaggi per la Società, ottenuti attraverso il compimento di attività penalmente vietate, non è mai consentito e che la Società adotterà ogni misura, anche radicale, ritenuta utile a garantire immediatamente una situazione di legalità e trasparenza.

Tuttavia, al solo fine di scongiurare il pur remoto rischio che per la devianza di singoli soggetti operanti all'interno della società, si possano in qualche modo agevolare dall'esterno, mediante il perfezionamento di rapporti contrattuali, organizzazioni di tipo criminale, si è ritenuto utile richiamare i principi di base e le regole che hanno, peraltro, ispirato da sempre la filosofia della Società, per esigerne il rispetto.

Poiché i delitti di criminalità organizzata possono essere finalizzati anche alla commissione dei reati già analizzati nelle singole Parti Speciali, si ritiene opportuno specificare che le aree a rischio di seguito menzionate devono intendersi integrate con le altre specificatamente individuate in relazione a ciascuna fattispecie oggetto di trattazione nelle altre Parti Speciali del presente Modello.

Tale precisazione si ritiene necessaria per ragioni strettamente legate alla formazione di un Modello quanto più efficace e in linea con il dettato normativo del D.Lgs. 231/01.

Ciò precisato, rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società è significativo, soprattutto con riferimento ai seguenti **Soggetti/UU.OO. sensibili**:

- Componenti del Consiglio di Amministrazione
- Componenti del Management aziendale

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Selezione, negoziazione ed esecuzione di contratti con fornitori, prestatori di servizi ed appaltatori, consulenti (Ciclo Passivo: acquisti ed approvvigionamenti)
  - Stesura, autorizzazione e sottoscrizione contrattuale,
  - Gestione fatturazione passiva,
  - Gestione dati anagrafici dei Fornitori
  - Gestione subappalti: contrattualizzazione, in particolare in relazione agli obblighi sulla tracciabilità dei flussi finanziari
- Negoziazione, stipula ed esecuzione di contratti con clienti (Ciclo attivo)
  - Stesura Offerta-Contratto nei confronti di un Ente Pubblico
  - Processo di approvazione/autorizzazione preventivo fornitura di servizi
  - Project Management: controllo verifica, in corso d'opera, del rispetto dei requisiti contrattuali
- Flussi finanziari
  - Gestione Cassa/ Pagamenti in contanti

Le **modalità di commissione del reato** che si possono astrattamente ipotizzare sono le seguenti.

- In via del tutto generale: allacciamento e mantenimento di rapporti d'affari, economici o commerciali, di natura delittuosa con l'organizzazione di un Cliente, un Fornitore o di un Partner.
- In particolare si può astrattamente ipotizzare che vengano fatti pagamenti, in contanti o mediante bonifici, a favore di organizzazioni coinvolte in attività criminali.

Presidio del rischio attuato dalla Società

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.7.3.1. Principi specifici di comportamento

- Allo scopo di avere totale garanzia che nell'ambito di una fornitura a favore di qualunque Cliente, sia chiara la volontà della Società di rifuggire da qualsiasi comportamento di carattere corruttivo o, comunque, illecito (ancorché condotto nell'interesse o a vantaggio della Società), i Soggetti aziendali obbligatoriamente tenuti ad autorizzare la fornitura, anche con riferimento ad aspetti legati a fasi del "ciclo passivo" (quali, ad esempio, acquisizioni esterne finalizzate all'erogazione della fornitura) sono tenuti a sottoscrivere una dichiarazione con la quale si attesta:
  - che, sulla base delle informazioni a loro disposizione e fino alla data di sottoscrizione della dichiarazione in questione, in nessuna fase della trattativa commerciale o della formalizzazione contrattuale si sono verificati episodi che, anche ipoteticamente, appaiano riconducibili o comunque diretti ad atti RILEVANTI ai sensi del D.Lgs. 231/01;
  - l'impegno a comunicare immediatamente all'Organismo di Vigilanza ex D.Lgs. 231/01 eventuali tentativi, episodi o atti anche ipoteticamente inquadrabili fra gli illeciti sopra menzionati, laddove gli stessi si verificassero successivamente alla sottoscrizione della dichiarazione in questione, fino al completo espletamento della fornitura.

- Nell'ambito di una fornitura a beneficio di una Pubblica Amministrazione, va garantita la tracciabilità dei flussi finanziari, nel rispetto di quanto previsto dalla L. 136/10.

- Relativamente al processo di gestione, mediante applicativo software, dei dati anagrafici dei Fornitori, dati che comprendono, fra gli altri, le coordinate bancarie degli stessi, in SIAG le credenziali che abilitano alle funzioni SW di *inserimento* e *modifica* delle coordinate bancarie vengono rilasciate ad un massimo di due Dipendenti.

2.7.3.2. Protocolli aziendali e controlli relativi ai processi

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
03 – 01	Allo scopo di ridurre al minimo il rischio di commissione dei reati qui considerati, è obbligatorio rispettare col massimo rigore tutte le norme, aziendali e legislative, applicabili. In particolare: → "*Procedura di autorizzazione interna degli acquisti*"; → Gestione della cassa: rispetto delle norme di legge che regolano le transazioni commerciali, specialmente con riferimento al limite massimo nell'impiego del contante. In linea generale, deve essere rispettata la regola che vieta che una persona possa, da sola, attivare, gestire, autorizzare e chiudere un processo sensibile. In particolare, il processo degli acquisiti, dalla formulazione della richiesta interna al pagamento, deve obbligatoriamente coinvolgere almeno due diversi Attori.	**→ Vedasi "Procedura di autorizzazione interna degli acquisti" descritta nel presente documento.** **→ Processi aziendali: Procurement** **Regolamento contratti per l'affidamento di beni e servizi di importo inferiore alle soglie comunitarie; Administration Operative Financial Management for IT-Billing; Manuale operativo contabilità SAP;**
03 – 02	Allo scopo di ridurre al minimo il rischio di commissione dei reati qui considerati, è obbligatorio rispettare col massimo rigore tutte le norme, aziendali e legislative, applicabili In particolare: → *"Procedura di autorizzazione interna delle forniture"* In linea generale, deve essere prevista la stratificazione dei poteri autorizzativi e la segregazione dei compiti, nell'ambito dell'organizzazione societaria, tra responsabilità nei rapporti con i clienti, responsabilità nella definizione del prezzo di offerta e delle condizioni di tempo e pagamento, responsabilità nella scontistica e nella definizione di eventuali risoluzioni transattive in caso di contestazioni;	**→ Vedasi "Procedura di autorizzazione interna delle forniture" descritta nel presente documento.** **→ Processi aziendali: Order management; Service Catalouge Management; Operative Financial Management; Request for Change; Needs analysis Technical Solution definition; Development; Validation an Testing; Information Security Management; Operative Financial Management for IT-Billing; Manuale operativo contabilità SAP** **→ Provvedimenti/Contrattualistica: Programmi annuali e pluriennali con la PAB; contratti quadro e di servizio con la PAB;**
03 - 04	Con riferimento sia al ciclo attivo, che al ciclo attivo la Società ed i suoi dipendenti dovranno conformarsi ai seguenti ulteriori principi: • improntare la propria condotta ai principi generali contenuti nel Codice Etico ed ai principi di legalità, correttezza, tracciabilità e trasparenza; • tutti i soggetti coinvolti nel processo devono essere debitamente autorizzati; i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Società devono essere appositamente incaricati; • verificare l'attendibilità commerciale e professionale dei clienti/fornitori/appaltatori/partner commerciali; • selezionare fornitori/appaltatori/partner commerciali in base alle loro capacità di offerta in termini di qualità innovazione e costi, che dimostrino standard elevati di condotta etica aziendale, con particolare riferimento al rispetto dei diritti	**→ Vedasi "Procedura di autorizzazione interna degli acquisti" descritta nel presente documento.** **→ Vedasi "Procedura di autorizzazione interna delle forniture" descritta nel presente documento.** **→ Processi aziendali: Procurement** **Regolamento contratti per l'affidamento di beni e servizi di importo inferiore alle soglie comunitarie; Administration; Order management; Service Catalouge Management; Operative Financial Management; Request for Change; Needs analysis Technical Solution definition; Development; Validation an Testing; Information Security Management; Operative Financial**

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
	umani, dell'ambiente, ai principi di legalità, trasparenza e correttezza negli affari; • verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni; • valutare con particolare attenzione l'affidabilità dei fornitori/appaltatori/partner/commerciali anche in relazione alla gestione del personale, al costo ed alla provenienza della manodopera utilizzata; • pattuire corrispettivi coerenti con le condizioni ed i prezzi di mercato, assicurando la trasparenza e la correttezza sostanziale e procedurale delle operazioni con Società collegate per garantire la sana gestione della Società; • qualora venisse previsto per l'espletamento dell'attività il coinvolgimento di collaboratori o consulenti esterni questo dovrà essere formalizzato per iscritto ed il relativo contratto dovrà contenere apposita dichiarazione di conoscenza della normativa di cui al Decreto nonché condivisione dei principi di cui al Codice Etico. Il relativo contratto dovrà essere stipulato in conformità ai principi ed alle procedure aziendali in tema di conferimento di mandati. Non è consentito riconoscere compensi in favore di tali collaboratori o consulenti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto. Il corrispettivo deve essere congruo ed il servizio reso documentato o documentabile; • l'intero processo in ogni sua fase deve essere tracciato, sia a livello informatico che documentale, così che le attività svolte siano documentate, coerenti e congrue. La funzione responsabile archivierà e conserverà la relativa documentazione in adempimento alla relativa procedura aziendale.	**Management for IT-Billing; Manuale operativo contabilità SAP** → **Provvedimenti/Contrattualistica: Programmi annuali e pluriennali con la PAB; contratti quadro e di servizio con la PAB;**
03 - 05	In ogni caso è fatto esplicito divieto di porre in essere e/o di concorrere a porre in essere comportamenti che possano condurre alla commissione dei reati qui descritti ed in particolare di: contrattare, negoziare e/o acquistare beni e/o servizi da fornitori dei Paesi a rischio individuati nelle c.d. "Liste Paesi", ovvero da fornitori già collegati a reati di criminalità organizzata transnazionale compresi nelle c.d. "Liste Nominative".	

[redacted] Peculato, concussione, induzione indebita a dare o promettere altra utilità, corruzione e abuso d'ufficio (Art. 25, D.Lgs. n. 231/2001) [articolo modificato dalla L. n. 190/2012; modificato dalla L. n. 3/2019; modificato dal D.Lgs. n. 75/2020]

[redacted] Reati richiamati dal D.Lgs. 231/01

L'articolo 25 del Decreto richiama specificatamente i seguenti articoli del Codice Penale:

- Peculato – in danno degli interessi finanziari dell'UE (art. 314, co. 1, c.p.)
- Peculato mediante profitto dell'errore altrui – in danno degli interessi finanziari dell'UE (art. 326 c.p.)
- Concussione (art. 317)
- Corruzione per l'esercizio della funzione (art. 318) (come modificato dalla L. 190/2012 e dalla L. 69/2015)
- Corruzione per un atto contrario ai doveri di ufficio (art. 319) (come modificato dalla L. 190/2012 e dalla L. 69/2015)

- Corruzione per un atto contrario ai doveri d'ufficio aggravato ai sensi dell'art. 319-bis
- Corruzione in atti giudiziari (art. 319-ter) (come modificato dalla L. 69/2015)
- Induzione indebita a dare o promettere utilità (art. 319-quater) (articolo aggiunto dalla L. 190/2012 e modificato dalla L. n. 69/2015)
- Corruzione di persona incaricata di un pubblico servizio (art. 320)
- Pene per il corruttore (art. 321)
- Istigazione alla corruzione (art. 322)
- 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 di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis)
- Abuso d'ufficio – in danno agli interessi finanziari dell'UE (art. 323 c.p.)
- Traffico di influenze illecite (art. 346bis c.p.)

Esemplificazioni delle fattispecie di reato richiamate sono le seguenti.

A) Il pubblico ufficiale o l'incaricato di un pubblico servizio, che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, se ne appropria

B) Il pubblico ufficiale o l'incaricato di un pubblico servizio, il quale, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità

C) Il pubblico ufficiale o l'incaricato di un pubblico servizio che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità;

D) Il pubblico ufficiale o l'incaricato di un pubblico servizio che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa; commette il reato anche chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità;

E) Il pubblico ufficiale o l'incaricato di un pubblico servizio, che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa; commette il reato anche chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità

F) Abusando della qualità o dei poteri di pubblico ufficiale o di incaricato di pubblico servizio, si induce taluno a dare o a promettere indebitamente (a sé o a un terzo) denaro o altra utilità. Nella medesima circostanza, subendo la sollecitazione di un pubblico ufficiale o di un incaricato di pubblico servizio, si dà o si promette indebitamente denaro o altra utilità.

G) Offrire promettere denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, qualora l'offerta o la promessa non sia accettata; indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, qualora l'offerta o la promessa non sia accettata.

H) Viene commesso il reato di cui al punto D e E precedente finalizzato a favorire o danneggiare una parte in un processo civile, penale o amministrativo.

I) Il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto.

J) Sfruttare o vantare relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio, per fare dare o promettere, a sé o ad altri, denaro o altra utilità come prezzo della propria mediazione illecita verso un pubblico ufficiale o incaricato di un pubblico servizio ovvero per rimunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri.

K) Le fattispecie di reati fin qui considerati vengono commessi da chi, o nei confronti di chi, nell'ambito di altri Stati esteri (comunitari o extra-europei), svolga funzioni o attività corrispondenti a quelle di pubblico ufficiale o di incaricato di un pubblico servizio.

Contestualizzazione aziendale e modalità di commissione

Alcuni dei reati presupposto qui richiamati, sono "*reati propri*", che possono essere commessi solo da Soggetti qualificati Pubblico Ufficiale ovvero Incaricato di un Pubblico Servizio. Ciononostante, di seguito vengono comunque indicati Soggetti (appartenenti all'organizzazione di SIAG) che potrebbero risultare esposti al rischio di commissione dei reati qui richiamati; ciò in ragione di uno dei seguenti motivi:

- i reati potrebbero essere commessi da personale che, operando in SIAG, svolge/svolgerà incarichi di pubblico servizio per un Cliente della P. A.;
- svolgono la funzione di RUP, DEC o commissione di gara: verifica ed autorizzazione dei lavori/servizi/beni;
- un Dipendente SIAG, subendo la sollecitazione di un pubblico ufficiale o di un incaricato di pubblico servizio, indebitamente potrebbe dare o promettere a terzi denaro od altra utilità;
- un Dipendente SIAG potrebbe offrire/promettere denaro od un'altra utilità ad un Pubblico Ufficiale o Incaricato di un Pubblico Servizio, affinché questi commetta/ometta/ritarda un atto d'ufficio, nell'interesse ovvero a vantaggio della Società

Ciò premesso, rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società è significativo, soprattutto con riferimento ai seguenti **Soggetti/UU.OO. sensibili**:

- Management aziendale,
- Dipendenti SIAG operanti nei Settori *"Run"* e *"Production".*

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Selezione, negoziazione ed esecuzione di contratti con fornitori, prestatori di servizi ed appaltatori, consulenti (Ciclo Passivo: acquisti ed approvvigionamenti)
  - Svolgimento della funzione di RUP, DEC o commissione di gara
  - Incarichi a consulenti che nello svolgimento del loro incarico abbiano contatti con la PA
- Gestione dei rapporti con soggetti pubblici per l'ottenimento di autorizzazioni e licenze per l'attività aziendale
- Gestione di procedimenti volti a conseguire erogazioni, contributi, sovvenzioni e finanziamenti pubblici
  - Erogazione di forniture che godono di finanziamenti o rimborsi da parte di Enti Pubblici o Comunitari
  - Assunzione di Personale: conseguimento di agevolazioni fiscali/contributive
- Gestione dei rapporti con l'Amministrazione finanziaria, INPS, INAIL, Ufficio del lavoro
- Gestione dei rapporti con la GdF e con altri funzionari pubblici nell'ambito delle attività di verifica ispettiva e di controllo effettuate dalla PA
- Gestione delle spese di rappresentanza
- Flussi finanziari
  - Gestione cassa/pagamenti in contanti
- Negoziazione, stipula ed esecuzione di contratti con clienti:
  - Stesura Offerta-Contratto nei confronti di un Ente Pubblico
  - Processo di approvazione/autorizzazione preventivo fornitura di servizi
  - Project Management: controllo e verifica, in corso d'opera, del rispetto dei requisiti contrattuali
- Assunzione personale

Le **modalità di commissione del reato** che si possono astrattamente ipotizzare sono le seguenti.

- Con specifico riferimento al contesto che vede l'Azienda entrare in contatto con un Funzionario/Rappresentante dell'amministrazione dello Stato o di un Ente Pubblico o Comunitario o a persone a queste collegabili, ovvero all'ipotesi che un Dipendente della SIAG svolga la funzione di un Incaricato di un Pubblico Servizio (in particolare nell'ambito del processo di approvvigionamento) le

seguenti attività potrebbero astrattamente configurarsi come di natura corruttiva/concussiva, finalizzate, cioè, ad ottenere un indebito vantaggio o a ricompensare per il conseguimento dello stesso:

- acquisto di forniture o di prestazioni professionali (es.: apparati HW, prodotti SW, consulenze, ecc.)
- assunzione di personale da parte dell'Azienda
- offerta, donazione di beni, ad es.: orologi di valore, apparecchiature HW, viaggi turistici ecc.

Si segnala infine che la Società ha deciso di connotare come reati "*di particolare rilevanza*" gli eventuali reati commessi nell'ambito dei rapporti (preliminari o successivi alla formalizzazione contrattuale) instaurati con una Pubblica Amministrazione, *Centrale* o *Locale*, o con Istituzioni Comunitarie e di sanzionarli con maggior severità nell'ambito del *sistema disciplinare* descritto nel presente Modello.

Presidio del rischio attuato dalla Società

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.7.7.1. Principi specifici di comportamento

- Le casistiche di comportamento (A, B e C) che di seguito vengono vietate, restano tali, ovvero "vietate" in quanto i comportamenti ipotizzati siano adottati nell'interesse o a vantaggio della Società.
  - A) A chiunque si presenti in nome o per conto di Informatica Alto Adige è severamente vietato porre in essere atti finalizzati a corrompere un Funzionario/Rappresentante di un'Amministrazione dello Stato o di un Ente Pubblico o Comunitario, o un Incaricato di pubblico servizio.
  - B) Ad un Soggetto che, per conto di Informatica Alto Adige, si trovasse impegnato nella predisposizione di un'Offerta o nell'erogazione di una fornitura a favore di un Ente Pubblico, è severamente vietato richiedere per sé o per terzi ovvero indurre taluno ad offrire, a lui o a terzi, denaro o altra utilità, a fronte della commissione di un atto illecito.
  - C) Ad un Soggetto che, per conto di Informatica Alto Adige, si trovasse impegnato nell'erogazione di un servizio a favore di un Ente Pubblico, è severamente vietato:
    - abusando della qualità o dei poteri di Pubblico Ufficiale o di Incaricato di pubblico servizio (a lui eventualmente conferiti dal Cliente per l'erogazione del servizio), indurre taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità;
    - subendo la sollecitazione di un Pubblico Ufficiale o di un Incaricato di pubblico servizio, dare o promettere indebitamente denaro o altra utilità.

D) Ad un Soggetto che, per conto di Informatica Alto Adige, si trovasse nella situazione di svolgere la funzione di Incaricato di un Pubblico Servizio (p.es. RUP, DEC o componente di una commissione di gara) è severamente vietato abusare della propria qualità o dei poteri di soggetto privato che esercita una pubblica funzione, costringendo o inducendo taluno a dare o promettere indebitamente denaro o altra utilità.

- Allo scopo di avere totale garanzia che nell'ambito di una fornitura a favore di qualunque Cliente, sia chiara la volontà della Società di rifuggire da qualsiasi comportamento di carattere corruttivo o, comunque, illecito (ancorché condotto nell'interesse o a vantaggio della Società), i Soggetti aziendali obbligatoriamente tenuti ad autorizzare la fornitura, anche con riferimento ad aspetti legati a fasi del "ciclo passivo" (quali, ad esempio, acquisizioni esterne finalizzate all'erogazione della fornitura) sono tenuti a sottoscrivere una dichiarazione con la quale si attesta:
  - che, sulla base delle informazioni a loro disposizione e fino alla data di sottoscrizione della dichiarazione in questione, in nessuna fase della trattativa commerciale o della formalizzazione contrattuale si sono verificati episodi che, anche ipoteticamente, appaiano riconducibili o comunque diretti ad atti RILEVANTI ai sensi del D.Lgs. 231/01;
  - l'impegno a comunicare immediatamente all'Organismo di Vigilanza ex D.Lgs. 231/01 eventuali tentativi, episodi o atti anche ipoteticamente inquadrabili fra gli illeciti sopra menzionati, laddove

gli stessi si verificassero successivamente alla sottoscrizione della dichiarazione in questione, fino al completo espletamento della fornitura.

- Nei rapporti con Clienti e, più precisamente, con Funzionari o Rappresentanti della Pubblica Amministrazione (Stato, Ente pubblico o Ente Comunitario), omaggi o benefici materiali sono ammessi (eventualmente a favore di persone a loro vicine) solo ed esclusivamente se tali elargizioni rientrano nelle normali prassi commerciali e, cioè, se soddisfano entrambe le seguenti condizioni:
  A) l'omaggio (o beneficio) è di modico valore;
  B) l'omaggio (o beneficio) non è tale da poter apparire come:
     - capace di condizionare l'autonomia di giudizio del beneficiario ovvero
     - finalizzato ad incoraggiare o a ricompensare l'illecito comportamento del beneficia

  in entrambi i casi, a vantaggio di Informatica Alto Adige.

  A chiunque si presenti in nome o per conto di Informatica Alto Adige è quindi vietato offrire o promettere a Funzionari o a Rappresentanti della Pubblica Amministrazione (Stato, Ente pubblico o Ente Comunitario) omaggi (o benefici) non rientranti nelle normali prassi commerciali.

  Chiunque riceva, da parte di Terzi, l'offerta o la sollecitazione di un omaggio o di un beneficio che non rientri nelle normali prassi commerciali, è tenuto ad informare il proprio Responsabile diretto ed a darne formale comunicazione alla funzione di Internal Auditing ed all'Organismo di Vigilanza.
- Relativamente al processo di gestione, mediante applicativo software, dei dati anagrafici dei Fornitori, dati che comprendono, fra gli altri, le coordinate bancarie degli stessi, in SIAG le credenziali che abilitano alle funzioni SW di inserimento e modifica delle coordinate bancarie vengono rilasciate ad un massimo di due Dipendenti.
- Improntare la propria condotta ai principi generali contenuti nel Codice Etico ed ai principi di legalità, correttezza, tracciabilità e trasparenza.
- Stretta osservanza di tutte le leggi, regolamenti e procedure interne che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con la PA ed alle attività funzionali e strettamente correlate al servizio di trasporto pubblico.
- Instaurare e mantenere qualsiasi rapporto con terzi in tutte le attività di fornitura del servizio, nonché in tutte le attività funzionali al servizio di fornitura o ad attività ad esso strettamente correlate, sulla base di criteri di correttezza e trasparenza che garantiscano il buon andamento della funzione o servizio e l'imparzialità nello svolgimento degli stessi.
- Tutti i soggetti che intrattengano rapporti con la PA devono essere individuati e debitamente autorizzati; i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Società devono essere appositamente incaricati.
- I rapporti e gli adempimenti nei confronti della PA devono essere effettuati con la massima trasparenza, diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere.
- Qualora venisse previsto per l'espletamento dell'attività il coinvolgimento di collaboratori o consulenti esterni questo dovrà essere formalizzato per iscritto ed il relativo contratto dovrà contenere apposita dichiarazione di conoscenza della normativa di cui al Decreto nonché condivisione dei principi di cui al Codice Etico. Il relativo contratto dovrà essere stipulato in conformità ai principi ed alle procedure aziendali in tema di conferimento di incarichi esterni. Non è consentito riconoscere compensi in favore di tali collaboratori o consulenti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto. Il corrispettivo deve essere congruo ed il servizio reso documentato o documentabile.
- L'intero processo in ogni sua fase deve essere tracciato, sia a livello informatico che documentale, così che le attività svolte siano documentate coerenti e congrue. La funzione responsabile archivierà e conserverà la relativa documentazione in adempimento alla relativa procedura aziendale.

2.7.7.2. Protocolli aziendali e controlli relativi ai processi

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
04 – 01	Allo scopo di ridurre al minimo il rischio di commissione dei reati qui considerati, è obbligatorio rispettare col massimo rigore tutte le norme aziendali riportate nei protocolli qui referenziati ed, in particolare, quelle applicabili ai processi sensibili precedentemente evidenziati. Oltre alle norme contenute nei documenti referenziati, vanno rigorosamente osservate anche i seguenti protocolli, nonché i seguenti divieti con riferimento alle singole attività sensibili.	**→ Modello organizzativo: Codice etico e di comportamento** **PTPC (Piano Triennale per la Prevenzione della Corruzione)** **→ Vedasi "Procedura di autorizzazione interna degli acquisti" descritta nel presente documento.** **→ Vedasi "Procedura di autorizzazione interna delle forniture" descritta nel presente documento.** **→ <u>Processi aziendali</u>: Procurement; Order management; Service Catalouge Management; Operative Financial Management; Request for Change; Needs analysis Technical Solution definition; Development; Validation an Testing; Information Security Management; Recruiting, Onboarding, Training, Offboarding, Regolamento interno per il reclutamento; Administration Operative Financial Management for IT-Billing; Manuale operativo contabilità SAP;** **Regolamento contratti per l'affidamento di beni e servizi di importo inferiore alle soglie comunitarie;** **Regolamento di servizio** **→ <u>Provvedimenti/Contrattualistica</u>: Programmi annuali e pluriennali con la PAB; contratti quadro e di servizio con la PAB;**
04 – 02	<u>→ Gestione dei rapporti con la GdF e con altri funzionari pubblici nell'ambito delle attività di verifica ispettiva e di controllo effettuate dalla PA</u> La Società ed i suoi dipendenti dovranno attenersi ai suddetti principi cardini ed ai seguenti ulteriori principi: • in applicazione del principio di segregazione chi gestisce i rapporti con i funzionari pubblici durante le fasi ispettive non avrà il compito di supervisionare e firmare il verbale ispettivo; • verrà predisposto un report riepilogativo delle visite ispettive ricevute da trasmettere all'Organismo di Vigilanza: nel report verranno indicati oggetto, Ente ispettivo, periodo di riferimento, elenco documentazione chiesta e consegnata, eventuali rilievi/sanzioni/prescrizioni. In ogni caso è fatto divieto di: • predisporre e inviare, così come accettare documenti consapevolmente incompleti e/o comunicare dati falsi o alterati; • tenere una condotta ingannevole che possa indurre la PA;	**→ Modello organizzativo: Codice etico e di comportamento** **PTPC (Piano Triennale per la Prevenzione della Corruzione)**

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
	• promettere o dare seguito a richieste di funzionari pubblici in sede ispettive, ovvero di soggetti da questi indicati, al fine di indurre ad assicurare qualsiasi vantaggio alla Società.	
04 - 03	→ Gestione delle spese di rappresentanza • I parametri per le spese di rappresentanza devono essere predefiniti e le spese devono essere adeguatamente documentate. In ogni caso è fatto divieto di: ricevere o sollecitare elargizioni in denaro, omaggi, regali, o vantaggi di altra natura, nello svolgimento di tutte le attività inerenti il processo di approvvigionamento pubblico o ad esso strettamente correlati; promettere o corrispondere utilità e/o vantaggi, siano esse somme di denaro, doni, prestazioni al di fuori di quanto di prassi, al fine di promuovere o favorire gli interessi della Società o influenzare illecitamente atti o comportamenti della PA; affidare incarichi a collaboratori o consulenti esterni eludendo i criteri di cui alle policies e procedure aziendali.	→ **Modello organizzativo: Codice etico e di comportamento** **PTPC (Piano Triennale per la Prevenzione della Corruzione)** **Regolamento di servizio**
04 - 04	→ Flussi finanziari • in applicazione del principio di segregazione provvedere che il processo di incasso/pagamenti coinvolge una pluralità di attori, con responsabilità di gestione, verifica ovvero approvazione; • per quanto riguarda la gestione della cassa: rispetto delle norme di legge che regolano le transazioni commerciali, specialmente con riferimento al limite massimo nell'impiego del contante.	→ **Modello organizzativo: Codice etico e di comportamento** **PTPC (Piano Triennale per la Prevenzione della Corruzione)** **Administration Operative Financial Management for IT-Billing; Manuale operativo contabilità SAP;**
04 – 05	→ Assunzione personale La Società ed i suoi dipendenti dovranno attenersi ai suddetti principi cardini nonché ai seguenti ulteriori principi: • promozioni, premi ed incentivi: >> per Personale non dirigente: il *Management* fissa annualmente gli obiettivi della Società ed, in funzione di questi, gli obiettivi dei singoli Dipendenti; a fine anno i singoli Responsabili di Reparto formulano le valutazioni dei loro Collaboratori; tali valutazioni vengono discusse collegialmente dal *Management*, che fissa ed assegna ai Dipendenti i rispettivi riconoscimenti; • per Personale del Management: il processo da seguire è analogo al precedente, dove gli obiettivi vengono però fissati dal Direttore per ciascun membro del Management e, a fine anno, riconosciuti agli Stessi; • verificare in sede di assunzione in società di personale di eventuali precedenti penali per i reati presupposto di cui all'art. 231/2001. In ogni caso è fatto divieto di: • promettere o dare seguito a richieste di assunzione in favore di rappresentanti/esponenti della Pubblica Amministrazione ovvero di soggetti da questi indicati, al fine di influenzare l'indipendenza di giudizio o indurre ad assicurare qualsiasi vantaggio alla Società.	→ **Modello organizzativo: Codice etico e di comportamento** **PTPC (Piano Triennale per la Prevenzione della Corruzione)** **Recruiting, Onboarding, Training, Offboarding, Regolamento interno per il reclutamento;**

Delitti contro l'industria e il commercio (Art. 25-bis.1 del D.Lgs. 231/01)

Reati richiamati dal D.Lgs. 231/01

L'articolo 25-bis.1 del Decreto richiama specificatamente i seguenti reati.

A) Turbata libertà dell'industria o del commercio
B) Illecita concorrenza con minaccia o violenza
C) Frodi contro le industrie nazionali
D) Frode nell'esercizio del commercio
E) Vendita di sostanze alimentari non genuine come genuine
F) Vendita di prodotti industriali con segni mendaci
G) Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale
H) Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari

Esemplificazioni delle fattispecie di reato richiamate sono, rispettivamente, le seguenti.

A) Facendo violenza sulle cose o con mezzi fraudolenti si impedisce o si turba l'esercizio di un'industria
B) Nell'esercizio di un'attività si compiono atti di concorrenza con violenza o minaccia
C) Si vendono o si mettono in circolazione prodotti con nomi, marchi o segni distintivi contraffatti o alterati, cagionando un nocumento all'industria nazionale
D) Nell'esercizio di un'attività si consegna all'acquirente una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita
E) Si pone in vendita o si mettono in commercio come genuine sostanze alimentari non genuine
F) Si pone in vendita o si mettono in circolazione opere dell'ingegno o prodotti industriali con nomi, marchi o segni distintivi atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto
G) Potendo conoscere dell'esistenza del titolo di proprietà industriale, si fabbricano o si adoperano industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso. Ovvero, al fine di trarne profitto e con riferimento agli stessi beni, questi vengono introdotti nel territorio dello Stato o posti in vendita o comunque in circolazione
H) Si contraffanno o comunque si alterano indicazioni geografiche o denominazioni di origine di prodotti agroalimentari. Ovvero, al fine di trarne profitto e con riferimento agli stessi prodotti con indicazioni/denominazioni contraffatte, questi vengono introdotti nel territorio dello Stato o posti in vendita o comunque in circolazione

Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società è significativo, soprattutto con riferimento ai seguenti **Soggetti/UU.OO. sensibili**:

- Management aziendale
- Reparti coinvolti nell'erogazione di una fornitura al Cliente
- Service Area Manager

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Negoziazione, stipula ed esecuzione di contratti con clienti:
  - Stesura Offerta-Contratto nei confronti di un Ente Pubblico
  - Processo di approvazione/autorizzazione preventivo fornitura di servizi

Project Management: controllo e verifica, in corso d'orpera, del rispetto dei requisiti contrattuali

Modalità di commissione del reato.

- Con riferimento ai reati precedentemente elencati, di cui alle lettere A) e B): essendo SIAG una società "in house", il livello del rischio di commissione dei reati evocati può considerarsi, quanto meno, moderato.

- Con riferimento ai reati precedentemente elencati, di cui alle lettere C), E), F), G) ed H): nella realtà aziendale tali reati non sono neppure astrattamente ipotizzabili.
- Per il reato di cui alla lettera D) del precedente elenco: con riferimento ad un bene o ad un prodotto fornito ai propri Clienti (HW e SW) si può astrattamente ipotizzare che l'Azienda adotti uno dei seguenti comportamenti:

  viene consegnato al Cliente un bene/prodotto (HW o SW), per origne, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita.

Presidio del rischio attuato dalla Società

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.8.3.1. Principi specifici di comportamento

Si rimanda ai "*Principi generali di comportamento"* indicati nel paragrafo 2.2., nonché ai seguenti principi, ai quali la Società ed i suoi Dipendenti dovranno conformarsi:

- improntare la propria condotta ai principi generali contenuti nel Codice Etico e di Condotta ed ai principi di legalità, correttezza, tracciabilità e trasparenza;
- tenere condotte tali da garantire il libero e corretto svolgimento del commercio nonché una lecita concorrenza;
- qualora venisse previsto per l'espletamento dell'attività il coinvolgimento di collaboratori o consulenti esterni questo dovrà essere formalizzato per iscritto ed il relativo contratto dovrà contenere apposita dichiarazione di conoscenza della normativa di cui al Decreto nonché condivisione dei principi di cui al Codice Etico. Il relativo contratto dovrà essere stipulato in conformità ai principi ed alle procedure aziendali in tema di conferimento di mandati. Non è consentito riconoscere compensi in favore di tali collaboratori o consulenti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto. Il corrispettivo deve essere congruo ed il servizio reso documentato o documentabile;
- l'intero processo in ogni sua fase deve essere tracciato, sia a livello informatico che documentale, così che le attività svolte siano documentate coerenti e congrue. La funzione responsabile archivierà e conserverà la relativa documentazione.

2.8.3.2. Protocolli aziendali e controlli relativi ai processi

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
05 – 01	In ogni caso è fatto esplicito divieto di porre in essere e/o di concorrere a porre in essere comportamenti che possano condurre alla commissione dei reati qui descritti. Così in particolare, a titolo meramente esemplificativo e non esaustivo, è fatto divieto di: • effettuare la vendita o comunque mettere in altro modo in circolazione, prodotti con nomi, marchi o segni distintivi,	**→ Vedasi "Procedura di autorizzazione interna degli acquisti" descritta nel presente documento.** **→ Vedasi "Procedura di autorizzazione interna delle forniture" descritta nel presente documento.**

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
	certificazioni alterati o contraffatti, che possano produrre un danno per l'industria; • effettuare la vendita o comunque mettere in altro modo in circolazione, prodotti con nomi, marchi o segni distintivi altrui anche se non registrati, al fine di trarre in inganno il cliente; • utilizzare o mettere in altro modo in circolazione merci beni o altri prodotti con nomi, marchi o segni distintivi altrui anche se non registrati ovvero contraffatti, sia pure ove trattasi di prodotti semilavorati e destinati al solo assemblaggio con prodotti originali acquistati da fornitori non selezionati in modo conforme alle procedure della Società; • utilizzare o mettere in altro modo in circolazione merci beni o altri prodotti acquistati da fornitori dei Paesi a rischio individuati nelle c.d. "Liste Paesi", ovvero da fornitori già collegati a reati di criminalità organizzata transnazionale compresi nelle c.d. "Liste Nominative"; • consegnare ai Clienti, prodotti, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita; • utilizzare nell'ambito della propria attività produttiva beni, procedure e/o metodi brevettati usurpando titoli di proprietà industriale; • compiere atti di concorrenza con violenza o minaccia, quali ad esempio condotte di boicottaggio, rifiuto di contrattare, storno di dipendenti, minaccia e intimidazione, verso altri soggetti e competitors della Società operanti nello stesso settore e nella stessa area. In aggiunta a quanto precede, al fine di presidiare l'Area e le Attività Sensibili rispetto alla possibile commissione dei reati in esame dovranno inoltre essere rispettate le previsioni contenute nelle procedure aziendali in essere.	→ **Processi aziendali: Order management; Service Catalouge Management; Operative Financial Management; Request for Change; Needs analysis Technical Solution definition; Development; Validation an Testing; Information Security Management; Operative Financial Management for IT-Billing; Manuale operativo contabilità SAP** → **Provvedimenti/Contrattualistica: Programmi annuali e pluriennali con la PAB; contratti quadro e di servizio con la PAB;**

Reati societari (Art. 25-ter del D.Lgs. 231/01) (come modificato dal D.Lgs. 38/2017 e dalla Legge 3/2019).

Reati richiamati dal D.Lgs. 231/01

L'articolo 25-ter del Decreto richiama specificatamente i seguenti reati.

- False comunicazioni sociali (art. 2621 c.c.)
- False comunicazioni sociali previsto dall'art. 2621-bis c.c. (articolo introdotto dalla L. n. 69/2015)
- False comunicazioni sociali delle società quotate (art. 2622 c.c., come sostituito dalla L. n. 69/2015)
- Impedito controllo, indebita restituzione di conferimenti, illegale ripartizione degli utili e delle riserve, illecite operazioni sulle azioni o quote sociali o della società controllante, operazioni in pregiudizio dei creditori
- Formazione fittizia del capitale, indebita ripartizione dei beni sociali da parte dei liquidatori
- Illecita influenza sull'assemblea, aggiotaggio, ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza
- Omessa comunicazione del conflitto d'interessi
- Corruzione tra privati (modificato dal D.Lgs. n. 38/2017 e da ultimo con Legge 3/2019)
- Istigazione alla corruzione tra privati, previsto dall'art. 2635-bis c.c. (articolo aggiunto dal D.Lgs. 38/2017 e modificato con Legge 3/2019)

Esemplificazioni delle fattispecie di reato richiamate sono le seguenti.

- Con l'intenzione di ingannare i Soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali si espongono fatti materiali rilevanti non veri o si omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società, in modo concretamente idoneo ad indurre in errore i destinatari sulla predetta informativa.
- Si impedisce o si ostacola lo svolgimento delle attività di controllo ai Soggetti (Soci o altri Organi sociali) a cui sono state legalmente attribuite.
- Gli Amministratori:
  - illegittimamente, restituiscono (anche simulatamente) i conferimenti ai Soci o li liberano dall'obbligo di eseguirli
  - ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartiscono riserve che non possono per legge essere distribuite
  - illegittimamente, acquistano o sottoscrivono azioni o quote sociali (oppure azioni o quote emesse dalla società controllante), cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge
  - in violazione delle disposizioni di legge, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori.
- Gli Amministratori e i Soci conferenti formano o aumentano fittiziamente il capitale sociale
- I Liquidatori ripartiscono i beni sociali tra i Soci prima di pagare i creditori sociali, cagionando loro un danno
- Con atti simulati o fraudolenti si determina la maggioranza in assemblea allo scopo di procurare a sé o ad altri un ingiusto profitto
- Si diffondono notizie false, si pongono in essere operazioni simulate o altri artifici idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati, ovvero idonei ad
- incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari
- Nelle comunicazioni alle autorità pubbliche di vigilanza, al fine di ostacolarne l'esercizio delle funzioni, si espongono fatti materiali non rispondenti al vero sulla situazione economica, patrimoniale o finanziaria ovvero, allo stesso fine, (anche omettendo di fornire informazioni) si occultano con altri mezzi fraudolenti, in tutto o in parte, fatti concernenti la situazione medesima
- L'Amministratore o membro del CdA omette di informare sull'interesse che ha (per conto proprio o di terzi) in un'operazione della Società. In caso di Presidente, non si astiene dal compierla
- Nell'interesse della Società, si dà o si promette denaro o altra utilità ad un Soggetto appartenente ad una Società privata, , affinché questi compi o ometta un atto in violazione degli obblighi inerenti al suo ufficio o degli obblighi di fedeltà.

Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società è teoricamente *significativo* e coinvolge i seguenti **Soggetti/UU.OO. sensibili**:

- Componenti del Consiglio di Amministrazione
- Componenti del Management aziendale.

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Predisposizione di bilanci, relazioni e comunicazioni

  - Gestione della contabilità generale ed analiticagestione chiusure contabili e formazione Bilancio
  - gestione adempimenti fiscali
  - gestione immobilizzazioni/gestione cespiti
- Gestione dei rapporti con il Collegio Sindacale, con il Revisore dei conti e con i Soci
- Gestione sociale: conferimenti utili, riserve ed operazioni sul capitale
- Rapporti con i Soci
- Gestione dei rapporti con le autorità di vigilanza
- Selezione, negoziazione ed esecuzione di contratti con fornitori, prestatori di servizi ed appaltatori, consulenti
- Gestione delle spese di rappresentanza
- Flussi finanziari
  - Gestione cassa/pagamenti in contanti

Relativamente alle **modalità di commissione del reato** si rileva che molteplici sono i Soggetti astrattamente in grado di operare per la commissione di questi reati-presupposto, così come molteplici sono, teoricamente, le modalità con cui gli stessi reati potrebbero essere commessi.

A titolo esemplificativo (qualunque elenco risulterebbe infatti inevitabilmente parziale), astrattamente si possono ipotizzare, a livello generale, le seguenti possibili modalità di compimento dei reati in questione:

- uno o più Amministratori, in deroga allo spirito ed al contenuto del codice Etico, dagli stessi approvato, inducono uno o più soggetti ad operare al fine di produrre dati di Bilancio, relazioni o comunicazioni sociali non veritiere
- uno o più Amministratori, non fornendo una piena e trasparente collaborazione ai Soggetti a cui sono state legalmente attribuite attività di controllo (Soci o altri Organi sociali), inducono gli stessi Soggetti a valutazioni parziali o errate
- Componenti del Management aziendale, attuando un livello di controllo inadeguato presso le strutture che a loro rispondono, non rilevano la sistematica produzione di dati contabili errati, con impatto distorcente su specifiche voci di Bilancio (ad es.: accantonamenti, dati del ciclo attivo/passivo inerenti le commesse, ecc.).
- allo scopo ultimo di conseguire un vantaggio per Informatica Alto Adige, si offre denaro o altra utilità ad un Soggetto operante in altra Società, inducendolo a venir meno ai propri doveri di correttezza e fedeltà verso la Società per la quale opera.

Presidio del rischio attuato dalla Società

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.9.3.1. Principi specifici di comportamento

- Tutti i soggetti che intrattengano rapporti con, fornitori di beni e servizi, appaltatori, devono essere debitamente autorizzati; i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Società devono essere appositamente incaricati.
- La trasparenza nel ciclo passivo verrà garantita con la segregazione di compiti e responsabilità con particolare riferimento alla valutazione delle offerte, all'esecuzione delle prestazioni, nonché alla liquidazione dei pagamenti; la regolarità dei pagamenti andrà verificata con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni.

- Pattuire corrispettivi coerenti con le condizioni ed i prezzi di mercato, assicurando la trasparenza e la correttezza sostanziale e procedurale delle operazioni con Società collegate per garantire la sana gestione della Società.
- E' severamente vietato a chiunque si presenti in nome o per conto di Informatica Alto Adige, offrire denaro o altra utilità ad un Soggetto operante in altra Società, anche privata, inducendolo così a venir meno ai doveri di correttezza e fedeltà verso la Società per la quale opera, tutto ciò allo scopo ultimo di conseguire un vantaggio per Informatica Alto Adige.

- A chiunque è vietato offrire danaro o altri beni a singoli Membri del Collegio Sindacale o ad altri Soggetti (eventualmente professionisti esterni a SIAG) che svolgono, anche di fatto, funzioni di revisione e controllo contabile, il tutto al fine di ottenere un loro atteggiamento connivente.

- Il Responsabile Funzione Finance deve comunicare all'Organismo di Vigilanza, con adeguata motivazione, l'eventuale verificarsi di uno dei seguenti eventi:
  - revoca di incarico al Commercialista che assiste la Società;
  - assegnazione di incarico ad un nuovo Commercialista.

- In Informatica Alto Adige, ai fini dell'elaborazione e della rappresentazione dei bilanci, delle relazioni, dei prospetti o di altre comunicazioni sociali è vietato a chiunque comunicare o utilizzare informazioni o dati non veritieri, lacunosi e tali comunque da non consentire la rappresentazione della reale situazione economica, patrimoniale e finanziaria della Società.

- Gli Amministratori, i componenti del Management aziendale e tutte le strutture che ad essi rispondono, così come la funzione di Internal Auditing, sono tenuti ad un comportamento di massima collaborazione nei confronti dei Soggetti a cui sono state legalmente attribuite attività di controllo (Soci o altri Organi sociali), fornendo loro informazioni vere, chiare, complete e tempestive.

- SIAG è tenuta a redigere ed a pubblicare annualmente il proprio Bilancio. A soli fini interni, vengono effettuate anche chiusure contabili semestrali.

  Il processo che porta all'approvazione del Bilancio annuale deve prevedere i seguenti macro-step (se non diversamente indicato, le attività sono a carico della Funzione Finance):

  - chiusura contabile delle partite ordinarie (stipendi, fatture attive e passive, movimenti bancari, ecc);
  - controllo (a campione) di voci particolarmente critiche e/o significative (ad es.: debiti/crediti erariali, contributi sociali, debiti vs Fornitori, crediti vs Clienti, fatture da emettere/da ricevere, ecc); al termine viene effettuato un ulteriore controllo a campione, pilotato da apposita check-list;
  - inserimento di scritture di rettifica, con raccolta di pezze giustificative;
  - verifica, da parte del consulente Commercialista, della bozza del Bilancio;
  - trasmissione del progetto di Bilancio al Collegio sindacale, che lo verifica e che può, ad esempio, richiedere un certo numero di circolarizzazioni, chiedere chiarimenti su alcune scritture di rettifica, autorizzare la movimentazione di un fondo di svalutazione crediti, ecc;
  - il Direttore ed il Presidente verificano e firmano la bozza di Bilancio;
  - la bozza di Bilancio viene presentata, discussa ed approvata dal CdA;
  - il Bilancio viene presentato, discusso ed approvato dall'Assemblea dei Soci.

- Ad ogni commessa/progetto è assegnato, tramite l'applicazione SW Work Manager, un Responsabile di commessa/Capo progetto/Service Area Manager ("SAM").

  Sempre mediante l'impiego dell'applicazione SW Work Manager, il citato Responsabile è tenuto, con periodicità mensile o, al massimo, trimestrale:

  - ad autorizzare i consuntivi dei Colleghi che hanno lavorato, nel periodo, per la commessa;

- a dichiarare i ricavi maturati nel rispetto dei seguenti criteri:
  - ✓ in caso di commesse "T&M": [numero giorni] x tariffa (con rendicontazione, al Cliente, dei costi sostenuti);
  - ✓ in caso di servizi a canone: canone prefissato;
  - ✓ in caso di contratto "chiavi in mano": in proporzione ai costi sostenuti.

Ogni Responsabile di Reparto/SAM è tenuto, prima del consolidamento di un periodo contabile, a verificare la correttezza dei consuntivi di tutti i Dipendenti del Reparto.

- Periodicamente, ma in particolar modo in fase preliminare alla chiusura del Bilancio, la funzione di Internal Auditing svolge, presso la Funzione Finance, verifiche a campione circa la completezza e veridicità delle scritture contabili.
  - Qualora venisse previsto per l'espletamento dell'attività il coinvolgimento di collaboratori o consulenti esterni questo dovrà essere formalizzato per iscritto ed il relativo contratto dovrà contenere apposita dichiarazione di conoscenza della normativa di cui al Decreto nonché condivisione dei principi di cui al Codice Etico. Il relativo contratto dovrà essere stipulato in conformità ai principi ed alle procedure aziendali in tema di conferimento di mandati. Non è consentito riconoscere compensi in favore di tali collaboratori o consulenti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto. Il corrispettivo deve essere congruo ed il servizio reso documentato o documentabile.

2.9.3.2. Protocolli aziendali e controlli relativi ai processi

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
06 – 01	Allo scopo di ridurre al minimo il rischio di commissione dei reati qui considerati, è obbligatorio rispettare col massimo rigore tutte le norme di legge ed aziendali applicabili ai seguenti processi sensibili: ➢ Predisposizione di bilanci, relazioni e comunicazioni o Gestione della contabilità generale ed analiticagestione chiusure contabili e formazione Bilancio o gestione adempimenti fiscali o gestione immobilizzazioni/gestione cespiti ➢ Gestione dei rapporti con il Collegio Sindacale, con il Revisore dei conti e con i Soci ➢ Gestione sociale: conferimenti utili, riserve ed operazioni sul capitale ➢ Rapporti con i Soci ➢ Gestione dei rapporti con le autorità di vigilanza ➢ Selezione, negoziazione ed esecuzione di contratti con fornitori, prestatori di servizi ed appaltatori, consulenti ➢ Gestione delle spese di rappresentanza ➢ Flussi finanziari o Gestione cassa/pagamenti in contanti Oltre alla puntuale applicazione del sistema aziendale di deleghe nei processi autorizzativi svolti a monte dell'approvazione del Bilancio,	→ **Vedasi "Procedura di autorizzazione interna degli acquisti" descritta nel presente documento.** → **Vedasi "Procedura di autorizzazione interna delle forniture" descritta nel presente documento.** → **Processi aziendali: Administration; Operative Financial Management for IT-Billing; Manuale operativo contabilità SAP; Procurement** **Regolamento contratti per l'affidamento di beni e servizi di importo inferiore alle soglie comunitarie**

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
	nello svolgimento dei processi citati va inoltre assicurato che le informazioni generate e comunicate a valle di detti processi siano: → corrette e complete, → supportate da un adeguato livello di documentazione, con archiviazione a storico delle registrazioni principali. Infine deve essere rispettata la regola che vieta che una persona possa, da sola, attivare, gestire, autorizzare e chiudere un processo sensibile.	

Delitti contro la personalità individuale (Art. 25-quinquies del D.Lgs. 231/01)

Reati richiamati dal D.Lgs. 231/01

L'articolo 25-quinquies del Decreto richiama specificatamente i seguenti reati.

- Riduzione o mantenimento in schiavitù o in servitù
- Prostituzione minorile, pornografia minorile, detenzione di materiale pornografico
- Pornografia virtuale
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile
- Tratta di persone, acquisto e alienazione di schiavi
- Intermediazione illecita e sfruttamento del lavoro

Considerata l'attività svolta dalla SIAG si ritiene rilevante esclusivamente il neo-introdotto reato di intermediazione illecita e sfruttamento del lavoro. Il reato consiste

1) nel reclutamento di manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;
2) nell'utilizzo, assunzione o impiego di manodopera, anche mediante l'attività di intermediazione di cui al numero precedente, sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.

Contestualizzazione aziendale e modalità di commissione

Rispetto al reato di intermediazione illecita e sfruttamento del lavoro l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- *Management aziendale*
- *I Responsabili dei reparti RUN e Production in qualità di RUP nel processo di approvvigionamento.*

Per quanto riguarda gli altri reati-presupposto, non si ritiene di poter evidenziare **Soggetti/UU.OO.** come particolarmente **sensibili**.

I processi/sottoprocessi sensibili al rischio sono i seguenti:

- Selezione, negoziazione ed esecuzione di contratti con fornitori, prestatori di servizi ed appaltatori, consulenti
  - Incarichi ad appaltatori e prestatori di servizi con impiego di maestranze

Relativamente alle **modalità di commissione del reato** ed, in particolare, in relazione al reato di *Intermediazione illecita e sfruttamento del lavoro* si può astrattamente ipotizzare la seguente situazione: ricorso alla prestazione di appaltatori e/o prestatori d'opera che nei confronti dei propri lavoratori dipendenti ed impiegati nell'appalto/contratto d'opera violino la normativa in materia di salario minimo, previdenza, assicurazione, salute e sicurezza sul lavoro.

Presidio del rischio attuato dalla Società

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.10.3.1. Principi specifici di comportamento

Rammentato come la condotta delittuosa consista da un lato nell'illecita reclutamento di manodopera per impiegarla presso terzi, in condizioni di sfruttamento, approfittando dello stato di bisogno, e dall'altro lato nell'utilizzo, assunzione o impiego di manodopera reclutata con le suddette modalità, nell'ambito dell'area in esame, la Società si conformerà ai seguenti principi di comportamento:

- improntare la propria condotta ai principi generali contenuti nel Codice Etico, ed ai principi di legalità, correttezza, tracciabilità e trasparenza;
- tutti i soggetti che intrattengano rapporti con fornitori di manodopera e/o subappaltatori devono essere debitamente autorizzati; i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Società devono essere appositamente incaricati;
- selezionare fornitori di manodopera e/o subappaltatori in base alle loro capacità di offerta in termini di qualità, innovazione e costi, che dimostrino standard elevati di condotta etica aziendale, con particolare riferimento al rispetto dei diritti umani, della sicurezza, dell'ambiente, ai principi di legalità, trasparenza e correttezza negli affari;
- valutare con particolare attenzione l'attendibilità dei fornitori/subappaltatori in relazione alla gestione del personale, sia sotto l'aspetto della provenienza della manodopera utilizzata, del rispetto della normativa in materia di corretta retribuzione, regolarità contributiva ed assicurativa, che sotto l'aspetto del rispetto di tutte le prescrizioni in materia di salute e sicurezza sul luogo di lavoro;
- l'intero processo in ogni sua fase deve essere tracciato, sia a livello informatico che documentale, così che le attività svolte siano documentate coerenti e congrue. La funzione responsabile archivierà e conserverà la relativa documentazione in adempimento alla relativa procedura aziendale.

2.10.3.2. Protocolli aziendali e controlli relativi ai processi

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
07 – 01	In ogni caso è fatto esplicito divieto di porre in essere e/o di concorrere a porre in essere comportamenti che possano condurre alla commissione dei reati qui descritti ed in particolare di: • contrattare, utilizzare, impiegare od assumere manodopera da fornitori di manodopera/subappaltatori ad un costo evidentemente inferiore al costo medio del mercato; • contrattare, utilizzare, impiegare od assumere manodopera da fornitori di manodopera/subappaltatori che pongono in essere condotte evidentemente in contrasto con la normativa sulla salute e sicurezza sul luogo di lavoro. In aggiunta a quanto precede, al fine di presidiare l'Area e le Attività Sensibili rispetto alla possibile commissione dei reati in esame, dovranno inoltre essere rispettate le previsioni più specifiche contenute nelle procedure aziendali in essere.	**→ Vedasi "Procedura di autorizzazione interna degli acquisti" descritta nel presente documento.** **→ Processi aziendali: Procurement** **Regolamento contratti per l'affidamento di beni e servizi di importo inferiore alle soglie comunitarie**

Omicidio colposo e lesioni colpose gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (Art. 25-septies del D.Lgs. 231/01)

Reati richiamati dal D.Lgs. 231/01

L'articolo 25-septies del Decreto richiama specificatamente i seguenti reati.

- Omicidio colposo commesso con violazione dell'art. 55, comma 2, del D.Lgs. 81/2008 (*Attuazione dell'articolo 1 della legge 3/8/2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro*)
- Lesioni personali colpose commesso con violazione delle norme in materia di salute e sicurezza sul lavoro.

Esemplificazione delle fattispecie di reato richiamate è la seguente.

Per *colpa* (negligenza, imprudenza o imperizia nell'applicazione delle norme di legge) viene commesso un omicidio colposo o una persona subisce lesioni personali gravi o gravissime.

Contestualizzazione aziendale e modalità di commissione

Con questa tipologia di reato per la prima volta nell'ambito del D.Lgs. 231/01 viene introdotta la responsabilità per reati di natura "*colposa*" (caratterizzati dal fatto che l'evento verificatosi *non era voluto* da colui che ha agito). Ciò pone una questione interpretativa, osservando che in tal caso la "*non volontarietà*" che caratterizza tali reati *colposi* (omicidio o lesioni personali gravi o gravissime) va conciliata con il presupposto della responsabilità dell'Ente, ex D.Lgs. 231/01, ovvero con la condizione che dal fatto illecito derivi un vantaggio per l'Ente. Tale conciliazione si realizza laddove si osservi che la mancata adozione di un adeguato *Sistema di Gestione della Salute e della Sicurezza sul lavoro* potrebbe essere interpretato come un "risparmio" in termini, ad esempio, di costi, da parte dell'Ente.

Rispetto ai reati-presupposto qui richiamati ed in considerazione della tipologia di attività svolte abitualmente in Azienda, l'esposizione al rischio di *Informatica Alto Adige* non è ritenuta di estrema rilevanza *statistica*, soprattutto se confrontata con quella che caratterizza l'insieme delle aziende a cui la

norma di riferimento (il D.Lgs. 81/08 - *Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro*) si applica.

Nondimeno, *Informatica Alto Adige* ha ritenuto di considerare i reati qui trattati come "*reati di particolare rilevanza*" e di sanzionarli con maggior severità nell'ambito del sistema disciplinare descritto nel presente Modello.

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- Datore di Lavoro o persona intestataria di specifica Procura rilasciata dal CdA
- Responsabile del Servizio di Prevenzione e Protezione ("RSPP")
- Soggetto delegato dal Datore di Lavoro ex art. 16, TU 81/2008

Il processo/sottoprocessi sensibili al rischio sono i seguenti:

- Gestione del sistema di salute e sicurezza dei lavoratori..

La **modalità di commissione del reato** che si può ipotizzare è la seguente.

Per *negligenza, imprudenza* o *imperizia*, quindi in assenza della volontà che caratterizza il dolo, ma come conseguenza, casuale e non voluta, del perseguimento di una determinata finalità (quale, ad esempio, il contenimento dei costi), si determina un evento accidentale che porta alla morte di una persona o ne cagiona lesioni gravi o gravissime.

La commissione dei reati qui considerati potrebbe essere resa possibile dall'inosservanza del *Sistema di Gestione della Salute e Sicurezza sul lavoro*. Tale Sistema, recepito nel presente Modello come sua parte integrante, è specificamente volto a scongiurare il verificarsi di un evento accidentale come quello a cui s'è appena fatto riferimento. Esso prevede infatti il rispetto di tutti gli obblighi elencati all'art. 30 del D. Lgs. 81/08.

In particolare l'art. 30 del D.Lgs. 81/2008, rubricato "Modelli di organizzazione e gestione", dispone che il modello organizzativo idoneo ad avere efficacia esimente della responsabilità della Società deve:

1. assicurare 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;

b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione;

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;

e) alle attività di informazione e formazione dei lavoratori;

f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;

h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

2. prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività elencate al precedente punto 1;

3. prevedere, in relazione alla natura, alle dimensioni dell'ente e all'attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio; nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;

4. prevedere un idoneo sistema di controllo sull'attuazione del Modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione

degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

Presidio del rischio attuato dalla Società

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.11.3.1. Principi specifici di comportamento

- In ottemperanza al D.Lgs. 81/08 in tema di *tutela della salute e della sicurezza nei luoghi di lavoro*, la Società integra il presente Modello con un sistema normativo, il *Sistema di Gestione della Salute e Sicurezza sul lavoro* ("SGSS"), che prevede specifici obblighi giuridici, specifici protocolli e procedure. Il Sistema *SGSS* deve prevedere, fra l'altro:
  - l'obbligatorietà della sua osservanza da parte di chiunque operi nella Società (Vertice aziendale e Dipendenti);
  - l'impegno a diffondere la cultura della Sicurezza in tutti gli ambiti della vita aziendale, interni ed esterni, promuovendo anche la creazione di apposite strutture destinate a valutare ed, eventualmente, a sanzionare comportamenti che violino le norme applicabili;
  - l'orientamento verso le azioni preventive tramite il monitoraggio e l'esame periodico delle situazioni di potenziale rischio;
  - l'obiettivo del miglioramento continuo tramite la partecipazione di tutti i dipendenti attraverso la diffusione delle informazioni pertinenti e la circolazione di comunicazioni in tutti i livelli.
  -

- Ogniqualvolta sia previsto che un Fornitore di *Informatica Alto Adige* presti la sua attività presso la sede della Società e/o presso sedi di Clienti, è obbligatorio che vengano puntualmente attuate le prescrizioni previste dall'Art. 26 del D.Lgs. n. 81/2008 (*Obblighi connessi ai contratti d'appalto o d'opera o di somministrazione*), in particolare con riferimento alla gestione dei rischi specifici da interferenza.

- La funzione di Internal Auditing è tenuta a svolgere un controllo di 2° livello rispetto all'adozione ed effettiva attuazione del sistema SGSS e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate.

2.11.3.2. Protocolli aziendali e controlli relativi ai processi

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
08 – 01	Nell'ambito di tali Attività Sensibili, la Società seguirà, inoltre, i seguenti principi: • improntare la propria condotta ai principi generali dettati dal Codice Etico ed ai principi di legalità, correttezza e trasparenza e tracciabilità; • monitorare costantemente la politica per la salute e la sicurezza sul lavoro e, di conseguenza, revisionare prontamente il relativo sistema di gestione al mutare delle condizioni di rischio, predisponendo idonee misure di prevenzione e protezione e assicurando il costante aggiornamento dei presidi elaborati dalla Società alle vigenti disposizioni legislative;	→ **Vedasi *Documenti di riferimento per la Gestione della Salute e Sicurezza sul lavoro***

	• assicurare gli adempimenti in materia di salute e sicurezza dei lavoratori sui luoghi di lavoro, osservando le misure generali di tutela e valutando scrupolosamente il rispetto degli standard tecnico–strutturali relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici; • in caso di coinvolgimento di soggetti terzi nella gestione/prevenzione dei rischi in materia di salute e sicurezza sul lavoro, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al Decreto e di impegno al suo rispetto; • adottare una condotta trasparente e collaborativa nei confronti degli enti preposti al controllo in occasione di ispezioni; • effettuare tutte le necessarie attività di natura organizzativa (quali la gestione delle emergenze, del primo soccorso, delle riunioni periodiche di sicurezza, delle consultazioni dei rappresentanti dei lavoratori per la sicurezza), di sorveglianza sanitaria, di informazione e formazione dei lavoratori, e di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori. In aggiunta a quanto precede, andranno altresì acquisite tutte le documentazioni e certificazioni obbligatorie di legge; • favorire e promuovere la formazione interna relativa ai rischi connessi allo svolgimento delle attività, misure ed attività di prevenzione e protezione adottate, procedure primo soccorso, antincendio ed evacuazione dei lavoratori; • curare il rispetto delle normative in tema di salute e sicurezza nei contratti di appalto ed in caso di associazioni temporanee di imprese e partecipazione a consorzi; • verificare che il Personale osservi le disposizioni di legge, la normativa interna e le istruzioni impartite dai responsabili delle funzioni coinvolte e utilizzi correttamente i macchinari, le apparecchiature, i mezzi di trasporto, i dispositivi di sicurezza e le altre attrezzature di lavoro. In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D.Lgs. 231/2001. In aggiunta a quanto precede, al fine di presidiare l'Area e le Attività Sensibili rispetto alla possibile commissione dei reati in esame, dovranno inoltre essere rispettate le previsioni contenute nelle procedure aziendali in essere, individuate nella matrice rischi/processi. ➢	

Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Art. 25-octies del D.Lgs. 231/01)

Reati richiamati dal D.Lgs. 231/01

L'articolo 25-octies del Decreto richiama specificatamente i seguenti reati.

- Ricettazione
- Riciclaggio
- Impiego di denaro, beni o utilità di provenienza illecita
- Autoriciclaggio (fattispecie di reato introdotta dalla legge 15 dicembre 2014, n. 186)

Alcune considerazioni in tema di autoriciclaggio.

Il reato di autoriciclaggio, di cui all'art. 648–ter.1 c.p., introdotto con la Legge n. 186/2014 punisce chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce in attività economiche, finanziarie, imprenditoriali o speculative il denaro, i beni o le altre utilità

provenienti dalla commissione di tale delitto in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.
La nuova fattispecie di autoriciclaggio è stata inserita tra i reati-presupposto della responsabilità dell'ente ai sensi dell'art. 25 *octies* del D.Lgs. 231/2001 con il chiaro intento del legislatore di neutralizzare gli sviluppi economici del reato compiuto a monte dal reo, evitando che le condotte di riciclaggio o reimpiego dei beni di provenienza illecita possano essere svolte per mezzo o attraverso la copertura di una persona giuridica. Presupposto della responsabilità degli enti è il delitto di autoriciclaggio e non già i delitti non colposi che la norma penale richiama esclusivamente quali fonti di provenienza delle disponibilità economiche di cui si vieta l'autoriciclaggio stesso. L'ente non deve quindi prevenire la commissione del delitto presupposto dell'autoriciclaggio, ma solo la condotta che descrive la fattispecie dell'art. 648-ter.1. c.p.. Fulcro del ragionamento preventivo per la responsabilità dell'ente, allora, attiene non alla prevenzione di qualsiasi reato anche non rientrante nel novero del catalogo, ma nel controllo dei flussi di denaro. L'ente, per non rischiare una responsabilità per autoriciclaggio, deve verificare la provenienza dei flussi di denaro in entrata e la loro destinazione; in mancanza, l'omessa verifica lascia residuare la possibiità che il delitto, in quanto pulizia del denaro sporco, sia perfezionato attraverso il reimpiego di tali flussi di ricchezza di origine illecita. Tesi abbracciata da Cass.pen., sez.II, 04.05.2018, n.25979; Cass.pen., sez.II, 21.06.2019, n.37503

Il presente Modello Organizzativo, al fine di risultare capace di prevenire il rischio di commissione del reato di autoriciclaggio, prevede i seguenti presidi:

- presidi volti ad evitare che siano impiegati in attività imprenditoriali, economiche o finanziarie della Società, proventi illeciti derivanti da qualsiasi delitto non colposo (anche se non previsto come reato–presupposto della responsabilità dell'ente).

Tali presidi predisposti ad hoc andranno ad aggiungersi, nel caso in cui il reato–base sia, altresì, previsto come reato–presupposto della responsabilità dell'ente, alle cautele già adottate per la prevenzione del reato fonte.
Premesse tali considerazioni, si elencano le seguenti esemplificazioni delle fattispecie di reato richiamate dall'art. 25-octies del D.Lgs. 231/01.

- Si acquista, si riceve o si occulta denaro o cose di provenienza illecita
- Si sostituiscono o si trasferiscono denaro, beni o altre utilità di provenienza illecita, ovvero si compiono, in relazione ad essi, altre operazioni in modo da ostacolare l'identificazione della loro illecita provenienza
- Si impiegano, in attività economiche o finanziarie, denaro, beni o altre utilità di illecita provenienza
- Avendo commesso o concorso a commettere un *delitto non colposo*, si impiega, si sostituisce, si trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Con riferimento all'ultimo punto citato (*autoriciclaggio*), come già anticipato, l'analisi dei rischi svolta in SIAG ha portato ad identificare come *delitto non colposo* "più probabile" il reato-base di *evasione delle imposte*. Alla luce delle norme civilistiche che SIAG è tenuta a rispettare, considerato lo Statuto di SIAG ed anche la natura pubblica della sua *Proprietà*, risulta particolarmente modesto il rischio di commissione delle citate fattispecie di *reato-base*, così come particolarmente esiguo sarebbe il vantaggio di cui SIAG potrebbe beneficiare.

Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- Management aziendale
- Responsabili di reparto

In particolare, in relazione all'ipotesi di commissione del *reato-base* (per l'autoriciclaggio) di evasione delle imposte:

- Responsabile della Funzione Finance e suoi Collaboratori (Dipendenti o Professionisti esterni) coinvolti nel processo di gestione delle imposte.

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Flussi finanziari
    - Gestione cassa/pagamenti in contanti
- Predisposizione e sottoscrizione delle dichiarazioni fiscali

- Gestione della contabilità fiscale
  - Gestione delle imposte dirette (IRES, IRAP ecc.), dal loro calcolo al pagamento
  - Gestione delle imposte indirette (IVA ecc.) dal loro calcolo al pagamento
  - Gestione delle imposte locali (IMI, TASI, ecc.), dal loro calcolo al pagamento
  - Gestione delle attività di sostituto d'imposta.
- Investimenti mediante operazioni straordinarie

La **modalità di commissione del reato** che si può astrattamente ipotizzare è la seguente.
Con riferimento a denaro, beni o altre utilità di provenienza illecita:
- si compiono operazioni di acquisto, ricezione od occultamento;
- si impiegano tali beni in operazioni di tipo economico/finanziario;
- si impiegano tali beni in operazioni di tipo economico/finanziario in modo da ostacolare concretamente l'identificazione della loro illecita provenienza.

In particolare, in relazione all'ipotesi di commissione del *reato-base* (per l'autoriciclaggio) di evasione delle imposte:
- nello svolgimento del processo di gestione delle varie tipologie di imposta, dalla dichiarazione di un reddito o di un bene *imponibile*, al calcolo della relativa imposta, fino al regolare pagamento della stessa, ricorrendo ad artifici o simulazioni, si pone in atto un comportamento che genera, a beneficio della Società, una *provvista illecita*.

Presidio del rischio attuato dalla Società

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.12.3.1. Principi specifici di comportamento

- Allo scopo di avere totale garanzia che nell'ambito di una fornitura a favore di qualunque Cliente, sia chiara la volontà della Società di rifuggire da qualsiasi comportamento di carattere corruttivo o, comunque, illecito (ancorché condotto nell'interesse o a vantaggio della Società), i Soggetti aziendali obbligatoriamente tenuti ad autorizzare la fornitura, anche con riferimento ad aspetti legati a fasi del "ciclo passivo" (quali, ad esempio, acquisizioni esterne finalizzate all'erogazione della fornitura) sono tenuti a sottoscrivere una dichiarazione con la quale si attesta:
  - che, sulla base delle informazioni a loro disposizione e fino alla data di sottoscrizione della dichiarazione in questione, in nessuna fase della trattativa commerciale o della formalizzazione contrattuale si sono verificati episodi che, anche ipoteticamente, appaiano riconducibili o comunque diretti ad atti RILEVANTI ai sensi del D.Lgs. 231/01;
  - l'impegno a comunicare immediatamente all'Organismo di Vigilanza ex D.Lgs. 231/01 eventuali tentativi, episodi o atti anche ipoteticamente inquadrabili fra gli illeciti sopra menzionati, laddove gli stessi si verificassero successivamente alla sottoscrizione della dichiarazione in questione, fino al completo espletamento della fornitura.

- Allo scopo di ridurre al minimo il rischio di compimento dei reati qui considerati, con particolare riferimento al reato di autoriciclaggio, la Società:
  • condanna qualunque comportamento volto ad impiegare in proprie attività economiche, finanziarie, imprenditoriali o speculative denaro, beni o altre utilità di provenienza delittuosa;
  • vigila affinché coloro i quali operano nelle aree giudicate a rischio reato rispettino le leggi, regolamenti e le procedure di comportamento stabiliti in materia di gestione delle risorse finanziarie, azionarie e immobiliari, volti ad impedire ogni possibile utilizzo economico di proventi delittuosi;
  • prevede obblighi di segnalazione in ordine ad operazioni "atipiche" di impiego in attività economiche, finanziarie, imprenditoriali e speculative della società.
  Rappresentano indici di atipicità di un'operazione che la rendono meritevole di essere oggetto di specifica valutazione al fine di garantire la legittimità rispetto alle finalità di prevenzione del rischio antiriciclaggio:
  1) l'estraneità o incoerenza con l'oggetto sociale, con l'attività o con il profilo economico – patrimoniale della Società;

2) l'assenza di adeguata giustificazione, sotto il profilo della normale attività gestionale e sociale, avuto riguardo alla straordinarietà dell'importo o alle inusuali modalità di realizzazione;
3) la presenza di controparti commerciali operanti in Paesi con regime antiriciclaggio non equivalente a quello dei Paesi della Comunità Europea.
In presenza di uno o più indici di atipicità sono previste le seguenti modalità di segnalazione:
a) in caso di operazioni rientranti nei limiti dei poteri di firma e di spesa di un singolo Responsabile, questi ne informa prontamente il Presidente del CdA e l'OdV per le verifiche necessarie;
b) se l'operazione atipica è di competenza del CdA, quest'ultimo trasmette, agli stessi fini, all'OdV l'ordine del giorno o la relativa delibera.
Le predette segnalazioni devono essere formalizzate in apposite schede di evidenza.

- La Società provvede a far sì che risulti sempre adeguata la formazione/competenza dei Soggetti responsabili di operazioni economiche, finanziarie, imprenditoriali o speculative, in relazione alla loro capacità di individuare, in tali operazioni, eventuali elementi di atipicità.

- Relativamente al processo di gestione, mediante applicativo software, dei dati anagrafici dei Fornitori, dati che comprendono, fra gli altri, le coordinate bancarie degli stessi, in SIAG le credenziali che abilitano alle funzioni SW di inserimento e modifica delle coordinate bancarie vengono rilasciate ad un massimo di due Dipendenti.

In particolare, in relazione all'ipotesi di commissione del *reato-base* (per l'autoriciclaggio) di evasione delle imposte:
- Chiunque, in SIAG, Dipendenti ed eventuali Professionisti esterni, sono tenuti alla più rigorosa applicazione delle norme di legge in tema di normativa fiscale e nel rispetto della norme sulla tracciabilità.

- Un Professionista esterno eventualmente coinvolto in una o più fasi della gestione delle imposte, deve essere selezionato sulla base di dimostrabili requisiti di professionalità e competenza. Il contratto con cui viene acquisita la sua prestazione deve contenere specifiche clausole sanzionatorie nel caso di mancato rispetto della normativa fiscale applicabile e, in generale, nel caso di commissione (o di concorso alla commissione) di un reato di cui al D. Lgs. 231/2001.

2.12.3.2. 2.12.3.2. Protocolli aziendali e controlli relativi ai processi

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
09 – 01	Allo scopo di ridurre al minimo il rischio di commissione dei reati qui considerati, è obbligatorio rispettare col massimo rigore tutte le norme aziendali applicabili ai processi sensibili rientranti nei processi di seguito elencati: → Gestione Anagrafica Fornitori: censimento nuovi Fornitori/modifica dati anagrafici e riferimenti bancari; → Gestione Ciclo passivo: autorizzazione alla spesa, analisi e sottoscrizione contratto, gestione fatturazione passiva e mandati di pagamento; → Gestione Ciclo attivo: verifica e autorizzazione preventivi costi-ricavi, analisi e sottoscrizione contratto, gestione fatturazione attiva. Deve essere rispettata la regola che vieta che una persona possa, da sola, attivare, gestire, autorizzare e chiudere un processo sensibile. In particolare, i processi autorizzativi dei contratti, sia d'acquisto che di vendita, debbono obbligatoriamente coinvolgere, formalmente, almeno due diversi Responsabili. Entrambi i tipi di contratto devono essere firmati da chi è dotato di apposita specifica Procura. Infine vanno assicurati, nello svolgimento dei processi citati, la trasparenza ed un adeguato livello di documentazione.	**→ Vedasi "Procedura di autorizzazione interna degli acquisti" descritta nel presente documento.** **→ Vedasi "Procedura di autorizzazione interna delle forniture" descritta nel presente documento.** **→ Procedure aziendali: Administration Operative Financial Management for IT-Billing; Manuale operativo contabilità SAP;**
09 – 02	Allo scopo di ridurre al minimo il rischio di commissione del reato il processo di gestione delle imposte, dal calcolo al pagamento delle stesse, coinvolge almeno due diversi Soggetti (Dipendenti o	**→ Procedure aziendali: Administration Operative Financial**

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
	Professionisti esterni) e risulta tracciabile, con evidenze disponibili su supporto cartaceo o elettronico.	**Management for IT-Billing; Manuale operativo contabilità SAP;**
09-03	Con riguardo all'impiego dei proventi illeciti endogeni o esogeni, allo scopo di ridurre al minimo il rischio d condotte orientare ad ostacolare concretamente l'identificazione della provenienza delittuosa, la società si conformerà ai seguenti principi di comportamento: • tutti i soggetti che prendono decisioni in materia di investimenti devono essere debitamente autorizzati sulla base del sistema dei poteri e delle deleghe in essere; i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Società devono essere appositamente incaricati; • garantire la segregazione dei poteri nell'ambito del processo prevedendo il coinvolgimento di una pluralità di attori, con responsabilità di gestione, verifica ovvero approvazione. In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del Decreto, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di: • concorrere o commettere reati finalizzati alla maturazione di proventi illeciti endogeni o esogeni; • porre in essere comportamenti finalizzati ad ostacolare concretamente l'identificazione della provenienza delittuosa della provvista.	

Delitti in materia di violazione del diritto d'autore (Art. 25-novies del D.Lgs. 231/01)

Reati richiamati dal D.Lgs. 231/01

L'articolo 25-novies del Decreto richiama specificatamente i seguenti reati.

A) Messa a disposizione del pubblico, in un sistema di reti telematiche,... di un'opera dell'ingegno protetta, o di parte di essa
B) Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione o con usurpazione della paternità dell'opera...
C) Abusiva duplicazione, per trarne profitto,... di programmi per elaboratore o, allo stesso scopo: importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale... di qualsiasi mezzo atto a rimuovere o a facilitare la rimozione... di dispositivi di protezione di un programma per elaboratore... o anche: ... riproduzione, trasferimento..., distribuzione, ... presentazione in pubblico..., vendita o concessione in locazione del contenuto di una banca dati
D) Abusiva riproduzione, trasmissione o diffusione in pubblico, con qualsiasi procedimento,... di opere o parti di opera letterarie... ovvero multimediali... o banche dati...
E) Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione
F) Fraudolenta produzione, vendita,... installazione... di apparati... atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato...La descrizione già fornita dei vari reati richiamati ci sembra sufficientemente esemplificativa delle varie fattispecie di reato.

La descrizione già fornita dei vari reati richiamati sembra sufficientemente esemplificativa delle varie fattispecie di reato.

Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- Management aziendale
- Reparti coinvolti nell'erogazione di una fornitura al Cliente
- Service Area Manager

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Acquisto, gestione e sviluppo di programmi e software
- Gestione sit SIAG e siti della PAB e di SABES

Modalità di commissione del reato.

Relativamente ai reati precedentemente elencati, di cui alle lettere E) ed F): il compimento di tali fattispecie di reato non sono neppure astrattamente ipotizzabili in Azienda.

Per quanto riguarda almeno una delle fattispecie di reato elencate dalla lettera A) alla D) comprese, si può astrattamente ipotizzare che in Azienda si verifichino una o entrambe le seguenti situazioni:

- si ha la disponibilità di un'opera dell'ingegno di Terzi quali, a titolo esemplificativo: un programma per elaboratore, una banca dati, una soluzione tecnologica, un documento o un'opera multimediale;
- con riferimento ai diritti d'autore eventualmente connessi alle opere dell'ingegno sopra citate, si detengono mezzi intesi unicamente alla rimozione funzionale di dispositivi posti a protezione di tali diritti;
- si pubblicano opere (fotografie, videoregistrazioni) di Terzi sui propri siti web o siti web in gestione da Terzi senza indicazione del titolare dell'opera e/o senza relativa autorizzazione da parte del titolare dell'opera.

In tali circostanze, allo scopo di trarne profitto ed eventualmente previa rimozione dei dispositivi di protezione originariamente predisposti, l'Azienda potrebbe (con riferimento alle citate opere dell'ingegno):

- mettere a disposizione, su reti telematiche, un'opera dell'ingegno protetta (o parte di essa), con usurpazione della paternità dell'opera,

  ovvero potrebbe
- abusivamente duplicare, riprodurre, trasferire, distribuire, diffondere in pubblico, vendere o dare in locazione un'opera dell'ingegno.

Presidio del rischio attuato dalla Società

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.13.3.1. Principi specifici di comportamento

Si rimanda ai "*Principi generali di comportamento*" indicati nel paragrafo 2.2.

Inoltre, la Società conformerà le proprie azioni ai seguenti, ulteriori, principi:

- improntare la propria condotta ai principi generali contenuti nel Codice Etico ed ai principi di legalità, correttezza, tracciabilità e trasparenza;
- provvedere affinché l'utilizzo di software, banche dati, immagini altrui e di qualsiasi opera intellettuale o protetta da privativa industriale avvenga nel rispetto dei diritti d'autore e dei diritti di proprietà industriale (licenze d'uso, autorizzazioni, etc.).

- evitare comportamenti idonei a ledere gli altrui diritti di proprietà industriale ed intellettuale;
- qualora venisse previsto per l'espletamento dell'attività il coinvolgimento di collaboratori o consulenti esterni questo dovrà essere formalizzato per iscritto ed il relativo contratto dovrà contenere apposita dichiarazione di conoscenza della normativa di cui al Decreto nonché condivisione dei principi di cui al Codice Etico. Il relativo contratto dovrà essere stipulato in conformità ai principi ed alle procedure aziendali in tema di conferimento di incarichi esterni. Non è consentito riconoscere compensi in favore di tali collaboratori o consulenti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto. Il corrispettivo deve essere congruo ed il servizio reso documentato o documentabile;
- l'intero processo in ogni sua fase deve essere tracciato, sia a livello informatico che documentale, così che le attività svolte siano documentate coerenti e congrue. La funzione responsabile archivierà e conserverà la relativa documentazione in adempimento alla relativa procedura aziendale.

2.13.3.2. Protocolli aziendali e controlli relativi ai processi

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
10 – 01	Sono espressamente vietati, in quanto lesivi del diritto d'autore, i seguenti comportamenti: - la ricezione, la diffusione o l'uso di software qualora tali operazioni risultino in contrasto con la dichiarata volontà del legittimo proprietario; - la detenzione o l'uso di software finalizzato a eludere o a forzare i sistemi di protezione dalla copia del software; - qualsiasi operazione finalizzata a compromettere l'integrità dei dati, la funzionalità o le prestazioni di sistemi informatici; - qualsiasi operazione finalizzata a eludere o forzare sistemi di controllo o sistemi informatici; - qualsiasi altro utilizzo vietato dalla legislazione vigente.	→ **Processi aziendali: Workplace Policy; Information Security Management; Procurement;** **Regolamento contratti per l'affidamento di beni e serivizi di importo inferiore alle soglie comunitarie;**
10 – 02	A) Il Dipendente non può installare di sua iniziativa sulla postazione di lavoro software non autorizzato senza prima interpellare il reparto "Run". B) A fronte di specifiche esigenze, l'Azienda può effettuare lo scan da remoto dei dischi fissi dei PC dei Collaboratori, al fine di rilevare i file eseguibili presenti, i software installati e le licenze utilizzate.	→ **Processi aziendali: Workplace Policy; Information Security Management; Procurement;** **Regolamento contratti per l'affidamento di beni e serivizi di importo inferiore alle soglie comunitarie**
10 – 03	Con specifico riferimento alla vendita abusiva di un'opera dell'ingegno sulla quale un soggetto terzo vanta un legittimo diritto d'autore, devono risultare regolarmente documentati ed autorizzati: - la Richiesta d'Acquisto relativa alla prescritta licenza d'uso - l'*Autorizzazione Preventivo commessa* nella quale figura una specifica voce di costo inerente la licenza. Per entrambi i documenti il processo di autorizzazione deve vedere coinvolti almeno due Responsabili.	→ **Vedasi "Procedura di autorizzazione interna degli acquisti" descritta nel presente documento.** → **Vedasi "Procedura di autorizzazione interna delle forniture" descritta nel presente documento.** → **Processi aziendali: Workplace Policy; Information Security Management; Procurement;** **Regolamento contratti per l'affidamento di beni e serivizi di importo inferiore alle soglie comunitarie**

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25-decies del D.Lgs. 231/01)

Reati richiamati dal D.Lgs. 231/01

L'articolo 25-decies del Decreto richiama specificatamente il seguente reato: *Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria*.

Una semplice esemplificazione della fattispecie di reato è la seguente: con violenza, minaccia, offerta o promessa di denaro o altra utilità si induce una persona a non rendere dichiarazioni all'autorità giudiziaria o a rendere dichiarazioni mendaci.

Contestualizzazione aziendale e modalità di commissione

Rispetto al reato-presupposto qui richiamato, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO**. **sensibili**:

- I Presidente del CdA ed il Direttore, nella loro qualità di rappresentanti legali della Società
- Il Management aziendale.

I processi/sottoprocessi sensibili al rischio sono i seguenti:

- Gestione di contenzioso giudiziale e stragiudiziale

Modalità di commissione del reato: nella previsione di procurare all'Azienda un illecito vantaggio, con minacce o promesse si induce una persona chiamata a rendere dichiarazioni davanti all'Autorità Giudiziaria a non renderle o a rendere dichiarazioni mendaci.

Presidio del rischio attuato dalla Società

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.14.3.1. Principi specifici di comportamento

Si rimanda ai "*Principi generali di comportamento"* indicati nel paragrafo 2.2.

Più in dettaglio è indispensabile:

- che tutte le attività e le operazioni svolte per conto della Società siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza e trasparenza;
- che si eviti qualsiasi comportamento che abbia lo scopo o l'effetto di indurre un soggetto terzo a rilasciare false dichiarazioni nell'ambito di un processo penale;
- che sia mantenuto un contegno chiaro, trasparente, diligente e collaborativo con le Pubbliche Autorità, con particolare riguardo alle Autorità Giudicanti ed Inquirenti, mediante la comunicazione di tutte le informazioni, i dati e le notizie eventualmente richieste;
- qualora venisse previsto per l'espletamento dell'attività il coinvolgimento di collaboratori o consulenti esterni, che l'incarico sia formalizzato per iscritto e contenga apposita dichiarazione di conoscenza della normativa di cui al Decreto, nonché condivisione dei principi di cui al Codice Etico. Il relativo contratto dovrà essere stipulato in conformità ai principi ed alle procedure aziendali in tema di conferimento di incarichi esterni. Non è consentito riconoscere compensi in favore di tali collaboratori o consulenti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto. Il corrispettivo deve essere congruo ed il servizio reso documentato o documentabile;

- che l'intero processo in ogni sua fase sia tracciato, sia a livello informatico che documentale, così che le attività svolte siano documentate coerenti e congrue. La funzione responsabile archivierà e conserverà la relativa documentazione in adempimento alla relativa procedura aziendale;
- che verrà predisposta informativa all'Organismo di Vigilanza nel caso in cui la Società sia coinvolta in un procedimento ai sensi del D.Lgs. 231/01 con indicazione del legale esterno incaricato.

In ogni caso è assolutamente vietato, per chiunque operi in nome o per conto della Società, porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da configurare il compimento di questo reato.

Reati ambientali (Art. 25-undecies del D.Lgs. 231/01)

Reati richiamati dal D.Lgs. 231/01

L'articolo 25-undecies del Decreto richiama specificatamente i "Reati ambientali". Più precisamente, prevede una serie di sanzioni pecuniarie applicabili ad un Ente a fronte della commissione di una lunga serie di reati. Di seguito si riporta un elenco, *non esaustivo*, dei reati referenziati:

- art. 452–bis del Codice Penale: inquinamento ambientale;
- art. 452–quater del Codice Penale: disastro ambientale;
- art. 452–quinquies del Codice Penale: disastro ambientale commesso con colpa;
- art. 452–octies del Codice Penale: associazione per delinquere e di stampo mafioso finalizzata a commettere uno qualsiasi dei delitti previsti nel nuovo Titolo VI–bis del Codice Penale;
- art. 452–sexies del Codice Penale: traffico e abbandono di materiale ad alta radioattività;
- art. 727-bis del Codice Penale: uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette;
- art. 733-bis del Codice Penale: distruzione o deterioramento di habitat all'interno di un sito protetto.

- Con riferimento al D.Lgs 152/06:
  - art. 137: scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili;
  - art. 256: attività di gestione di rifiuti non autorizzata;
  - art. 257: inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee;
  - art. 258: violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari;
  - art. 259: traffico illecito di rifiuti;
  - art. 260: attività organizzate per il traffico illecito di rifiuti;
  - ;
  - art. 279, comma 5: emissioni in atmosfera.
- Reati previsti o richiamati dagli artt. 1 commi 1 e 2, 2 commi 1 e 2, 3-bis comma 1 e 6 comma 4 della L. 150/92: importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette.
- Con riferimento alla L. n. 549/93, art. 3, comma 6: impiego di sostanze lesive dell'ozono stratosferico e dell'ambiente.
- Con riferimento al D.Lgs 202/07:
  - art. 8, commi 1 e 2: inquinamento doloso provocato dalle navi;
  - art. 9, commi 1 e 2: inquinamento colposo provocato dalle navi.

In estrema sintesi, le varie tipologie di reato potrebbero essere così descritte: omettendo di applicare le prescritte norme di legge, vengono smaltite componenti hardware non più utilizzabili o rifiuti pericolosi quali, ad esempio, quelli risultanti dall'attività di manutenzione di apparati quali stampanti.

Contestualizzazione aziendale e modalità di commissione

Rispetto ai numerosi reato-presupposto qui richiamati, l'esposizione al rischio della Società appare circoscritto allo smaltimento dei rifiuti industriali prevalentemente costituiti da apparecchiature (o parti di apparecchiature) hardware giunte al termine del loro ciclo di vita o esaurite (es.: schermi video, apparecchiature fax, cartucce toner, ecc.)

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- Management aziendale
- Responsabili di settore, in particolare del settore "Run"

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Gestione del sistema ambientale
    - Smaltimento, con varie modalità, dei rifiuti prodotti.
    - Gestione Ciclo passivo: analisi e sottoscrizione contratto, in particolare, dei contratti di manutenzione:
        - della sede di SIAG (es.: impresa di pulizia, revisione struttura e/o impiantistica nello stabile, ecc.)
        - delle apparecchiature elettriche ed elettroniche (stampanti, PC, trasformatori, modem, cavi, ecc.).

Modalità di commissione del reato: allo scopo di evitare i costi correlati, la Società, nell'attività di smaltimento dei rifiuti, omette di rispettare puntualmente le norme di legge cui sono collegate le sanzioni previste dall'art. 25-undecies qui considerato.

In particolare, a titolo esemplificativo:

nella predisposizione di un certificato di analisi di rifiuti, si forniscono false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti (Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari, vedasi art. 258, comma 4 del D.Lgs. 152/2006).2.15.3. Presidio del rischio attuato dalla Società

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.15.2.1. Principi specifici di comportamento

Si rimanda ai "*Principi generali di comportamento"* indicati nel paragrafo 2.2.

La Società rispetta, in maniera dinamica e costante, tutti gli obblighi di legge in materia di tutela dell'ambiente conformandosi, da ultimo, alle previsioni contenute nel D.lgs. 152/2006.

In conformità ai principi affermati nel proprio Codice Etico, nella scelta dei fornitori, appaltatori, partner commerciali e collaboratori esterni, la Società pone particolare attenzione agli standard di tutela dell'ambiente.

La Società esige dai propri fornitori, appaltatori, partner commerciali e collaboratori esterni il puntuale rispetto delle prescrizioni in materia di tutela dell'ambiente, in particolare di cui al D.Lgs. 152/2006.

La Società stessa, nonché i propri fornitori, appaltatori, partner commerciali e collaboratori esterni dovranno implementare procedure idonee a prevenire i reati ambientali.

Nell'ambito delle attività a potenziale impatto ambientale la Società conformerà le proprie azioni ai seguenti principi:

- improntare la propria condotta ai principi generali contenuti nel Codice Etico ed ai principi di legalità, correttezza, tracciabilità e trasparenza;

- tutti i soggetti che intrattengano rapporti con la PA per la gestione dello smaltimento dei rifiuti devono essere debitamente autorizzati; i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Società devono essere appositamente incaricati;
- i rapporti e gli adempimenti nei confronti della PA devono essere effettuati con la massima trasparenza, diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere;
- nella selezione di fornitori, appaltatori, partner commerciali e collaboratori esterni verrà verificata attentamente la performance in materia di tutela dell'ambiente, scegliendo tra gli offerenti quelli che garantiscono i più elevati standard qualità;
- i fornitori di servizi ambientali verranno verificati in relazione all'possesso mantenimento delle necessarie autorizzazioni e/o certificazioni;
- qualora venisse previsto per l'espletamento dell'attività il coinvolgimento di collaboratori o consulenti esterni questo dovrà essere formalizzato per iscritto ed il relativo contratto dovrà contenere apposita dichiarazione di conoscenza della normativa di cui al Decreto nonché condivisione dei principi di cui al Codice Etico. Il relativo contratto dovrà essere stipulato in conformità ai principi ed alle procedure aziendali in tema di conferimento di incarichi esterni. Non è consentito riconoscere compensi in favore di tali collaboratori o consulenti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto. Il corrispettivo deve essere congruo ed il servizio reso documentato o documentabile;
- l'intero processo in ogni sua fase deve essere tracciato, sia a livello informatico che documentale, così che le attività svolte siano documentate coerenti e congrue. La funzione responsabile archivierà e conserverà la relativa documentazione in adempimento alla relativa procedura aziendale.

2.15.2.2. Protocolli aziendali e controlli relativi ai processi

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
11 – 01	In SIAG per lo smaltimento delle varie tipologie di rifiuti, vanno applicate le norme di seguito riportate: ➢ frazioni oggetto di raccolta differenziata (carta e cartone, vetro, plastica, tubi fluorescenti, ecc.): previa raccolta differenziata, ci si rivolgerà a servizi (di norma pubblici) autorizzati a tale tipo di raccolta; ➢ rifiuti della produzione, formulazione, fornitura ed uso di inchiostri per stampa (toner esauriti, ecc.): in tutti i contratti relativi ai servizi di manutenzione delle stampanti (e analoghi apparati) è necessario che sia espressamente previsto che è a carico del Fornitore la rimozione delle componenti equiparabili a rifiuti (vedasi D.Lgs. 152/06, art. 266, comma 4); ➢ Rifiuti (RAEE) provenienti da Apparecchiature Elettriche ed Elettroniche (PC, trasformatori, modem, cavi, ecc.): SIAG è tenuta a gestire la raccolta e lo smaltimento del citato materiale, una volta che sia stato catalogato come "rifiuto", nel rispetto delle leggi vigenti in materia (vedasi artt. n. 188, 188-BIS, 188-TER del D.Lgs. 152/06); ➢ in SIAG, con riferimento ai rifiuti RAEE, vanno puntualmente rispettate le norme inerenti la gestione dei registri di carico e scarico (vedasi artt. n. 190 e 193 del D.Lgs. 152/06).	→ **Vedasi "Procedura di autorizzazione interna degli acquisti" descritta nel presente documento.**

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
11 – 02	In ogni caso è fatto esplicito divieto di porre in essere e/o di concorrere a porre in essere comportamenti che possano condurre alla commissione dei reati qui descritti. Così in particolare, a titolo meramente esemplificativo e non esaustivo, è fatto divieto di: • porre in essere attività fonte di danno ambientale • predisporre e inviare, così come accettare documenti consapevolmente incompleti e/o comunicare dati falsi o alterati; • tenere una condotta ingannevole che possa indurre la PA in errore; • affidare incarichi a terzi, prestatori di servizi o consulenti esterni eludendo i criteri di cui alle policies e procedure aziendali.	→ **Vedasi "Procedura di autorizzazione interna degli acquisti" descritta nel presente documento.**

Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies del D.Lgs. 231/01 e aggiornato come da L. 17 ottobre 2017, n. 161)2.16.1. Reati richiamati dal D.Lgs. 231/01

L'articolo 25-duodecies del Decreto contestualizza nel seguente modo il reato qui considerato:

un Datore di lavoro occupa alle proprie dipendenze lavoratori stranieri (extraeuropei):

- privi del permesso di soggiorno
- il cui permesso è scaduto e del quale non sia stato chiesto il rinnovo nei termini di legge
- il cui permesso è revocato o annullato

ed, in qualunque dei tre casi citati, si verifica una delle seguenti situazioni:

- i lavoratori occupati sono in numero superiore a tre;
- i lavoratori occupati sono minori in età non lavorativa;
- i lavoratori occupati sono sottoposti a condizioni di particolare sfruttamento di cui al 3° comma dell'art. 603-BIS del codice penale (*violazioni della normativa in materia di sicurezza e igiene nei luoghi di lavoro, tale da esporre il lavoratore a pericolo per la salute, la sicurezza o l'incolumità personale*).

La descrizione già fornita delle casistiche che configurano il reato in questione appare già sufficientemente esemplificativa.

.

Contestualizzazione aziendale e modalità di commissione

Rispetto ai reati-presupposto qui richiamati, l'esposizione al rischio della Società riguarda i seguenti **Soggetti/UU.OO. sensibili**:

- Direttore Generale
- Responsabile del reparto Human Resources

I **processi/sottoprocessi sensibili** al rischio sono i seguenti.

- Selezione ed assunzione di personale
  - Gestione, nel tempo, del rapporto di collaborazione con un Dipendente o con un Lavoratore autonomo
  - Acquisizione di una prestazione di lavoro autonomo.

Modalità di commissione del reato: allo scopo di conseguire un vantaggio economico (quale potrebbe essere, ad esempio, il riconoscimento di un compenso inferiore a quello di mercato, a parità di competenze), la Società impiega personale extracomunitario non in regola con le norme previste per il soggiorno sul territorio nazionale.

Presidio del rischio attuato dalla Società

Di seguito: princìpi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.16.2.1. Principi specifici di comportamento

Si rimanda ai "*Principi generali di comportamento"* indicati nel paragrafo 2.2.

- Nell'ambito del processo di acquisizione di una prestazione da parte di un Lavoratore autonomo, qualora si tratti di una persona extracomunitaria, è obbligatorio acquisire, prima del perfezionamento del rapporto contrattuale di collaborazione, copia del regolare e valido Permesso di soggiorno rilasciato al Lavoratore dalle Autorità competenti. Sempre prima del perfezionamento del rapporto contrattuale di collaborazione, è obbligatorio acquisire dal Lavoratore una sua dichiarazione sottoscritta con la quale egli si impegna:
  - a comunicare tempestivamente alla Società qualsiasi variazione di stato del Permesso di soggiorno (scadenza, rinnovo, sospensione o revoca);
  - in caso di rinnovo, a trasmettere copia del nuovo Permesso a lui rilasciato.
- Nell'ambito del processo di selezione/assunzione di personale, sia che si tratti di un candidato ad una posizione di "stage", sia che si tratti di una persona candidata all'instaurazione di un rapporto di lavoro subordinato o para-subordinato, qualora si tratti di un Candidato extracomunitario, è obbligatorio acquisire, prima del perfezionamento del rapporto contrattuale di collaborazione, copia del regolare e valido Permesso di soggiorno rilasciato al Candidato dalle Autorità competenti. Sempre prima del perfezionamento del rapporto contrattuale di collaborazione, è obbligatorio acquisire dal Candidato una sua dichiarazione sottoscritta con la quale egli si impegna:
  - a comunicare tempestivamente alla Società qualsiasi variazione di stato del Permesso di soggiorno (scadenza, rinnovo, sospensione o revoca)
  - in caso di rinnovo, a trasmettere copia del nuovo Permesso a lui rilasciato. Per tutta la durata del contratto, la Funzione aziendale competente verifica il perdurare della validità del permesso ed all'approssimarsi della data di scadenza dello stesso – nel caso in cui il rapporto contrattuale fosse ancora in essere – avverte il Collaboratore della necessità di rinnovo.

Reati tributari (Art. 25 quinquiesdecies del D.Lgs. 231/01)

Reati richiamati dal D.Lgs. 231/01

L'articolo 25-quinquiesdecies del Decreto richiama specificatamente i seguenti reati.

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti
- Dichiarazione fraudolenta mediante altri artifici
- Dichiarazione infedele – sistemi transfrontalieri ed evasione di IVA oltre Euro 10 mio
- Omessa dichiarazione – sistemi transfrontalieri ed evasione di IVA oltre Euro 10 mio
- Emissione di fatture o altri documenti per operazioni inesistenti
- Occultamento o distruzione di documenti contabili
- Indebita compensazione – sistemi transfrontalieri ed evasione di IVA oltre Euro 10 mio
- Sottrazione al pagamento di imposte

Esemplificazioni delle fattispecie di reato richiamate sono le seguenti.

Il reato di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

Il reato di dichiarazione fraudolenta mediante altri artifici sanziona la presentazione di dichiarazione inveritiera supportata da un impianto contabile atto a sviare ovvero ostacolare la successiva attività di accertamento dell'amministrazione finanziaria ovvero, comunque, ad avvalorare artificiosamente i dati in essa racchiusi.

La condotta della fattispecie di reato emissione di fatture o altri documenti per operazioni inesistenti consiste nell'emettere o rilasciare fatture o altri documenti per operazioni inesistenti e, quindi, in buona sostanza nella cessione a terzi di documenti fiscali ideologicamente falsi.

Il reato di occultamento o distruzione di documenti contabili incrimina chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui e' obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

Il reato di sottrazione fraudolenta al pagamento di imposte incrimina

- chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva
- chiunque, al fine di ottenere per se' o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila.

Contestualizzazione aziendale e modalità di commissione

Soggetti/ UU.OO. sensibili:

Il Direttore generale

Il Management aziendale

Il Responsabile della funzione Finance

I processi/sottoprocessi senisibili al rischio sono i seguenti:

- Selezione, negoziazione ed esecuzione di contratti con fornitori, prestatori di servizi ed appaltatori, consulenti
  - Stesura autorizzazione e sottoscrizione di contratti
  - Gestione fatturazione passiva
  - Gestione dati anagrafici dei fornitori
  - Gestione subappalti: contrattualizzazione, in particolare in relazione agli obblighi sulla tracciabilità dei flussi finanziari
- Flussi finanziari
  - Gestione cassa/pagamenti in contanti
- Predisposizione e sottoscrizione delle dichiarazioni fiscali
- Gestione della contabilità fiscale
  - Gestione delle imposte dirette (IRES; IRAP, ecc.)
  - Gestione delle imposte indirette (IVA)
  - Gestione delle imposte locali (IMU, TASI, ecc.)
  - Gestione delle attività di sostituto d'imposta

Modalità di commissione del reato.

A titolo esemplificativo, si può astrattamente ipotizzare la seguente situazione.

La società "gonfia" i propri costi al fine di abbattere il più possibile l'imponibile, utilizzando fatture o documenti relativi ad operazioni imponibili, in tutto o in parte inesistenti ovvero mai eseguite, ovvero eseguite in maniera differente da come documentate nelle pezze giustificative fiscali, oppure intercorse tra soggetti differenti da quelli che figurano in detti documenti.

La società trasferisce, senza dichiararlo in sede di accertamento, in luogo diverso dalla sede legale della società la documentazione contabile, conservandone solo una parte, rendendo più difficoltosa l'attività di verifica fiscale.

Al fine di ottenere un pagamento parziale delle imposte, la Società contabilizza ed indica nei documenti utilizzati ai fini delle dichiarazioni fiscali un attivo inferiore a quello effettivo ovvero elementi passivi inesistenti.

Presidio del rischio attuato dalla Scoietà

Di seguito: principi, norme di comportamento, protocolli e controlli applicati e documenti aziendali di riferimento.

2.17.3.1. Principi specifici di comportamento

Al fine di presidiare correttamente l'area di rischio in commento, la Società si conformerà ai seguenti principi di comportamento con riferimento alle seguenti attività:

- improntare la propria condotta ai principi generali contenuti nel Codice Etico, ed ai principi di legalità, correttezza, tracciabilità e trasparenza;
- tutti i soggetti che intrattengano rapporti con i fornitori devono essere debitamente autorizzati; i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Società devono essere appositamente incaricati;
- garantire la trasparenza dei rapporti di approvvigionamento beni e servizi da terzi (appaltatori, fornitori, consulenti ecc.), valutando accuratamente la qualità del soggetto fornitore di beni e servizi;
- provvedere al controllo di corrispondenza tra ordinato e fornito, sia con riferimento ai beni e servizi, nonché con riferimento alla perfetta corrispondenza dei documenti formati e ricevuti riferiti all'operazione imponibile;
- ogni rapporto relativo a forniture di beni o servizi da parte di soggetti terzi ed esterni dovrà essere formalizzato per iscritto ed il relativo contratto dovrà contenere apposita dichiarazione di conoscenza del Modello e nonché condivisione dei principi di cui al Codice Etico. Il relativo contratto dovrà essere stipulato in conformità ai principi ed alle procedure aziendali in tema di conferimento di incarichi esterni. Non è consentito riconoscere compensi in favore di tali collaboratori o consulenti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto. Il corrispettivo deve essere congruo, corrispondente a quello pattuito ed indicato nel contratto ed il servizio reso documentato o documentabile;
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto della legge e delle procedure aziendali interne, in tutte le fasi della contabilità fiscale a partire dalla registrazione delle fatture, tenuta dei registri fiscali, etc., attività finalizzate alla formazione del bilancio e della dichiarazione di reddito;
- ove la Società dia mandato a soggetti terzi per assisterla nella tenuta della contabilità, elaborazione delle retribuzioni, calcolo delle imposte, nella predisposizione del bilancio, delle comunicazioni sociali, e delle dichiarazioni di richiedere che i soggetti terzi rispettino puntualmente i principi contenuti nel Codice Etico;
- controllare la completezza e veridicità di tutti i documenti fiscali e contabili che contribuiscono alla formazione del bilancio di verifica ai fini della predisposizione della dichiarazione di reddito;
- identificare, analizzare e monitorare i rischi fiscali, mediante l'adozione di adeguate procedure;

- definire un adeguato piano di informazione e formazione del personale sul rischio fiscale;
- mantenere la tracciabilità del processo sia a livello di sistema informativo sia in termini documentali incluso il processo decisionale, con riferimento alle attività di gestione della contabilità fiscale e predisposizione delle dichiarazioni fiscali. La funzione responsabile archivierà e conserverà la relativa documentazione in adempimento alla relativa procedura aziendale.

2.17.3.2. Protocolli aziendali e controlli relativi ai processi

Id. Protoc.	Comportamento prescritto, protocolli e controlli applicati	Riferimenti a protocolli aziendali
12 – 01	Allo scopo di ridurre al minimo il rischio di commissione dei reati qui considerati, è obbligatorio rispettare col massimo rigore tutte le norme, aziendali e legislative, applicabili. In particolare: → "*Procedura di autorizzazione interna degli acquisti*"; → Gestione della cassa: rispetto delle norme di legge che regolano le transazioni commerciali, specialmente con riferimento al limite massimo nell'impiego del contante. In linea generale, deve essere rispettata la regola che vieta che una persona possa, da sola, attivare, gestire, autorizzare e chiudere un processo sensibile. In particolare, il processo degli acquisiti, dalla formulazione della richiesta interna al pagamento, deve obbligatoriamente coinvolgere almeno due diversi Attori.	**→ Vedasi "Procedura di autorizzazione interna degli acquisti" descritta nel presente documento.** **→ Processi aziendali: Procurement** **Regolamento contratti per l'affidamento di beni e servizi di importo inferiore alle soglie comunitarie; Administration Operative Financial Management for IT-Billing; Manuale operativo contabilità SAP;**
12 - 02	In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del Decreto. In aggiunta a quanto precede, al fine di presidiare l'Area e le Attività Sensibili rispetto alla possibile commissione dei reati in esame, dovranno inoltre essere rispettate le previsioni più specifiche contenute nelle procedure aziendali in essere, individuate nella matrice rischi/processi.	

Reati transnazionali – Induzione alla falsa testimonianza – Favoreggiamento personale (Art. 10 comma 9 della L. 146/06)

Reati richiamati dal D.Lgs. 231/01

L'articolo 10 della Legge 146/06, in relazione alla commissione dei reati di cui agli artt. 377-bis e 378 del Codice Penale, richiama la responsabilità amministrativa dell'Ente e l'applicazione delle sanzioni previste dal D.Lgs. 231/01; ciò in particolare per i seguenti reati "*transnazionali*":

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- Favoreggiamento personale

Si definisce "transnazionale" un reato che veda coinvolto un gruppo criminale organizzato e che:

- sia commesso in più di uno Stato

ovvero

- sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato

ovvero

- sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato

ovvero

- sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

Per quanto riguarda il reato di "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" si rimanda al medesimo reato precedentemente trattato con riferimento all'Art. 24-decies del D.Lgs 231/01.

Per quanto riguarda il reato di favoreggiamento personale non si rilevano soggetti/UU.OO. processi particolarmente sensibili da evidenziare.

Reati transnazionali – Associazione per delinquere e di tipo mafioso (Art. 10 comma 2 della L. 146/06)

Reati richiamati dal D.Lgs. 231/01

L'articolo 10 della Legge 146/06, in relazione alla commissione dei reati di cui agli artt. 416 e 416-bis del Codice Penale, richiama la responsabilità amministrativa dell'Ente e l'applicazione delle sanzioni previste dal D.Lgs. 231/01; ciò in particolare per i seguenti reati "*transnazionali*":

- Associazione per delinquere
- Associazione di tipo mafioso

Relativamente al concetto di "*reato transnazionale*" si rimanda all'omologo precedente paragrafo relativo al primo dei *reati transnazionali* illustrati.

Con riferimento ai reati richiamati, trova qui applicazione quanto riportato in sede di trattazione dei "Delitti di criminalità organizzata". (Art. 24-ter del D.Lgs 231/01).