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

Informatica Alto Adige S.p.A.

Redatto da:	Pier Luigi Cavicchi (Engineering-Ing. Inf.ca SPA)
Verificato da:	Felix Irsara – Alberto Zendrini
Approvato da:	Consiglio di Amministrazione
Autorizzato da:	----------
Data di validità:	22/12/2016
N.ro versione:	4.0
N.ro pagine:	78
Distribuzione:	Sito Intranet della Società

Nomefile: Modello_di_Organizzazione_e_Gestione_231_SIAG 4. 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.

Sommario

1 SEZIONE GENERALE

1.1 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 o di un Ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un Ente pubblico
b) reati informatici e trattamento illecito di dati
c) delitti di criminalità organizzata
d) concussione, induzione indebita a dare o promettere utilità e corruzione
e) falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento
f) delitti contro l'industria e il commercio
g) reati societari
h) delitti con finalità di terrorismo o di eversione dell'ordine democratico
i) pratiche di mutilazione degli organi genitali femminili
j) delitti contro la personalità individuale
k) abusi di mercato
l) omicidio colposo o lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro
m) ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio
n) delitti in materia di violazione del diritto d'autore
o) induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
p) reati ambientali
q) impiego di cittadini di paesi terzi il cui soggiorno è irregolare
r) 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.

1.2 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.

1.2.1 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).

1.2.2 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.

1.2.3 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.

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.

([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)

1.3 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.

1.4 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.

1.4.1 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.

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.

1.4.2 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.

1.4.2.1 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.

1.4.2.2 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.

1.4.2.3 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
- la descrizione sintetica dei controlli applicati
- i riferimenti ai documenti aziendali contenenti le norme ed i protocolli.

1.4.2.4 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.

([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.

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.

1.4.3 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.

1.4.4 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.

1.5 L'Organismo di Vigilanza

1.5.1 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.

1.5.2 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.

1.5.3 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.

1.5.4 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.

1.5.5 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.

1.5.6 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.

1.5.7 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.

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.

1.5.8 Obblighi di informativa

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.

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"; vedasi paragrafo successivo) 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.

Inoltre, al fine di garantire un corretto esercizio delle proprie funzioni, l'Organismo di Vigilanza deve essere informato, da chiunque ne abbia contezza, di ogni notizia attinente:

- all'effettiva attuazione del Modello all'interno della Società, anche con riferimento all'applicazione dei protocolli;
- all'eventuale esistenza di aree di attività prive del tutto o in parte di regolamentazione;
- alle eventuali lacune del sistema;
- all'individuazione di potenziali anomalie nell'applicazione del Modello;
- alle proposte di integrazione e le modifiche da apportare alle procedure operative o al Modello stesso;
- alle violazioni o sospette violazioni del Modello, delle procedure ivi richiamate e del Codice Etico;
- al compimento di operazioni straordinarie da parte della Società;
- alla commissione di reati all'interno dell'Azienda.

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

La suddetta casella di posta elettronica è accessibile solo ai Componenti dell'OdV e resa inaccessibile a Terzi.

L'Organismo di Vigilanza farà in modo che i Soggetti segnalanti siano tutelati contro ogni forma di ritorsione, discriminazione e/o penalizzazione, garantendo, nei limiti degli obblighi di legge e della tutela dei diritti della Società, l'anonimato dei medesimi segnalanti e la riservatezza di quanto segnalato.

1.5.9 Flussi informativi verso l'OdV

La funzione di Internal Auditing comunica in forma sintetica all'Organismo di Vigilanza le verifiche effettuate nell'ambito della Società e i relativi esiti.

I Responsabili flussi informativi 231, formalmente nominati dal Presidente, vengono individuati all'interno del Management della Società (Responsabili di Direzione e/o di Reparto).

I Responsabili flussi informativi 231 inviano all'Organismo di Vigilanza:

1) con cadenza quadrimestrale:
   - informazioni (di tipologia specificamente individuata) ritenute utili alla tempestiva identificazione di attività a rischio (in ottica D.Lgs. 231/01) ovvero utili a documentare la corretta applicazione delle prescrizioni contenute nel presente Modello;
   - ogni altro dato ritenuto utile per una migliore attuazione del Modello
2) a due mesi dalla scadenza del periodo quadrimestrale di cui al flusso precedente:
   - un'informativa sintetica di aggiornamento circa l'eventuale manifestarsi di fatti rilevanti e/o di inosservanze significative meritevoli di segnalazione;
3) di volta in volta, obbligatoriamente ed immediatamente, i dati relativi:
   - alla commissione dei reati-presupposto e all'adozione di comportamenti non in linea con le regole di condotta previste dal Modello;
   - ai provvedimenti e/o alle notizie da cui si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto, la cui commissione si assuma essere avvenuta nella Società; ovvero l'esistenza di un procedimento penale a carico della stessa Società;
   - alle richieste di assistenza legale inoltrate dai Soggetti nei confronti dei quali la Magistratura proceda per i reati previsti dal Decreto;
   - ad ogni anomalia o atipicità riscontrata nell'ambito delle attività a rischio, alle notizie relative alle asserite o accertate violazioni del Modello o del Codice Etico e alle eventuali sanzioni disciplinari irrogate, ovvero ai provvedimenti di archiviazione di tali procedimenti, con le relative motivazioni.

I Collaboratori esterni, i Fornitori ed i Partner effettuano le eventuali segnalazioni relative all'attività svolta per la Società direttamente all'Organismo di Vigilanza, via e-mail, con le modalità già precedentemente indicate.

L'Organismo di Vigilanza:

1) garantisce la riservatezza dell'identità del segnalante e delle persone oggetto della segnalazione; il segnalante è inoltre garantito contro qualsiasi forma di ritorsione, discriminazione o penalizzazione;
2) valuta le segnalazioni ricevute e, ove necessario, svolge un'attività istruttoria, senza obbligo di comunicare al segnalante la decisione assunta.

Ove ravvisi una violazione del Modello, l'Organismo di Vigilanza:

- promuove presso il Direttore un procedimento disciplinare a carico del Dipendente ritenuto responsabile;
- informa il Consiglio di Amministrazione e il Collegio sindacale, nel caso di violazione commessa da uno o più membri dei predetti Organi sociali;

- chiede alla Direzione di competenza di porre in esecuzione le clausole contrattuali di risoluzione e/o recesso dei rapporti con Collaboratori esterni, Fornitori e Partner, nel caso di violazione agli stessi addebitabile.

1.5.10 Risposta alla notizia di reato

Qualora venga a conoscenza, attraverso qualunque canale informativo, di una notizia di reato ex D.Lgs. 231/01 commesso all'interno dell'organizzazione della Società, l'Organismo di Vigilanza attiva una serie di iniziative volte a rilevare i punti di debolezza del Modello eventualmente sfruttati nella commissione del reato stesso.

A tal fine, anche usufruendo del supporto della funzione di Internal Auditing, vengono individuati ed intervistati i Soggetti coinvolti, in vario ruolo, o informati dei fatti che hanno determinato il concretizzarsi del reato, vengono ricostruite le fasi dei processi aziendali interessati, analizzati i controlli prescritti dai protocolli, sia quelli attuati (e relative evidenze), che quelli eventualmente omessi.

Laddove, a seguito di una segnalazione anonima, le indagini dovessero focalizzarsi sul comportamento di un Dipendente, lo stesso verrà informato della cosa da parte di un Responsabile incaricato dall'OdV, a garanzia di un comportamento trasparente da parte della Società ed allo scopo di fugare sospetti di un atteggiamento pregiudizialmente colpevolistico nei confronti del Dipendente.

Ottenuto un quadro sufficientemente chiaro di quanto accaduto e valutate, nel merito, le circostanze emerse, l'OdV procederà, di volta in volta, adottando una o più delle seguenti iniziative:

- informerà i Vertici della Società dell'accaduto, in particolare il Direttore, al quale proporrà, se del caso, l'applicazione di appropriate sanzioni disciplinari;
- informerà gli altri organi di controllo della Società, in primis il Collegio sindacale, per le loro eventuali autonome iniziative;
- solleciterà l'introduzione nel Modello di specifici protocolli (o, eventualmente, la modifica di quelli esistenti) al fine di meglio garantire rispetto al rischio del ripetersi di quanto accaduto;
- proporrà al Presidente e/o al Direttore adeguamenti degli interventi formativi normalmente svolti in Azienda, adeguamenti focalizzati sul rischio di commissione del reato in questione, così come potrà proporre a detti Responsabili la previsione di sanzioni disciplinari più severe.

1.6 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.

1.7 Il Sistema disciplinare

1.7.1 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.

1.7.2 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.

1.7.3 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.

1.7.4 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.