EQUASOFT

MODELLO
DI ORGANIZZAZIONE, GESTIONE
E CONTROLLO
AI SENSI DEL
D.Lgs. 231/2001

Sommario

1. FINALITÀ DEL DOCUMENTO

Il presente documento, denominato "Modello di Organizzazione, Gestione e Controllo" (di seguito il "Modello"), è stato redatto e deliberato da EQUASOFT S.R.L. (di seguito "Equasoft" o "Società") in attuazione del disposto di cui agli artt. 6 e 7 del Decreto Legislativo n. 231 dell'8 giugno 2001 e successive modifiche ed integrazioni. Scopo del presente documento è raggiungere e mantenere la conformità a quanto previsto dal Decreto Legislativo 231/2001

2. IL DECRETO LEGISLATIVO 231/2001 E LE NORME DI RIFERIMENTO

2.1. Breve disamina sulla normativa

L'introduzione della responsabilità amministrative delle persone giuridiche, avvenuta con d.lgs. 8 giugno 2001 n. 231 (di seguito "Decreto 231"), si inserisce nell'ambito dell'ampio movimento di lotta alla corruzione internazionale che ha imposto agli Stati aderenti all'Unione Europea l'assunzione di mezzi omogenei di repressione e prevenzione della criminalità che coinvolge il settore economico. La comunità internazionale ha cercato, da un lato, di creare un sistema sanzionatorio delle condotte illecite omogeneo e, dall'altro, di individuare specifiche responsabilità in capo alle imprese, al fine di garantire una generale correttezza ed eticità del mercato.

Il D. Lgs. 8 giugno 2001, n. 231, ha introdotto nel nostro ordinamento la responsabilità cd. amministrativa, degli enti (con ciò intendendosi anche le imprese, particolarmente in forma di società) per alcuni reati commessi, nel loro interesse o vantaggio, da determinati soggetti ad essa collegati: preposti, dipendenti o anche soggetti in rapporto funzionale con l'ente stesso. Tale responsabilità si aggiunge, e non si sostituisce, alla responsabilità della persona fisica che ha realizzato materialmente il fatto illecito.

Inoltre all'impresa "si applicano le disposizioni processuali relative all'imputato, in quanto compatibili". Invero, la responsabilità delle persone giuridiche (cd. enti), pur se espressamente definita dal D.Lgs. 231/2001 come "amministrativa", è in realtà di natura ibrida in quanto presenta vari aspetti di natura spiccatamente penale. In particolare il decreto ha previsto che l'accertamento della responsabilità delle imprese per illeciti amministrativi dipendenti da reato debba avvenire nell'osservanza delle norme richiamate al Capo III del decreto stesso nonché "secondo le disposizioni del codice di procedura penale e del D. Lgs. 28 luglio 1989 n. 271 in quanto compatibili" (Art. 34).

Le condizioni essenziali affinchè sia configurabile la responsabilità dell'ente sono tre:

- La commissione di un reato a cui la legge collega la responsabilità dell'ente;
- La commissione di tale reato nell'interesse o a vantaggio dell'ente;
- L'autore del reato sia:

- Un soggetto apicale: colui che riveste funzioni di rappresentanza, amministrazione o direzione della società, nonché colui che esercita, anche di fatto, la gestione e il controllo delle stesse;
- Un soggetto sottoposto alla direzione o alla vigilanza di soggetti apicali.

Nella configurazione data a questa nuova forma di responsabilità, il fatto di reato è sempre quello previsto dalla norma incriminatrice e commesso da una persona fisica. Tuttavia, nel caso in cui la legge esplicitamente preveda per tale reato la responsabilità dell'ente e in concreto questo sia stato commesso nel suo interesse si verifica un illecito amministrativo dipendente dal reato di cui l'ente stesso è responsabile. La responsabilità dell'ente discende, dunque, dalla commissione, da parte di soggetti ad esso appartenenti, di reati tassativamente indicati dal Decreto 231

L'ambito di applicazione, dal punto di vista soggettivo, è quindi piuttosto vasto: soggetti destinatari della nuova disciplina, secondo il dettato normativo, sono gli enti forniti di personalità giuridica, le società ed associazioni, quest'ultime anche se prive di personalità giuridica.

La ratio della riforma, per espressa ammissione del legislatore, è quella di coinvolgere il patrimonio degli enti e, in definitiva, gli interessi economici dei soci, nella punizione di alcuni illeciti penali, realizzati nell'interesse o a vantaggio dell'ente stesso, al fine di richiamare i soggetti interessati ad un maggiore (auto)controllo della regolarità e della legalità dell'operato aziendale in funzione preventiva.

Stante l'ampia previsione della legislazione, il regime di responsabilità previsto dalla normativa di cui si tratta, si applica anche a Equasoft.

2.2. Il catalogo dei reati-presupposto

Secondo il principio di legalità, solo i reati espressamente indicati dalla legge generano la responsabilità degli enti. Il **catalogo aggiornato dei reati-presupposto** previsti dal D.Lgs 231/2001 è consultabile quale **Allegato 01**:

2.3. L'apparato sanzionatorio a carico dell'ente

Le sanzioni previste dalla legge a carico dell'ente responsabile sono:

- sanzione pecuniaria;
- sanzione interdittiva;
- confisca;
- pubblicazione della sentenza.

Le sanzioni pecuniarie e la confisca vengono sempre applicate, mentre la sanzione interdittiva e la pubblicazione della sentenza sono previste solo per alcune tipologie di reato.

Sono sanzioni interdittive:

- Interdizione all'esercizio dell'attività;
- Sospensione o revoca delle autorizzazioni, licenze, concessioni che siano funzionali alla commissione dell'illecito;
- Divieto di contrattare con la Pubblica Amministrazione;
- Esclusione dalle agevolazioni, finanziamenti, contributi e sussidi e l'eventuale revoca di quelli già concessi;
- Divieto di pubblicizzare beni e servizi.

Tali sanzioni limitano notevolmente la libertà di azione dell'ente e sono generalmente temporanee. Di norma esse vengono irrogate:

- in caso di reiterazione dell'illecito;
- se l'ente ha tratto un profitto di rilevante entità;
- ove vengano evidenziate gravi carenze organizzative.

La normativa in oggetto è applicata, secondo i principi e le procedure del diritto penale, dal Giudice Penale.

2.4. Il modello organizzativo come esimente di responsabilità

E' bene precisare che la responsabilità amministrativa dell'ente sorge quando la condotta sia posta in essere da soggetti legati all'organizzazione collettiva da relazioni funzionali, classificate dalla legge in due categorie: quella facente capo ai "soggetti in cd. posizione apicale", che comprende pertanto i vertici dell'ente, e quella riguardante "soggetti sottoposti all'altrui direzione". La legge esonera dalla responsabilità l'ente qualora dimostri di aver adottato ed efficacemente attuato, prima della commissione del reato, modelli di organizzazione, gestione e controllo idonei a prevenire la realizzazione degli illeciti penali considerati.

A questo proposito il nuovo Testo Unico di cui al D. Lgs. n. 81/2008, all'art. 30 ben individua la necessità da parte delle imprese dell'adozione di un modello organizzativo avente le caratteristiche previste dal D. Lgs. n. 231/01 ed idoneo a prevenire la commissione di reati conseguenti all'inosservanza della normativa in materia di tutela della salute e della sicurezza nei luoghi di lavoro. Tale esimente opera diversamente a seconda che i reati siano commessi da soggetti in posizione apicale o soggetti sottoposti alla direzione di questi ultimi.

Il criterio di imputazione è, dunque, differente a seconda che il reato sia commesso da un soggetto in posizione apicale o da un semplice sottoposto. Nel primo caso è prevista un'inversione dell'onere della prova a carico della Società, la quale non risponde se prova:

- di aver adottato ed efficacemente attuato prima della commissione del reato da parte del soggetto in posizione apicale un "Modello di organizzazione, gestione e controllo" (di seguito "Modello) astrattamente idoneo a prevenire reati della specie di quello verificatosi;
- di aver attivato un organismo interno dotato di autonomi poteri di iniziativa e di controllo, cui è stato affidato il compito di vigilare sull'osservanza dei modelli, nonché di promuovere il loro aggiornamento, e che non vi sia stata omessa o insufficiente vigilanza da parte di tale organismo;
- che il soggetto in posizione apicale ha commesso il reato "eludendo fraudolentemente i modelli di organizzazione e di gestione", preventivamente adottati ed efficacemente implementati.

Nell'ipotesi in cui, invece, il reato sia commesso da un soggetto sottoposto all'altrui direzione, non è prevista alcuna inversione dell'onere della prova, la dimostrazione della mancata adozione del modello organizzativo gravando sulla pubblica accusa.

3. IL MODELLO ORGANIZZATIVO DI EQUASOFT

3.1. Dati aziendali,

Ragione sociale:	***EQUASOFT SRL***
Campo di attività:	***PROGETTAZIONE E REALIZZAZIONE DI ATTIVITA' FORMATIVE***
Legale rappresentante	***Vanzo Giuseppe***
Sede legale	***36100 Vicenza, Via Divisione Folgore 7/D,***
Partita iva	***02912990245***

3.2. Presentazione dell'azienda e analisi del contesto, funzioni e principi ispiratori

EQUASOFT è un ente di formazione e consulenza specializzato nello sviluppo delle risorse umane. La società opera nel contesto della Formazione Professionale svolgendo azioni formative rivolte sia ad adulti - già inseriti nel mondo del lavoro o alla ricerca di primo o nuovo impiego – che a giovani da avviare alla prima occupazione, post diploma o post laurea. EQUASOFT, in particolare, è punto di riferimento per la formazione e la consulenza in ambito informatico. Sono inoltre presenti anche attività formative in adempimento alla legislazione vigente, atte a rilasciare ai partecipanti particolari qualifiche o attestazioni.

EQUASOFT, infatti, oltre ad occuparsi di formazione, si dedica altresì alla certificazione dei percorsi, all'assistenza pre e post formazione e agli accreditamenti, essendo Organismo di Formazione accreditato dalla Regione Veneto.

L'attività svolta può prevedere il pagamento del servizio direttamente da parte del partecipante o di aziende committenti ma spesso essa è collegata a bandi pubblici, europei, nazionali e regionali.

3.3. Funzioni, obiettivi e principi ispiratori

Nel contesto in cui opera Equasoft e a seguito della crescente importanza che la formazione riveste durante tutta la vita della persona sono risultate chiare alla direzione dell'ente:

- da una parte, la necessità di adottare modelli di organizzazione, gestione e controllo tali da favorire l'efficacia e l'efficienza delle azioni svolte;
- dall'altra, di tutelare l'ente stesso a fronte di possibili pratiche scorrette, illecite o semplicemente inadeguate attuate dai propri collaboratori con l'obiettivo di procurare illeciti vantaggi.

A questo riguardo EQUASOFT ha adottato tale Modello che, unitamente al Codice Etico (il quale definisce i principi di condotta degli affari della Società nonché gli impegni e le responsabilità che riguardano tutti i destinatari del Codice Etico stesso), alle procedure organizzative e alle altre politiche e disposizioni della Società, assicura un'efficace prevenzione e rilevazione di violazione di leggi e permette una conduzione dell'impresa sana.

Inoltre, EQUASOFT in qualità di Ente di formazione accreditato dalla Regione Veneto ha implementato un modello organizzativo ai sensi del DL 231/01 a seguito del Decreto della Giunta Regionale del Veneto numero 581 del 19.05.2016 in tema di accreditamento degli Organismi di Formazione. Operare con l'Ente pubblico ed usufruire di finanziamenti pubblici rappresenta senz'altro un elemento di estrema delicatezza che rende necessarie politiche di trasparenza e moralità che nel rapporto tra privati sono spesso scongiurati dal continuo controllo reciproco.

Il modello è stato progettato secondo le linee guida fornite da vari organismi associativi, indicazioni provenienti da standard di certificazione volontaria, spunti metodologici provenienti da vari strumenti di management e gestione aziendale, quali il Risk Based Thinking ed il Quality Function Deployment. Nello sviluppo del modello, inoltre, si è tenuto in considerazione quanto già presente quale adempimento a requisiti normativi vigenti o a seguito di scelte aziendali, nell'ottica della creazione di un sistema di gestione integrato. Ci si riferisce in particolare alla presenza e piena operatività di strumenti per la sicurezza dei lavoratori, per il rispetto della privacy e per la conformità alla norma UNI EN ISO 9001.

EQUASOFT ritiene, altresì, che l'adozione del Modello costituisca un'opportunità importante di verifica, revisione ed integrazione dei processi decisionali ed applicativi aziendali, nonché dei sistemi di controllo dei medesimi, rafforzando l'immagine di correttezza e trasparenza alla quale si è sempre orientata l'attività aziendale.

EQUASOFT è altresì convinta che l'adozione del Modello possa costituire un valido strumento di sensibilizzazione nei confronti di tutti i dipendenti della Società e di tutti i soggetti coinvolti, a diverso titolo, dall'attività aziendale.

3.4. Processo di erogazione del servizio

EQUASOFT opera nell'ambito della progettazione ed erogazione di attività formative. Tali attività possono essere sviluppate a seguito di:

a) adesione a bandi pubblici europei, nazionali o regionali;

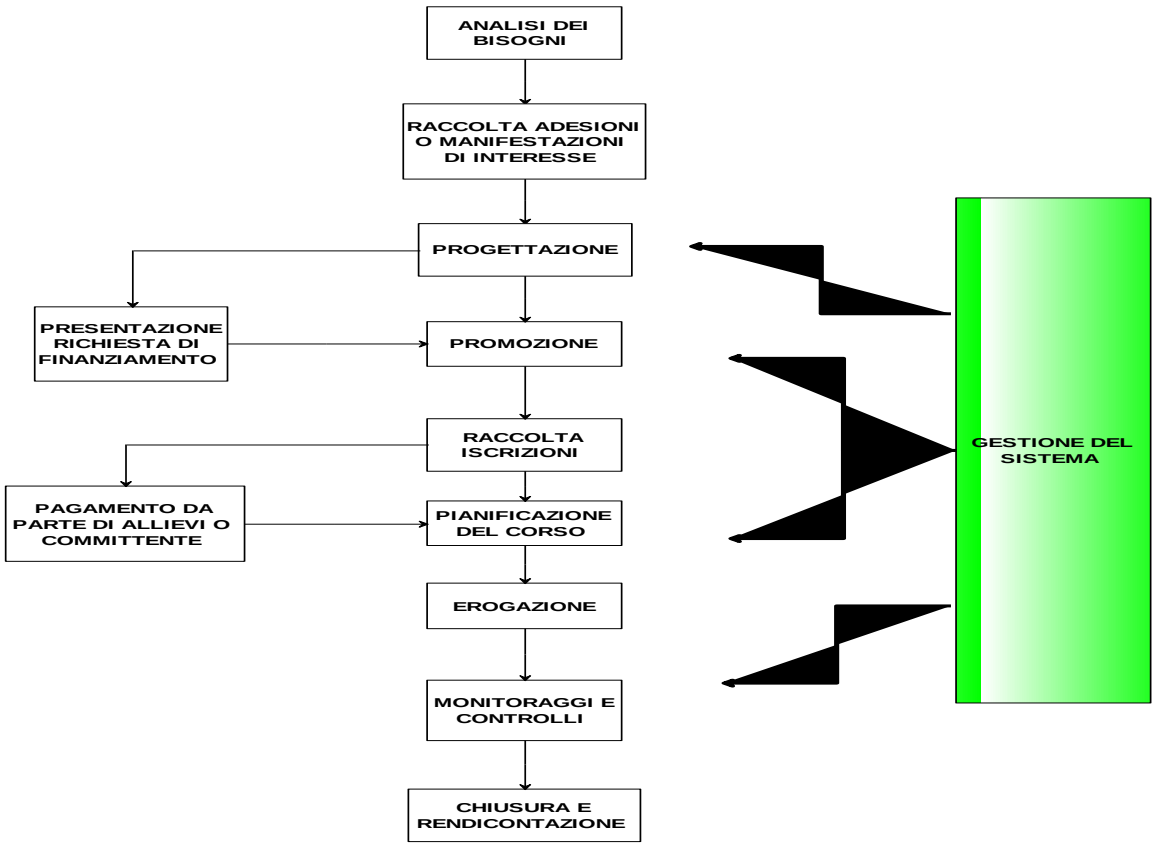
b) Necessità formative per adempimenti legislativi;

c) Richieste da parte di aziende pubbliche o private di azioni formative specifiche.

Mentre nel caso (c) il rapporto è esclusivamente tra soggetti privati, nei casi (a) e (b), seppur con diverse modalità, intervengono soggetti pubblici, nel primo come soggetti finanziatori e di controllo dell' effettivo e corretto impiego dei fondi erogati, nel secondo come autorità di controllo in merito alla effettiva e corretta erogazione del servizio.

Le attività si svolgono secondo il diagramma di flusso di seguito illustrato, nel quale sono state indicate le diverse alternative (attività soggetta a finanziamento o a pagamento da parte degli utenti). Successivamente, le varie attività qui dettagliate sono state inglobate nell'area "Gestione dell'erogazione del corso.

Nel diagramma è stato riportato anche il processo complessivo di "gestione dell'ente", che raccoglie tutte quelle attività di indirizzo, controllo e rappresentanza (successivamente divise in diverse aree/attività) non strettamente riconducibili alla specifica erogazione del servizio ma nelle quali comunque potrebbero configurarsi situazioni a rischio per la potenziale commissione di reati.



3.5. Destinatari del Modello

Le disposizioni del presente Modello sono vincolanti tanto per i "soggetti apicali", quanto per le persone sottoposte alla loro direzione o vigilanza. Sono dunque destinatari del Modello, ciascuno nell'ambito del ruolo ricoperto o delle attività svolte per Equasoft:

- gli amministratori e i componenti dell'organo di controllo;
- le "Risorse umane": insieme dei lavoratori dipendenti, somministrati e distaccati, nonché i lavoratori parasubordinati e gli altri soggetti che fanno parte dell'organico della Società, a prescindere dalla forma contrattuale o dalla normativa di riferimento,
- gli altri "collaboratori", a prescindere dalla categoria professionale e dalla forma contrattuale, nei limiti in cui la loro prestazione lavorativa sia coordinata con l'organizzazione aziendale di Equasoft e sottoposta alla direzione o vigilanza di un soggetto apicale.

3.6. Elaborazione ed approvazione del Modello

Il modello è stato redatto in conformità al decreto citato, nonché alle Linee Guida elaborate in materia da Confindustria del 21 luglio 2014; inoltre sono state tenute in considerazione le indicazioni provenienti fino ad oggi dalla giurisprudenza in materia. Gli *step* operativi per la creazione del modello sono stati i seguenti:

1. ANALISI DEL CONTESTO

2. DESCRIZIONE DEL PROCESSO DI EROGAZIONE DEL SERVIZIO

3. ANALISI DEL RISCHIO CORRELATO AI REATI PREVISTI DAL D.Lgs. 231/01

4. INCROCIO TRA POSSIBILI REATI E FASI DEL PROCESSO

5. INDIVIDUAZIONE DELLE AZIONI ATTE A PREVENIRE LA COMMISSIONE DEL REATO

6. CREAZIONE DEL SISTEMA DEI CONTROLLI

7. CREAZIONE DELL'ORGANISMO DI VIGILANZA

8. CODICE ETICO

9. QUADRO SANZIONATORIO

10. MIGLIORAMENTO CONTINUO

3.7. Verifica ed Aggiornamento del Modello

Il Modello è stato espressamente costruito per EQUASOFT sulla base della situazione attuale delle attività aziendali e dei processi operativi. Esso è uno strumento vivo e corrispondente alle esigenze di prevenzione e controllo aziendale; di conseguenza, deve provvedersi alla periodica verifica della rispondenza del Modello alle predette esigenze, provvedendo quindi alle integrazioni e modifiche che si rendessero di volta in volta necessarie. La verifica si rende inoltre necessaria ogni qualvolta intervengano modifiche organizzative aziendali significative, particolarmente nelle aree già individuate come a rischio.

Le verifiche sono svolte dall'Organismo di Vigilanza, che all'occorrenza può avvalersi della collaborazione ed assistenza di professionisti esterni, per poi proporre all'Organo Amministrativo e al Collegio Sindacale le modifiche opportune.

Il Modello Organizzativo è oggetto di valutazione annuale da parte del CdA non solo a seguito della relazione annuale dell'Organismo di Vigilanza ma anche in ragione di:

a) risultati degli audit interni.
b) Reclami e contestazioni provenienti dagli stakeholder.
c) Esito delle verifiche da parte degli organismi pubblici.
d) Esito dei monitoraggi interni.
e) Modifiche legislative intercorse.

A seguito di tale valutazione il CdA dispone:

- la conferma o la modifica del Modello e dei documenti ad esso correlati.
- La predisposizione del piano annuale di miglioramento .

Eventuali modifiche del modello approvato a mente del disposto ci cui all'art. 6 del D. Lgs. 231/01 saranno oggetto di approvazione da parte del Consiglio di Amministrazione nel caso in cui comportino integrazioni o modifiche necessarie in relazione all'evolversi della normativa o che comportino una modifica di ruolo e/o della composizione dell'Organismo di Controllo. Tali modifiche debbono ritenersi di carattere sostanziale. Viceversa, nel caso di implementazioni necessitate dall'evolversi dell'operatività aziendale le modifiche del modello, da non ritenersi sostanziali, saranno approvate e implementate dallo stesso Organismo di controllo. Lo stesso provvederà poi a comunicare al Consiglio di Amministrazione e contestualmente al Collegio Sindacale le modifiche effettuate e l'organo collegiale provvederà a ratificarle ovvero ad apportare ulteriori modifiche e/o integrazioni (la versione definitiva delle modifiche apportate sarà comunicata al collegio sindacale). Nel periodo transitorio intercorrente tra le modifiche decise e implementate le stesse saranno efficaci e cogenti.

4. ANALISI DEL RISCHIO CORRELATO AI REATI PREVISTI DAL D.LGS. 231/01

4.1. Risk assessment

In base all'analisi del processo di erogazione del servizio descritto al paragrafo 3.4 è stata svolta l'analisi dei pericoli, schematizzata nella tabella in allegato (**Allegato 02 – Risk Assessment**).

Le valutazioni in merito all'effettiva esistenza di un rischio sono state fatte attraverso una preventiva caratterizzazione della possibilità che un reato possa essere commesso. Tale valutazione non fa ovviamente riferimento alla effettiva probabilità di commissione del reato quanto piuttosto alla valutazione che, visto il contesto in cui l'ente opera, l'evento possa accadere e che quindi, in base a quanto indicato dal D.Lgs. 231, sia necessario mettere in atto dei protocolli volti a scongiurare tale possibilità.

In tal senso la possibilità di commissione di ogni reato previsto dal D.Lgs. 231 è stata valutata in base al contesto in cui l'ente opera e quindi alla opportunità che si può presentare per un suo componente di pianificarlo fraudolentemente o di commetterlo in modo colposo.

Così operando, ad ogni reato è stato attribuito un livello di possibilità di commissione secondo il seguente schema:

LIVELLO	DESCRIZIONE
NULLO	***Le caratteristiche dell'ente, il campo e la tipologia delle attività svolte sono tali da rendere impossibile la commissione del reato all'interno dell'ente stesso.***

BASSO	***I protocolli o le procedure operative con cui sono gestite le attività e il tipo e le frequenze dei controlli effettuati sono tali da rendere bassa la possibilità di commissione del reato.***
MEDIO	***La commissione del reato è possibile, ma i protocolli e le procedure operative, unitamente alle misure precauzionali adottate, contengono e normalizzano la probabilità di commissione del reato.***
ALTO	***La commissione del reato è possibile ed è necessario mettere in atto stringenti misure precauzionali al fine che solo con azione consapevolmente fraudolente e con l'elusione delle procedure in atto un membro dell'ente possa commettere il reato.***

In questo modo il primo risultato è consistito nella eliminazione di una serie di reati non concretamente realizzabili nel contesto operativo dell'ente. Ciò ha permesso al gruppo di lavoro di concentrarsi nei reati che potenzialmente possono accadere.

Tale valutazione è riportata nella prima parte dell'allegato***.***

Infine, per ogni singolo "reato presupposto" considerato possibile (sia a rischio "**Basso**" che "**Alto**") sono state individuate idonee regole interne ad integrazione del Codice Etico. Anche i risultati di tale analisi sono riportati nell'allegato 02.

4.2. Reati concretamente realizzabili in Equasoft

Si riportano di seguito i reati concretamente realizzabili nella società:

a) Reati contro la Pubblica Amministrazione: RISCHIO MEDIO
b) Delitti informatici e trattamento illecito di dati: RISCHIO BASSO
c) Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento: RISCHIO BASSO
d) Reati societari: RISCHIO MEDIO
e) Abusi di mercato: RISCHIO BASSO
f) Reati colposi commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro: RISCHIO BASSO
g) Delitti in materia di violazione del diritto d'autore: RISCHIO BASSO
h) Reati di razzismo e xenofobia: RISCHIO BASSO

4.3. Aree rilevanti

Sulla base dell'analisi di cui sopra e dei reati identificati come potenzialmente realizzabili, le aree rilevanti individuate, per le quali sono state identificate idonee regole interne (singole parti speciali del modello), sono indicate di seguito, unitamente al Protocollo/Procedura in cui sono regolamentate:

AREE RILEVANTI	REGOLAMENTAZIONE
Gestione dei rapporti con la PA di carattere generale	Parte Speciale 1, Codice Etico
Gestione dei rapporti con le Autorità di Vigilanza	Parte Speciale 1, Codice Etico
Gestione e concessione di omaggi e liberalità	Parte Speciale 1, Codice Etico
Gestione della tesoreria	Parte Speciale 1, Parte Speciale 3
Gestione di rimborsi spese a dipendenti e collaboratori	Parte Speciale 1
Gestione di finanziamenti, contributi ed erogazioni	Parte Speciale 1, Parte Speciale 5
Approvvigionamento di beni, servizi e prestazioni	Parte Speciale 1, Codice Etico
Gestione dell'erogazione del corso	Parte Speciale 1, Parte Speciale 2, Parte Speciale 3, Parte Speciale 5, Parte Speciale 6
Gestione dell'assunzione del personale	Parte Speciale 1, Parte Speciale 6
Gestione dei sistemi informativi aziendali	Parte Speciale 2
Sicurezza logica dei sistemi	Parte Speciale 2
Gestione degli incidenti	Parte Speciale 2
Misure per la sicurezza delle reti di trasmissione	Parte Speciale 2
Gestione dell'ambiente fisico	Parte Speciale 2
Comunicazioni esterne	Parte Speciale 3, Codice Etico
Formazione del bilancio, gestione della contabilità e degli adempimenti fiscali	Parte Speciale 3, Codice Etico
Gestione delle operazioni sul capitale	Parte Speciale 3, Codice Etico
Gestione delle operazioni straordinarie	Parte Speciale 3, Codice Etico
Funzionamento degli organismi di controllo	Parte Speciale 3
Comunicazioni all'assemblea e agli organismi di controllo	Parte Speciale 3, Codice Etico

Gestione delle informazioni privilegiate	Parte Speciale 3, Codice Etico
Gestione dei rapporti e degli adempimenti verso Soci, Sindaci e organismi di controllo	Parte Speciale 3
Gestione degli adempimenti in materia di salute e sicurezza degli impianti e dei luoghi di lavoro	Parte Speciale 4, Codice Etico
Gestione dei valori e del denaro incassato	Parte Speciale 5, Codice Etico

Si specifica che, al fine di individuare le aree rilevanti:

- la fase "gestione dell'ente" di cui al punto 3.4 è stata qui scissa in varie altre fasi/attività specifiche che consentono un'evidenziazione più chiara e precisa delle singole procedure predisposte;
- le varie attività individuate nello schema di cui al punto 3.4 sono state inglobate nell'area "Gestione dell'erogazione del corso".

5. SISTEMA DI CONTROLLO

5.1. Individuazione delle azioni atte a prevenire la commissione del reato

L'allegato 02 – Risk Assessment riporta anche le azioni preventive messe in atto dall'Ente per prevenire la commissione dei singoli, specifici reati. Nella specifica realtà di EQUASOFT le azioni preventive indicate in modo generico nell'allegato, sono state inserite e tradotte in prassi operative, nelle procedure del Sistema di Gestione per la Qualità impostato coerentemente alla norma internazionale ISO 9001.

5.2. Sistema dei controlli, monitoraggi e sorveglianza

Il sistema dei controlli messi in atto è così articolato, partendo dal livello più operativo per giungere ai controlli di carattere gestionale:

TIPO DI CONTROLLO	**ESECUTORE**	**FREQUENZA**	**REGISTRAZIONE**
Controlli in itinere e finali durante l'erogazione del servizio.	***Docenti Tutor Direzione Partecipanti***	***Continua su base campionaria. Finale.***	***Registri delle lezioni Relazioni intermedie Relazioni finali Questionari di soddisfazione.***
Controlli di sistema	***Auditor intero o esterno***	***Minimo annuale***	***Rapporto di audit***
Verifiche sul Modello Organizzativo	***OdV***	***Semestrale***	***Relazioni semestrali ed annuali***

Verifiche amministrative e di bilancio	***Collegio Sindacale Organismo di revisione del Bilancio***	***Annuale***	***Relazioni annuali***

Controlli specifici da parte di tutte le funzioni indicate possono avvenire in ogni momento a seguito di segnalazioni, presenza di non conformità, adozione di misure preventive particolari.

6. CODICE ETICO

6.1. Premessa

L'adozione di "**principi etici**" ai fini della prevenzione dei reati considerati costituisce un elemento essenziale del **sistema di controllo preventivo**.

Questi principi sono stati inseriti nel documento **Codice Etico**, redatto dal gruppo di lavoro ed approvato dal Consiglio di Amministrazione di EQUASOFT (**Allegato 03 – Codice Etico**).

Il "codice etico" è quindi a tutti gli effetti, un documento ufficiale dell'ente e contiene l'insieme dei diritti, dei doveri e delle responsabilità dell'ente nei confronti dei "portatori d'interesse" (dipendenti, fornitori, clienti, Pubblica Amministrazione, azionisti, mercato finanziario, ecc.) e di questi nei confronti dell'ente stesso.

Il Codice raccomanda, promuove o vieta determinati comportamenti, indipendentemente da quanto previsto a livello normativo, al fine di garantire le regole cui i destinatari devono attenersi nei rapporti con diversi interlocutori, ed in particolare con la Pubblica Amministrazione e i pubblici dipendenti.

6.2. Principi etici generali

EQUASOFT si conforma, nell'espletamento della propria attività, ai principi di legittimità, lealtà, correttezza e trasparenza, valori ritenuti fondamentali per la propria affermazione e reputazione.

I Soci, il Consiglio di Amministrazione, l'Amministratore Unico, i Dipendenti, e tutti i collaboratori dell' Ente, quali destinatari del presente Codice Etico, sono tenuti ad attenersi a tali principi e devono altresì mantenere un comportamento eticamente corretto, anche al di fuori dell'orario di lavoro, nei rapporti con i colleghi, clienti, fornitori, istituzioni pubbliche.

Per EQUASOFT principi quali la legalità, la concorrenza leale, l'onestà, l'integrità morale, la trasparenza, l'affidabilità e il senso di responsabilità rappresentano aspetti imprescindibili che ne improntano i comportamenti sia nelle relazioni interne sia nei rapporti con gli stakeholder e, più in generale, con l'esterno.

I principi generali da rispettare sono i seguenti:

- Legalità
- Onestà
- Rispetto della persona
- Trasparenza e Imparzialità
- Assenza di Conflitto di interessi
- Qualità
- Tutela del patrimonio aziendale e delle risorse strutturali e informatiche
- Tutela dell'ambiente e sviluppo sostenibile
- Repressione del terrorismo e tutela dell'ordine democratico

7. ORGANISMO DI VIGILANZA

7.1. Premessa

L'art. 6 del D.Lgs. 231 prevede che l'ente possa essere esonerato dalla responsabilità conseguente alla commissione di reati-presupposto se l'ente ha:

- adottato modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati;
- affidato il compito di vigilare sul funzionamento e l'osservanza del modello e curarne l'aggiornamento a un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo (Organismo di Vigilanza o "OdV").

7.2. Individuazione, composizione e revoca dell'Organismo di Vigilanza.

In ottemperanza a quanto previsto dall'art.6 del D.Lgs. 231/2001, è stato costituito un Organismo di Vigilanza, dotato di autonomi poteri di iniziativa e di controllo, cui è affidato il compito di vigilare sul funzionamento e l'osservanza del modello, nonché quello di curarne l'aggiornamento e le verifiche periodiche. Le Linee Guida di Confindustria suggeriscono che si tratti di un organo diverso dal CdA e dal Collegio Sindacale, composto da uno o più membri esterni alla Società, che sia caratterizzato da autonomia, indipendenza, professionalità e continuità d'azione.

L'OdV non costituisce, dunque, una sovrapposizione rispetto agli organi di controllo previsti nel sistema di gestione ma, come indicato al precedente paragrafo, si integra ad essi allo scopo di attuare e mantenere una corretta gestione e un efficiente apparato di controllo. In tale ottica il Modello prevede un sistema di scambio incrociato di informazioni tra i vari organi e le varie funzioni dell'ente.

Applicando tali principi alla realtà di Equasoft, il Consiglio di Amministrazione ha ritenuto opportuno provvedere alla costituzione di un Organismo di Vigilanza monocratico, composto da un soggetto che disponga delle caratteristiche di professionalità, indipendenza, continuità di azione e che non

abbia alcuna attribuzione di compiti di indirizzo politico - amministrativo nella gestione aziendale e di compiti decisionali.

La nomina è di competenza del Consiglio di Amministrazione.

L'Organismo opera secondo quanto definito nello specifico **Regolamento dell'Organismo di Vigilanza** (**Allegato 04 – Regolamento dell'OdV**) a sua volta approvato in sede di Consiglio di Amministrazione.

L'Organismo di Vigilanza ha la possibilità di avvalersi di consulenti esterni ai quali delegare circoscritti ambiti di indagine. In tale caso i detti consulenti saranno nominati dall'Organismo di Vigilanza in piena autonomia ed avranno rapporti diretti esclusivamente con l'Organismo di Vigilanza medesimo.

La revoca dell'Organismo di Vigilanza, di competenza del CdA, o di alcuno dei suoi membri, ovvero dei poteri loro attribuiti nell'ambito della relativa carica, può avvenire soltanto per una giusta causa, intendendo con ciò una grave negligenza nell'assolvimento dei compiti connessi con l'incarico.

7.3. Compiti dell'Organismo di Vigilanza ai sensi degli artt. 6 e 7 D. Lgs. 231/01

L'Organismo opera secondo quanto definito nello specifico Regolamento dell'Organismo di Vigilanza, (allegato 03). In linea generale, le attività che l'organismo è chiamato ad assolvere sono le seguenti:

a) **vigilanza sull'***effettività* **del modello**, che si sostanzia nella verifica della coerenza tra i comportamenti concreti ed il modello istituito;
b) **disamina in merito all'***adeguatezza* **del modello**, ossia della sua reale capacità di prevenire, in linea di massima, i comportamenti non voluti;
c) analisi circa il *mantenimento* **nel tempo** dei requisiti di solidità e funzionalità del modello;
d) cura dell' *aggiornamento* **del modello**, nell'ipotesi in cui le analisi operate rendano necessario effettuare correzioni per garantire che il modello si mantenga "adeguato" nel tempo.
e) **segnalazione** all'organo dirigente, per gli opportuni provvedimenti, di quelle *violazioni accertate del modello organizzativo* che possano comportare l'insorgere di una responsabilità in capo all'ente.

L'Organismo di Vigilanza ha libero accesso presso tutte le funzioni di Equasoft – senza necessità di alcun consenso preventivo – onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei propri compiti, fermo restando il dovere di osservare il divieto di comunicare e/o diffondere le informazioni e/o dati acquisiti, salvo il caso in cui la comunicazione e/o la diffusione siano richieste dalle forze dell'ordine, dall'autorità giudiziaria, da organismi di sicurezza o da altri

soggetti pubblici per finalità di difesa o sicurezza dello stato o di prevenzione, accertamento o repressione di reato. Fatto salvo in ogni caso il divieto di diffusione dei dati sensibili. Le attività poste in essere dall'Organismo, se conformi all'incarico ricevuto, non possono essere sindacate da alcun altro organismo o struttura aziendale, fermo restando però che l'Organo Amministrativo è in ogni caso chiamato a svolgere un'attività di vigilanza sull'adeguatezza del suo intervento, in quanto all'Organo Amministrativo compete la responsabilità ultima del funzionamento (e dell'efficacia) del Modello Organizzativo.

7.4. Reporting dell'Organismo di Vigilanza

L'OdV riferisce in merito all'attuazione del modello ed al suo sviluppo:

- su base continuativa alla Direzione dell'ente;
- su base periodica e almeno annualmente, al Consiglio di Amministrazione ed al Collegio Sindacale.

In particolare l'OdV informa i suddetti organi sullo stato di attuazione del Modello, evidenziando le attività di verifica e di controllo compiute, l'esito di dette attività, le eventuali lacune emerse, i suggerimenti per le eventuali azioni da intraprendere propone le modifiche ed integrazioni di volta in volta ritenute necessarie.

L'OdV potrà chiedere di essere sentito dal Consiglio di Amministrazione ogni qualvolta ritenga opportuno per riferire specifici fatti o accadimenti inerenti il funzionamento e l'efficace attuazione del Modello. L'OdV potrà, a sua volta, essere convocato in ogni momento dal Consiglio di Amministrazione e dagli altri Organi Sociali per riferire su particolari eventi o situazioni relative al funzionamento e al rispetto del Modello.

Il ruolo di vigilanza dovrà ordinariamente espletarsi attraverso la messa in atto di riunioni, almeno ogni 6 mesi, nel corso delle quali l'organismo procederà a riscontrare il rispetto delle procedure previste dal modello. All'esito di tali riunioni dovrà essere redatta apposita relazione informativa da presentare al C.d.A. e al Collegio Sindacale.

Alla chiusura di ciascun esercizio finanziario dovrà essere redatta la relazione illustrativa annuale riguardo l'attività svolta da presentare al C.d.A. e al Collegio Sindacale.

7.5. Obblighi di informazione e segnalazione

In conformità a quanto previsto dal secondo comma dell'art. 6 del D. Lgs. 231/2001 sono adottati nei confronti dell'Organismo di Vigilanza dei flussi informativi per agevolare l'attività di vigilanza sull'efficacia del Modello e di accertamento delle cause che possono rendere o hanno reso possibile il verificarsi delle ipotesi rilevanti ai fini di cui si tratta. Dipendenti, dirigenti, amministratori

e collaboratori a diverso titolo, hanno l'obbligo di riferire all'organismo di vigilanza notizie rilevanti e relative alla vita dell'ente, a violazioni del modello o alla consumazione di reati attraverso i seguenti canali:

- trasmissione di atti ufficiali attinenti alle tematiche di cui al DL 231 da parte dei diversi organismi e funzioni, quali delibere del CdA, rapporti di audit interni ed esterni, reclami, esiti dei monitoraggi interni.
- Invio di comunicazioni specifiche attraverso qualsiasi forma per segnalare comportamenti ritenuti non idonei.
- Richiesta di colloquio.

Allo scopo di agevolare il flusso di comunicazioni con l'OdV sono resi pubblici i nomi dei membri dell'Organismo e le modalità attraverso le quali contattarli.

L'Organismo di Vigilanza valuta le segnalazioni ricevute e gli eventuali provvedimenti conseguenti a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere ad un'indagine interna. L'O.d.V. agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

8. SEGNALAZIONE DEGLI ILLECITI. TUTELA DELL'INFORMATORE (WHISTLEBLOWING POLICY)

Il presente paragrafo appresta disposizioni:

a. volte a codificare la modalità di trasmissione all'Azienda di segnalazioni di condotte illecite (tentate o consumate) rilevanti ai sensi del presente Modello organizzativo;
b. a tutela del dipendente/collaboratore (altrimenti detto informatore o whistleblower) che quelle segnalazioni trasmetta all'Azienda;
c. sulla responsabilità del whistleblower;
d. sulle sanzioni.

8.1. Segnalazione di illeciti

8.1.1. Oggetto della segnalazione

Oggetto della segnalazione sono le condotte illecite di cui il whistleblower sia venuto a conoscenza in ragione del rapporto di lavoro o collaborazione.

Le condotte illecite oggetto delle segnalazioni meritevoli di tutela comprendono non solo l'intera gamma dei reati presupposto di cui al Dlgs 231/2001 ed, in particolare, quelli contemplati dal presente modello ma, altresì, qualsiasi comportamento penalisticamente illecito oppure anche non conforme ai regolamenti interni aziendali.

8.1.2. Contenuto della segnalazione

Affinché la segnalazione possa essere presa in considerazione, il contenuto della stessa dovrà essere adeguatamente circostanziato e fornito - possibilmente - dei dovuti riferimenti/elementi di riscontro. Si precisa che non saranno prese in considerazione le segnalazioni fondate su meri sospetti o voci.

Segnatamente appare opportuno che la segnalazione sia circostanziata delle seguenti informazioni:

- identità del soggetto che effettua la segnalazione, con indicazione di qualifica/funzione/ruolo;
- chiara e completa descrizione dei fatti oggetto di segnalazione;
- circostanze di tempo e di luogo in cui i fatti sono stati commessi;
- generalità o altri elementi che consentano di identificare il soggetto che ha posto in essere i fatti segnalati;
- eventuali ulteriori soggetti che possano riferire sui fatti oggetto di segnalazione;
- eventuali documenti che possano confermare l'effettività dei fatti segnalati;
- ogni ulteriore informazione che si ritenga utile

8.1.3. Soggetti destinatari della segnalazione e modalità di segnalazione

La segnalazione dovrà essere inoltrata mediante email all'indirizzo di posta elettronica dedicata facente capo all'Organismo di Vigilanza (ovvero al diverso indirizzo, sempre dell'OdV, che la Società provvederà a rendere noto).

8.1.4. Verifica della fondatezza della segnalazione

L'Organismo di Vigilanza provvederà ad effettuare una valutazione completa circa la fondatezza delle circostanze rappresentante dal whistleblower nella segnalazione nel rispetto dei principi di imparzialità e riservatezza.

A tal fine, potrà essere richiesta l'audizione personale del segnalante e di eventuali altri soggetti che possano riferire sui fatti segnalati.

Di tali incontri verrà tenuto riscontro verbale, garantendosi peraltro la totale riservatezza e confidenzialità delle informazioni raccolte e dei soggetti interpellati.

Qualora dall'esito della verifica la segnalazione risultasse non manifestamente infondata, l'OdV provvederà a:

a. inoltrare la segnalazione all'Autorità giudiziaria competente in caso di rilevanza penale dei fatti;
b. trasmettere la segnalazione alle funzioni aziendali interessate, per l'acquisizione di elementi istruttori (solamente per le segnalazioni i cui fatti rappresentati non integrano ipotesi di reato);
c. trasmettere la segnalazione al Consiglio di Amministrazione;
d. inoltrare la segnalazione alle funzioni competenti per i profili di responsabilità disciplinare, se esistenti.

L'OdV trasmetterà la segnalazione ai soggetti, così come sopra indicati, priva di tutte quelle informazioni/dati da cui sia possibile desumere l'identità del segnalante, fermo restando che tutti i soggetti che vengano a conoscenza della segnalazione sono tenuti alla riservatezza e all'obbligo di non divulgare quanto venuto a loro conoscenza, se non nell'ambito delle eventuali indagini giudiziarie.

L'OdV evidenzierà, qualora la segnalazione sia trasmessa a soggetti esterni, che si tratta di una segnalazione pervenuta da un soggetto al quale l'ordinamento riconosce una tutela rafforzata della riservatezza.

8.2. Tutela del whistleblower

L'identità del whistleblower verrà protetta sia in fase di acquisizione della segnalazione che in ogni contesto successivo alla stessa, ad eccezione dei casi in cui l'identità debba essere rilevata per legge (es. indagini penali, tributarie o amministrative).

L'identità del whisleblower potrà essere rivelata ai soggetti responsabili della gestione del procedimento disciplinare e all'incolpato solo nei seguenti casi:

consenso espresso esteso per iscritto del segnalante;

la contestazione dell'addebito disciplinare si palesi come fondata e la conoscenza dell'identità del segnalante risulti indispensabile alla difesa dell'incolpato.

Tutti i soggetti che ricevono o sono coinvolti nella gestione della segnalazione sono tenuti a tutelare la riservatezza dell'identità del segnalante.

Nei confronti del dipendente che effettua una segnalazione non è consentita, né tollerata alcuna forma di ritorsione o misura discriminatoria (es. azioni disciplinari ingiustificate, molestie sul luogo di lavoro ed ogni altra forma di ritorsione) diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati, direttamente o indirettamente, alla denuncia.

Il soggetto che ritiene di aver subito una discriminazione per il fatto di aver effettuato una segnalazione di illecito deve dare notizia circostanziata dell'avvenuta discriminazione all'OdV che, condotta tempestivamente attività di verifica, potrà segnalare la circostanza a) al Responsabile dell'Ufficio di appartenenza del dipendente affinché siano tempestivamente adottati gli atti o i provvedimenti per ripristinare la corretta situazione e/o per rimediare agli effetti negativi della discriminazione e la sussitenza degli estremi per avviare il procedimento disciplinare nei confronti del dipendente autore della discriminazione; al Consiglio di amministrazione, qualora l'autore della discriminazione sia un Dirigente della Società c) alla Procura della Repubblica, qualora si siano verificati fatti penalmente rilevanti.

8.3. Responsabilità del whistleblower.

La presente procedura non tutela il whistleblower in caso di segnalazione calunniosa o diffamatoria o comunque dolosa (es. segnalazione effettuata al solo scopo di danneggiare il denunciato).

Ugualmente saranno passibili di sanzioni i soggetti che - intervenuti per qualsiasi ragione nel procedimento - agiscano per le finalità quivi sopra indicate.

8.4. Sanzioni.

Sono sanzionabili le seguenti condotte:

- violazioni delle misure di tutela del segnalante, come sopra segnalate;

- effettuazione, con dolo o colpa grave, di segnalazioni infondate.

La disciplina sanzionatoria e il relativo procedimento è quella individuata per le violazioni del modello, cui si rinvia.

9. SISTEMA SANZIONATORIO

9.1. Principi generali

Un aspetto molto importante è costituito dalla predisposizione di un adeguato "**sistema sanzionatorio"** per la violazione del Modello di Equasoft. La definizione di tale sistema sanzionatorio costituisce, infatti, ai sensi dell'art. 6 primo comma lettera e) del D.Lgs. 231/2001, un requisito essenziale del Modello medesimo ai fini dell'esimente rispetto alla responsabilità dell'ente.

La predisposizione di un sistema disciplinare idoneo ad irrogare sanzioni (commisurate alla violazione e dotate di deterrenza) applicabili in caso di violazione delle regole di cui al presente Modello, delle procedure e dei protocolli ad esso correlati, rende efficiente l'azione di vigilanza dell'O.d.V. ed ha lo scopo di garantire l'effettività del Modello stesso.

L'applicazione del sistema sanzionatorio presuppone la semplice violazione delle disposizioni del Modello, ed anzi, nasce proprio al fine di contrastare comportamenti prodromici al reato e non comportamenti già di per sé costituenti reato e per i quali le sanzioni sono poste in essere dalla magistratura. Pertanto l'applicazione del meccanismo sanzionatorio verrà attivata indipendentemente dallo svolgimento e dall'esito del procedimento penale, eventualmente avviato dall'autorità giudiziaria, nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del D.Lgs. 231/2001.

L'apparato disciplinare opera quindi come presidio interno dell'Ente al fine di prevenire l'applicazione di sanzioni da parte dello Stato, rendendo efficiente l'azione dell'OdV e garantendo l'effettiva attuazione del Modello.

Con l'approvazione del presente Modello, Equasoft non ha inteso stabilire un autonomo sistema sanzionatorio, in quanto esso risulta già definito dagli istituti legislativi vigenti (Statuto dei lavoratori, Codice Civile, norme legislative cogenti), dagli impegni contrattuali e dalle norme deontologiche di categoria.

Pertanto, le sanzioni che saranno erogate in caso di violazione delle regole di cui al presente Modello debbono ritenersi quelle previste dalle disposizioni del codice civile e dal Contratto Collettivo Nazionale di Lavoro applicabile ed in vigore.

È tuttavia da assumere che l'infrazione alle regole stabilite con il presente Modello costituisca evidenza o circostanza aggravante, punibile ai sensi della legislazione vigente e delle norme di diritto che regolano i rapporti di collaborazione diretta ed indiretta.

9.2. Indicazioni generali sul sistema disciplinare

Il quadro sanzionatorio prevede:

- sistema disciplinare rispetto ai sottoposti;
- sistema disciplinare relativo ai soggetti apicali;
- sistema disciplinare relativo ai collaboratori e ai terzi.

Il sistema disciplinare distingue inoltre la violazione posta in essere da un collaboratore dipendente rispetto a quella commessa da collaboratori esterni. Essendo questi ultimi connotati dalla mancata sottoposizione al potere disciplinare, sono previste clausole contrattuali che impongono il rispetto del modello e del codice etico e che ne sanzionano le violazioni, anche con la risoluzione del contratto nei casi più gravi.

Le sanzioni previste sono graduate in ragione della gravità delle violazioni accertate e prendono spunto anche dal contratto nazionale di riferimento.
La funzione deputata a valutare e disporre i provvedimenti disciplinari per violazioni del Codice Etico e/o del Modello è esclusivamente il CdA, eventualmente su proposta della Direzione o dell' Organismo di vigilanza.

10. DIFFUSIONE DEL MODELLO E FORMAZIONE DELLE RISORSE

EQUASOFT opera affinché il modello e le sue regole di funzionamento siano adeguatamente portate a conoscenza di tutti i portatori di interesse, con ciò intendendo tutti coloro che operano per EQUASOFT e cioè i soci, i dipendenti, i componenti del Consiglio di Amministrazione e del Collegio Sindacale, nonché i collaboratori interni ed esterni che contribuiscono al conseguimento degli obiettivi della Azienda.

Tale diffusione riguarda tutti i soggetti sopra evidenziati con un livello di approfondimento che varia a seconda del ruolo e delle competenze attribuite agli stessi. Tutto il personale è stato informato in merito alla implementazione del Modello Organizzativo ed ha accesso alla relativa documentazione.

Sono pianificati interventi formativi e di aggiornamento su base annuale. In tali programmi sono inclusi anche momenti di formazione e informazione in merito al Modello Organizzativo. Gli interventi formativi sono registrati.

Dell'attività informativa eseguita viene tempestivamente relazionato l'Organismo di Vigilanza.

11. DOCUMENTI DI RIFERIMENTO.

I documenti utilizzati per la corretta gestione del modello sono inseriti nel più vasto sistema documentale aziendale.
Tutti i documenti sono codificati e muniti di numero di revisione al fine di garantire l'utilizzo delle versioni più recenti.
I documenti specifici richiamati dal modello sono:

1) ***Catalogo dei reati-presupposto***
2) ***Matrice Reati – Processi***
3) ***Codice etico***
4) ***Regolamento dell'Organismo di Vigilanza***

12. ELENCO DELLE MODIFICHE

Rev. 0	30/11/2016	Prima emissione
Rev. 1	__/__/2019	

MODELLO
DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D.Lgs. 231/2001
- Parte speciale

INDICE

PARTE SPECIALE 1 – Reati nei rapporti con la Pubblica Amministrazione

1. Le fattispecie di reato nei rapporti con la P.A. (artt. 24-25 d.lgs. 231/2001)

In considerazione dell'analisi dei rischi effettuata, sono risultati concretamente realizzabili nel contesto aziendale di EUQASOFT, nell'ambito dei rapporti tra società e P.A., i seguenti reati, brevemente descritti:

- Malversazione a danno dello Stato o di altro ente pubblico (art. 316-bis c.p.)

Il reato in oggetto viene commesso qualora contributi, sovvenzioni o finanziamenti concessi dallo stato, da un ente pubblico o dall'Unione Europea, destinati alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non vengano destinati dal soggetto percettore alle predette finalità. Scopo della norma è quello di reprimere le frodi successive all'ottenimento di prestazioni pubbliche aventi un interesse generale il quale risulterebbe vanificato qualora il vincolo di destinazione venisse eluso.

- Indebita percezione di erogazioni a danno dello Stato o della UE (art. 316-ter c.p.)

Tale ipotesi di reato si configura nei casi in cui, mediante l'utilizzo e la presentazione di falsi documenti e dichiarazioni o mediante l'omissione di informazioni dovute, si ottengano contributi, finanziamenti, mutui agevolati o altre erogazioni, per se o per altri senza averne diritto, concessi dallo Stato, da altri enti pubblici o dall'Unione Europea. Tale reato può essere commesso in concorso con quello di cui al punto precedente, in quanto in tal caso non rileva il corretto utilizzo delle erogazioni.
Rispetto all'ipotesi della truffa, questa ha carattere residuale e si applica quando, ad esempio, non è provata la attuazione di raggiri o artifizi.

- Corruzione per l'esercizio della funzione (art. 318 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, 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. E' il caso, per esempio, in cui il pubblico funzionario accetta dazioni di denaro o la loro promessa al fine di accelerare il rilascio di una pratica ovvero di farle seguire un iter preferenziale rispetto al normale.

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

A differenza del reato previsto dall'art. 318 in precedenza esaminato si tratta in questo caso del compimento da parte del pubblico ufficiale, dietro corresponsione di denaro o altra utilità, di un atto

non dovuto anche se formalmente regolare quindi contrario ai principi di buon andamento e imparzialità della Pubblica Amministrazione.

- Corruzione in atti giudiziari (art. 319-ter c.p.)

Questa fattispecie si realizza nel caso di comportamenti finalizzati alla corruzione commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo.

- Truffa in danno dello Stato, di altro ente pubblico o della UE (art. 640, comma 2, nr. 1 c.p.)

Commette il reato in oggetto chiunque con artifizi o raggiri induca in errore l'ente pubblico (Stato o UE) allo scopo di procurare a sé o ad altri un ingiusto profitto con altrui danno. L'attività attraverso la quale si realizza il reato di truffa consiste in qualunque comportamento che tragga in errore lo Stato o l'ente pubblico che deve effettuare l'atto di disposizione patrimoniale.

- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)

Il reato in oggetto si verifica allorquando i fatti di cui al precedente art. 640 c.p. riguardano l'ottenimento di contributi, finanziamenti, mutui agevolati o altre erogazioni concessi dallo Stato, da altri enti pubblici o dalle Comunità Europee. L'elemento specializzante rispetto al reato di truffa, ex art. 640 c.p. è costituito dall'oggetto materiale della frode, dove per erogazione pubblica si intende ogni attribuzione economica agevolata erogata da parte dello Stato, di altri enti pubblici o delle Comunità Europee

- Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)

Si configura tale reato quando al fine di procurare a sé o ad altro un ingiusto profitto venga alterato in qualsiasi modo il funzionamento di un sistema informatico o si intervenga senza diritto su dati, informazioni o programmi contenuti in un sistema informatico.

- Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)

Questa fattispecie si realizza quando un Pubblico Ufficiale o l'incaricato di un Pubblico Servizio induce taluno a dare o promettere indebitamente, a lui o ad un terzo, denaro o altra utilità. La norma sanzione anche colui che da o promette utilità.

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

Si tratta dei medesimi reati di corruzione sopra indicati, ma si verifica quando l'offerta è rifiutata dal pubblico ufficiale. In tale ipotesi è punito solo il privato.

- Concussione (art. 317 c.p.)

Siamo in presenza di un reato specifico del funzionario pubblico che, abusando della sua qualità e dei suoi poteri, costringe un soggetto privato a dare, a lui terzi, denaro o altre utilità. Nel reato di concussione decisiva è la preminenza prevaricatrice esercitata dal pubblico ufficiale sulla controparte privata per creare o insinuare nel soggetto passivo uno stato di timore atto a eliderne la volontà. Nella concussione il privato è spinto ad assecondare la richiesta del funzionario pubblico al fine di evitare un danno ingiusto derivante altrimenti dall'atteggiamento sfavorevole dello stesso mentre, al contrario, nella corruzione la condotta del privato è animata dall'intento di realizzare un ingiusto vantaggio ai danni della Pubblica Amministrazione. Questo reato si distingue dalla corruzione perché non si è in presenza di un accordo tra il privato ed il pubblico ufficiale, ma quest'ultimo, abusando della sua posizione, costringe il privato a procurare a sé o ad altri denaro o altra utilità.

2. Aree di attività a rischio

Nell'ambito dei possibili rapporti con la P.A., considerato che EQUASOFT è un ente di formazione e consulenza, specializzato nello sviluppo delle risorse umane, e si dedica altresì alla certificazione dei percorsi, all'assistenza pre e post formazione e agli accreditamenti, essendo Organismo di Formazione accreditato dalla Regione Veneto, si possono individuare le seguenti tipologie di attività a rischio:

- Gestione dei rapporti con la PA di carattere generale, quali esemplificativamente:
    - Gestione degli adempimenti in materia tributaria;
    - Gestione degli adempimenti in materia di salute, sicurezza, igiene;
    - Gestione delle ispezioni;
- Gestione dei rapporti con le Autorità di Vigilanza;
- Gestione e concessione di omaggi e liberalità;
- Gestione della tesoreria;
- Gestione di rimborsi spese a dipendenti e collaboratori
- Gestione di finanziamenti, contributi ed erogazioni;
- Approvvigionamento di beni, servizi e prestazioni;
- Gestione dell'erogazione del corso dalla progettazione e presentazione della richiesta di finanziamento, alla raccolta delle adesioni, fino alla chiusura e rendicontazione;
- Gestione dell'assunzione del personale.

3. Regole di carattere generale

Le seguenti regole di carattere generale si applicano agli organi sociali, ai dirigenti e ai dipendenti di EQUASOFT in via diretta, nonché ai consulenti, fornitori e partner in forza di apposite clausole

contrattuali. A tali soggetti è fatto divieto di porre in essere, concorrere o dare causa alla realizzazione di comportamenti tali da integrare, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra elencate.
Tutte le attività dell'azienda nelle aree a rischio sono svolte conformandosi alle leggi vigenti, alle norme del Codice Etico e seguendo i principi, le procedure ed i protocolli aziendali di cui al presente Modello.
In particolare, è fatto divieto di:

- Effettuare elargizioni in denaro a pubblici funzionari italiani o stranieri;
- Promettere o versare somme o beni in natura a qualsiasi soggetto, ovvero ricorrere a forme diverse di aiuti o contribuzioni nonché accordare vantaggi di qualsiasi natura in favore di rappresentanti della P.A., al fine di promuovere o favorire gli interessi della società;
- Selezionare personale o favorire l'avanzamento di carriera o il riconoscimento di premi non ispirandosi a criteri meritocratici od oggettivi;
- Presentare dichiarazioni non veritiere ad organismi pubblici al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- Destinare somme ricevute da organismi pubblici per scopi diversi da quelli cui erano destinati;
- Alterare e/o utilizzare abusivamente e in modo improprio i sistemi informatici aziendali.

4. Regole specifiche di condotta

Ad integrazione del Codice Etico, sono state formalizzate specifiche procedure e norme aziendali. Le procedure aziendali sono caratterizzate dalla separazione dei ruoli di impulso decisionale, di esecuzione e realizzazione, nonché di controllo, con adeguata formalizzazione e supporto documentale delle fasi principali del processo.

L'Azienda regola la propria politica retributiva e di carriera tenendo in debita considerazione la correttezza e legalità dei comportamenti, offrendo pari opportunità a tutti i dipendenti, sulla base delle loro qualifiche e capacità individuali senza alcuna forma di discriminazione, penalizzando ogni comportamento che tenda al raggiungimento di obiettivi a discapito del rispetto delle regole aziendali o legali.

Qualsiasi rapporto con funzionari pubblici è improntato alla massima trasparenza, correttezza e legalità, nonché documentabile ed attento alle molteplici implicazioni che da esso possono derivare.

5. Controlli dell'organismo di vigilanza

L’Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività connesse alle attività a rischio al fine di verificare la corretta esplicazione delle stesse in relazione alle regole del Modello. A tal fine, per ciascuna operazione a rischio, il Responsabile Interno, deve:

- informare l’O.d.V. in merito all’inizio ed alla chiusura di ogni Operazione a Rischio;
- tenere a disposizione dell’O.d.V. la sottostante documentazione di supporto;
- segnalare all’O.d.V. e richiedere la sua assistenza per ogni situazione che si ritenga non conforme alle regole aziendali in materia.

L’Organismo di Vigilanza dovrà evitare, per quanto possibile, di interferire con i processi decisionali aziendali, ma dovrà intervenire prontamente con gli strumenti a sua disposizione per prevenire e, se del caso, reprimere, ogni comportamento che sia in contrasto con le regole aziendali.

L’Organismo di Vigilanza ha accesso, per i fini della attività ad esso attribuita, ad ogni documentazione aziendale che esso ritenga rilevante per la prevenzione e repressione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello, fermo restando il dovere di osservare il divieto di comunicare e/o diffondere le informazioni e/o dati acquisiti, salvo il caso in cui la comunicazione e/o la diffusione siano richieste da forze di polizia, dall’autorità giudiziaria, da organismi di sicurezza o da altri soggetti pubblici per finalità di difesa o sicurezza dello stato o di prevenzione, accertamento o repressione di reato. Fatto salvo in ogni caso il divieto di diffusione dei dati sensibili.

PARTE SPECIALE 2 – Delitti informatici e trattamento illecito di dati

1. Le fattispecie di reato di delitto informatico e trattamento illecito di dati (art. 24-bis d.lgs. 231/2001)

In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente realizzabili, nel contesto aziendale di EQUASOFT, i seguenti reati:

- Falsità in documenti informatici pubblici aventi efficacia probatoria (art. 491-bis cp in relazione agli artt. 476, 477, 478,479, 480, 481, 482, 483, 484, 487, 488, 489, 490, 492 e 493 cp)

Tale norma estende le sanzioni previste per la falsità degli atti pubblici e privati alle falsità riguardanti un documento informatico pubblico o privato avente efficacia probatoria.

- Accesso abusivo ad un sistema informatico o telematico (art. 625-ter cp)

Tale fattispecie di reato punisce l'accesso non autorizzato ad un sistema informatico o telematico altrui, protetto da misure di sicurezza interna. Il reato è aggravato se commesso da un soggetto che abusa della sua qualità di operatore del sistema informatico o telematico.

- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater cp)

La norma in esame punisce la condotta di chi si procura illecitamente codici, parole chiave o altri mezzi idonei ad accedere ad un sistema informatico o telematico protetto da misure di sicurezza. È sanzionata anche l'attività di diffusione, comunicazione o consegna a terzi dei predetti codici, nonché di comunicazione di indicazioni o istruzioni idonee a tale scopo.

- Diffusione di apparecchiature, dispositivi o programmi informativi diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies cp)

Tale ipotesi di reato ha ad oggetto le condotte abusive che si sostanziano nella diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.

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

Nel reato in oggetto rientra l'attività di chi distrugge, deteriora o rende inservibili sistemi informatici o telematici altrui, indipendentemente se ciò avvenga per trarre profitto o semplicemente per "vandalismo informatico".

- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635-ter cp)

La norma in questione punisce al primo comma le condotte prodromiche e preparatorie al danneggiamento di informazioni, dati e programmi informatici di cui all'articolo precedente, riguardanti informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o, comunque, di pubblica utilità. La concreta realizzazione del danno, invece, integra un'autonoma ipotesi di reato, sanzionata dal comma 2.

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

Ad essere sanzionata è la condotta di chi, tramite la distruzione, la cancellazione, il deterioramento o alterazione di dati o programmi informatici, o mediante l'introduzione abusiva nel sistema informatico, distrugge, cancella, deteriora o altera sistemi informatici o telematici altrui.
La norma punisce dunque più duramente il colpevole della fattispecie di cui all'art. 635 bis, qualora ne derivi una compromissione irreversibile di un sistema informatico, e non di semplici dati o informazioni.

- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies cp)

Tale fattispecie di reato punisce i fatti di danneggiamento previsti dall'art. 635-quater, riguardanti i sistemi informatici o telematici di pubblica utilità.

- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies cp)

L'ipotesi di reato punisce la frode informatica commessa esclusivamente dal soggetto che presta servizi di certificazione di firma elettronica ovvero fornisce altri servizi connessi con quest'ultimo. La condotta punita consiste nella violazione degli obblighi di controllo e garanzia previsti dal D.Lgs. 82/2005 per il rilascio di un certificato.

2. Aree di attività a rischio

Con riferimento ai delitti informatici di trattamento illecito di dati previsti dall'art.24-bis, le principali attività ritenute più specificamente a rischio sono le seguenti:

- Gestione dei sistemi informativi aziendali;
- Sicurezza logica dei sistemi;
- Gestione degli incidenti;
- Misure per la sicurezza delle reti di trasmissione;
- Gestione dell'ambiente fisico;

- Gestione dell'erogazione del corso dalla progettazione e presentazione della richiesta di finanziamento, alla raccolta delle adesioni, fino alla chiusura e rendicontazione.

3. Regole di carattere generale

Le seguenti regole di carattere generale si applicano a tutti i soggetti aziendali coinvolti a vario titolo nella gestione o nell'utilizzo dei sistemi informativi aziendali, nonché a tutti i dipendenti, collaboratori, fornitori che abbiano accesso fisico o logico ai sistemi informativi di Equasoft. A tali soggetti è fatto divieto di:

- Porre in essere condotte miranti all'accesso ai sistemi informatici altrui al fine di tenere condotte abusive e/o illecite
- Porre in essere condotte miranti alla distruzione o all'alterazione dei documenti informatici aventi finalità probatoria;
- Utilizzare o installare programmi diversi da quelli autorizzati;
- Aggirare o tentare di aggirare i meccanismi di sicurezza aziendale;
- Lasciare il proprio PC sbloccato e incustodito;
- Rivelare ad alcuno le proprie credenziali di autenticazione;
- Detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- Entrare nella rete aziendale e nei programmi con un codice diverso da quello assegnato

Gli operatori del sistema informatico di Equasoft verificano la sicurezza della rete e dei sistemi informativi aziendali; identificano le potenziali vulnerabilità nel sistema dei controlli IT e vigilano sulla corretta applicazione di tutti gli accorgimenti necessari per fronteggiare i delitti informatici e di trattamento dei dati.
Equasoft si attiva per monitorare il corretto utilizzo degli accesi ai sistemi informativi di terze parti.

Tutti i soggetti sopra indicati, per le attività di rispettiva competenza, devono:

- Utilizzare gli strumenti aziendali nel rispetto delle policy e procedure aziendali;
- Verificare periodicamente le credenziali utente ed assicurare l'aggiornamento delle password dei singoli utenti;
- Non consentire l'accesso alle aree riservate a persone che non dispongono di idonea autorizzazione;
- Limitare la navigazione in internet e l'uso della posta elettronica per le sole attività lavorative;
- Rispettare i principi e le regole aziendali al fine di tutelare la sicurezza dei dati ed il corretto accesso ai sistemi applicativi ed informatici.

4. Regole specifiche di condotta

Ad integrazione del Codice Etico, sono state formalizzate specifiche procedure e norme aziendali aventi ad oggetto: la sicurezza informatica, la gestione degli accessi e dei profili utente, le modalità di utilizzo dei sistemi e delle dotazioni informatiche, le modalità di gestione dei dati personali.

Equasoft ha inoltre definito le misure di sicurezza delle reti aziendali e di trasmissione e le procedure per garantire la continuità di servizio.

Nello svolgimento delle attività a rischio, tutti i Destinatari del Modello devono tenere un comportamento corretto e trasparente, in conformità a quanto disposto dalle previsioni legislative, dal Codice Etico e dalle procedure sopra richiamate.

5. Controlli dell'organismo di vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle operazioni a rischio al fine di verificare la corretta esplicazione delle stesse in relazione alle regole del Modello. A tal fine esso ha autonomi poteri di iniziativa e controllo e libero accesso a tutta la documentazione aziendale; può intervenire anche a seguito di informazioni e segnalazioni ricevute.

PARTE SPECIALE 3 – Reati societari e di abuso di mercato

1. Le fattispecie di reati societari e di abuso di mercato (artt. 25-ter e 25-sexies d.lgs. 231/2001)

- False comunicazioni sociali (art. 2621 e 2621-bis cc);

La condotta sanzionata consiste nell'esporre consapevolmente fatti materiali rilevanti non rispondenti al vero od omettere consapevolmente fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo concretamente idoneo a indurre altri in errore, al fine di conseguire per sé o per altri un ingiusto profitto.

- Impedito controllo (art. 2625 cc)

Questa fattispecie di reato si realizza quando gli amministratori, occultando i documenti o con altri idonei artifici, impediscono o ostacolano lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali o alle società di revisione. La finalità perseguita dal presente articolo è quella di garantire, sanzionando i comportamenti ostativi degli amministratori, il controllo sia interno che esterno della società.
Soggetti attivi del reato possono essere esclusivamente gli amministratori.
Il dolo è generico, e consiste nella coscienza e volontà di impedire il controllo sulla società.

- Indebita restituzione dei conferimenti (art. 2626 cc)

La condotta rilevante è costituita dalla restituzione effettiva o simulata dei conferimenti ai soci, o dalla liberazione dall'obbligo di eseguire detti conferimenti, al di fuori delle ipotesi in cui è espressamente permesso.
La finalità di tale articolo è da rinvenire nell'esigenza di garantire l'effettività del capitale sociale.
Soggetti attivi del reato sono esclusivamente gli amministratori.
Il dolo è generico e consiste nella cosciente e volontaria restituzione, reale o fittizia, dei conferimenti o nella liberazione dall'obbligo degli stessi al di fuori dei casi espressamente previsti dalla legge.

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

Questa ipotesi di reato si realizza quando gli amministratori ripartiscono utili o acconti sugli utili fittizi o destinati per legge a riserva, in violazione dei limiti legali di distribuzione, o ripartiscono riserve legali non distribuibili.
La finalità perseguita dalla norma è quella di impedire la distribuzione di utili fittizi.
Soggetti attivi del reato sono gli amministratori. Occorre, tuttavia, precisare, che non avendo gli amministratori il potere diretto di porre in essere dette distribuzioni o ripartizioni di utili prescindendo

da apposite deliberazioni assembleari in merito, la condotta integrante il reato sembra sussistere anche nel caso in cui gli amministratori, pur senza procedere direttamente alla distribuzione o alla ripartizione, pongano in essere delle rappresentazioni contabili sulla base delle quali l'assemblea deliberi detta distribuzione o ripartizione, pur in assenza delle condizioni oggettive che lo consentirebbero. Il dolo è generico e consiste nella coscienza e volontà dì effettuare la distribuzione o la ripartizione al di fuori dei limiti posti dalla legge.
La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, estingue il reato.

- Operazioni in pregiudizio dei creditori - Art. 2629 c.c.

Questa fattispecie si realizza quando gli amministratori, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzione del capitale sociale, fusioni con altre società o scissioni, cagionando danno ai creditori. La finalità dell'articolo è quella di impedire operazioni dannose per i creditori sociali. Soggetti attivi del reato possono essere solo gli amministratori. Il dolo è generico e consiste nella coscienza e volontà di attuare le descritte operazioni societarie violando le norme poste a tutela dei creditori sociali.

- Formazione fittizia del capitale (art. 2632 cc)

Questa fattispecie si realizza quando gli amministratori e i soci conferenti formano o aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

- Corruzione tra privati (art. 2635 comma 3 cc)

Rispondono di tale reato gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.

- Istigazione alla corruzione tra privati (art. 2635-bis comma 1 cc)

Ne risponde chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di

funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, qualora l'offerta o la promessa non sia accettata.

- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, cc).

Questa ipotesi di reato si realizza quando gli amministratori, i direttori generali, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle Pubbliche Autorità di Vigilanza o tenuti ad obblighi nei loro confronti, nelle comunicazione alle predette autorità previste per legge, al fine di ostacolare le funzioni di vigilanza, espongono fatti materiali non rispondenti al vero sulla situazione economica, patrimoniale o finanziaria dei sottoposti a vigilanza ovvero occultano con altri mezzi fraudolenti fatti che avrebbero dovuto comunicare concernenti la situazione medesima.

- Abuso di informazioni privilegiate (art. 184 D. Lgs. 58/1998)

Questa fattispecie si realizza quando chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:

a) Acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o di terzi, su strumenti finanziari utilizzando le informazioni medesime;
b) Comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;
c) Raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a).

La fattispecie si realizza anche quando chiunque, essendo in possesso di informazioni privilegiate, a motivo della preparazione o esecuzione di attività delittuose compie taluna delle azioni precedenti.

- Manipolazione del mercato (art. 185 D. Lgs. 58/1998)

Questa ipotesi di reato si realizza quando chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

2. Aree di attività a rischio

Con riferimento ai reati societari previsti dall'art. 25-ter, le principali attività ritenute più specificamente a rischio sono le seguenti:

- Comunicazioni esterne
- Formazione del bilancio, gestione della contabilità e degli adempimenti fiscali
- Gestione della tesoreria

- Gestione delle operazioni sul capitale
- Gestione delle operazioni straordinarie
- Funzionamento degli organismi di controllo
- Comunicazioni all'assemblea e agli organismi di controllo
- Gestione delle informazioni privilegiate
- Gestione del rapporto con le Autorità di Vigilanza
- Gestione dei rapporti e degli adempimenti verso Soci, Sindaci e organismi di controllo
- Gestione dell'erogazione del corso con particolare riguardo alla raccolta delle adesioni, all'erogazione, ai monitoraggi e controlli e alla chiusura e rendicontazione.

3. Regole di carattere generale

Le seguenti regole di carattere generale si applicano agli Amministratori, agli Apicali e ai Preposti alla redazione dei documenti contabili societari, nonché ai Sindaci, alla società di revisione e controllo contabile ed ai soggetti sottoposti a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio.

Obiettivo della presente Parte Speciale è che tutti i destinatari, come sopra individuati, siano precisamente consapevoli della valenza dei comportamenti censurati e che quindi adottino regole di condotta a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti dal Decreto.

In particolare, in coerenza con il Codice Etico e le procedure aziendali, tali soggetti dovranno:

- Tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire una informazione veritiera e completa sulla situazione economica, patrimoniale e finanziaria della realtà aziendale della Società;
- Rispettare le disposizioni di legge, i principi contabili e le regole aziendali, ponendo la massima attenzione, professionalità ed accuratezza, nella acquisizione, elaborazione, valutazione ed illustrazione dei dati e delle informazioni necessarie alla predisposizione del bilancio e delle altre comunicazioni sociali;
- Attivarsi affinchè i fatti di gestione siano rappresentati correttamente e tempestivamente nella contabilità;
- Assicurarsi che ogni operazione sia autorizzata, verificabile, legittima e coerente con la documentazione di supporto;
- Assicurare il rispetto dei principi contabili adottati e la corretta contabilizzazione delle operazioni;

- Applicare adeguate procedure di controllo in caso di sopravvenienze attive apparentemente non giustificate o in caso di registrazioni di incassi (e pagamenti) di cui non si riscontri una contropartita di credito (o debito) corrispondente;
- Effettuare con tempestività, correttezza e buona fede tutte le comunicazioni nei confronti di Autorità di Vigilanza, evitando ogni comportamento che possa risultare di ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate;
- Assicurare il regolare funzionamento degli organi sociali, agevolando e collaborando con il Collegio Sindacale e con la società di revisione;
- Mantenere riservati i documenti e le informazioni acquisiti nello svolgimento dei propri compiti e non comunicare le informazioni privilegiate;
- Osservare scrupolosamente le norme a tutela dei creditori e della integrità ed effettività del capitale sociale.

È altresì fatto divieto di

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi, fuorvianti o, comunque, non rispondenti alla realtà, in particolare sulla situazione economica, patrimoniale e finanziaria della Società;
- omettere dati o informazioni imposti dalla legge e dai regolamenti sulla situazione economica, patrimoniale e finanziaria della Società;
- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o comunque che ostacolino lo svolgimento dell'attività di controllo e di revisione da parte degli Azionisti, del Collegio Sindacale e della società di revisione;
- determinare o influenzare l'assunzione delle deliberazioni dell'Assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare.

4. Regole specifiche di condotta

Ad integrazione dei principi già indicati nel Codice Etico, sono state formalizzate specifiche procedure e norme aziendali aventi ad oggetto: la chiusura delle situazioni contabili annuali e infrannuali, l'approvvigionamento di beni e servizi, le gestione delle informazioni privilegiate, la gestione degli adempimenti verso la P.A. e le autorità di Vigilanza, la gestione della tesoreria.
Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole, protocolli e procedure aziendali già citate, gli organi sociali devono, oltre alla normativa applicabile, conoscere e rispettare:

- il Codice Etico;
- le regole operative di contabilità e finanza nel rispetto delle norme civilistiche e fiscali applicabili;
- la documentazione e le disposizioni inerenti la struttura funzionale aziendale ed organizzativa dell'azienda (organigramma);
- il sistema disciplinare di cui al CCNL;

Inoltre sono previste:

- Informazione e formazione dei soggetti responsabili circa la normativa societaria;
- Diffusione del Codice Etico.

5. Controlli dell'organismo di vigilanza

L'Organismo di Vigilanza potrà discrezionalmente attivarsi con controlli, verifiche ed ispezioni, anche a campione o a seguito di segnalazione, delle fasi di ciascuna Operazione a Rischio. A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo e libero accesso a tutta la documentazione aziendale rilevante per la prevenzione e repressione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello. L'OdV dovrà evitare, per quanto possibile, di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione per prevenire e, se del caso, reprimere, ogni comportamento che sia in contrasto con le regole aziendali.

PARTE SPECIALE 4 – Sicurezza, igiene e prevenzione infortuni

1. Le fattispecie di reati colposi commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies d.lgs. 231/2001)

La legge n. 123 del 3 agosto 2007 ha dettato nuove misure in materia di tutela della salute e della sicurezza sui luoghi di lavoro, il cui articolo 9, modificando il D.Lgs. 231/2001, ha esteso la responsabilità amministrativa degli enti per gli illeciti commessi con la violazione di norme di sicurezza e antinfortunistiche.
Occorre evidenziare che i reati di cui al presente capitolo, a differenza degli altri fin qui previsti dal D.Lgs. 231/2001 e sue modifiche, sono reati di natura colposa e come tali possono essere commessi come conseguenza di una violazione di norme o regolamenti nelle materie della sicurezza, prevenzione ed igiene del lavoro. Per la commissione di tali reati, dunque, non occorre l'elemento soggettivo del dolo, cioè la coscienza e la volontà di cagionare l'evento lesivo, ma basta la mera negligenza, imprudenza o imperizia del soggetto, o una violazione delle disposizioni legali e regolamentari in materia, dalla quale derivi, come conseguenza non voluta, l'infortunio o la malattia comportanti la lesione grave, gravissima o la morte.

- <u>Omicidio colposo (art. 589 cp)</u>

La condotta punita da tale fattispecie di reato si concretizza in quei comportamenti che, violando le norme dettate ai fini della prevenzione degli infortuni sul lavoro e della tutela dell'igiene e della salute sui luoghi di lavoro, cagionano il decesso di una persona.

- <u>Lesioni personali colpose, gravi o gravissime (art. 590 cp)</u>

Il reato si realizza nel caso in cui per colpa si cagionino ad una persona lesioni gravi o gravissime a seguito della violazione delle norme per la prevenzione degli infortuni sul lavoro.
Le lesioni si considerano gravi nel caso in cui:

a) dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;
b) il fatto produce l'indebolimento permanente di un senso o di un organo.

Le lesioni si considerano gravissime se dal fatto deriva:

a) una malattia certamente o probabilmente insanabile;
b) la perdita di un senso;
c) la perdita di un arto o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella;

d) la deformazione o lo sfregio permanente del viso.

2. Aree di attività a rischio

Con riferimento ai reati colposi commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro previsti dall'art. 25-septies, le principali attività ritenute più specificamente a rischio sono le seguenti:

- Gestione degli adempimenti in materia di salute e sicurezza degli impianti e dei luoghi di lavoro

Tutte le aree di attività aziendale ove opera personale dipendente, sono a rischio di commissione dei reati previsti da questo capitolo, pur se con differenti tipologie e gradi di rischio.

3. Regole di carattere generale

Obiettivo del Modello è che tutti i Destinatari adottino e facciano adottare regole di condotta conformi a quanto prescritto dalle norme in materia, incluse quelle regolamentari, al fine di impedire il verificarsi delle violazioni delle disposizioni di cui si tratta e, in conseguenza, dei reati in essa considerati.

In particolare, il Datore di Lavoro e tutti i soggetti aventi compiti, attribuzioni e/o responsabilità nella gestione degli adempimenti previsti dalle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, quali, a titolo esemplificativo Responsabile del Servizio di Prevenzione e Protezione (RSPP), Medico competente, addetti al primo soccorso, addetti emergenze in caso d'incendio etc., ognuno nell'ambito della propria competenza devono garantire:

- La definizione degli obiettivi per la sicurezza e la salute dei lavoratori e l'identificazione continua dei rischi;
- Un adeguato livello di informazione/formazione dei dipendenti e dei fornitori sul sistema di gestione della sicurezza e della salute definito da Equasoft e sulle conseguenze derivanti da un mancato rispetto delle norme di legge e delle regole definite dalla società;
- La definizione e l'aggiornamento di procedure specifiche per la prevenzione di infortuni e malattie, in cui siano disciplinate le modalità di gestione degli incidenti e delle emergenze e dei segnali di rischio/pericolo;
- La manutenzione ordinaria e straordinaria degli strumenti, degli impianti e delle strutture aziendali;
- Rispettare gli obblighi previsti dal D.Lgs. 81/2008, dalla normativa vigente in materia di salute e sicurezza sul lavoro e quanto definito dalla Società al fine di preservare la salute e la sicurezza dei lavoratori;

- Comunicare tempestivamente eventuali segnali di rischio/pericolo e violazioni alle regole di comportamento o alle procedure aziendali.

È inoltre fatto espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-speties D.Lgs. 231/01) o violazioni di principi comportamentali e procedure aziendali.

La Società si impegna a porre in essere le seguenti misure generali di tutela:

- La programmazione e la destinazione di adeguate risorse economiche, umane ed organizzative necessarie per il rispetto delle misure di prevenzione e sicurezza, per la verifica della loro attuazione e per la vigilanza sull'osservanza degli adempimenti prescritti;
- La programmazione dei processi produttivi in modo da ridurre al minimo l'esposizione a rischio dei lavoratori;
- Manutenzione regolare degli ambienti di lavoro, delle attrezzature, delle macchine e degli impianti e programmi di verifica periodica;
- Segnalazione delle vie di esodo, delle uscite di emergenza, dell'attrezzatura di pronto soccorso e dei presidi di sicurezza da apposita segnaletica a norma di legge, al fine di richiamare con immediatezza l'attenzione su situazioni costituenti pericolo o sui comportamenti da adottare per prevenirlo e combatterlo;

4. Regole specifiche di condotta

Ad integrazione del Codice Etico, sono state previste specifiche procedure e norme aziendali aventi ad oggetto il sistema di gestione della sicurezza.
Nello svolgimento delle attività a rischio, tutti i destinatari del Modello e, in particolare, i soggetti aziendali coinvolti nelle aree a rischio, devono tenere un comportamento corretto e trasparente, in conformità a quanto disposto dalle previsioni di legge esistenti in materia, dal Codice Etico e dalle procedure aziendali.

5. Controlli dell'organismo di vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli, verifiche ed ispezioni, anche a campione o a seguito di segnalazione, delle operazioni a rischio al fine di verificare la corretta esplicazione delle stesse. A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo e libero accesso a tutta la documentazione aziendale rilevante che esso ritenga rilevante per la prevenzione e repressione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello. L'OdV dovrà evitare, per quanto possibile, di interferire con i processi

decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione per prevenire e, se del caso, reprimere, ogni comportamento che sia in contrasto con le regole aziendali.

PARTE SPECIALE 5 – Tutela di strumenti e segni di riconoscimento e del diritto d'autore

1. Le fattispecie di reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis d.lgs. 231/2001) e in materia di violazione del diritto d'autore (art. 25-novies d.lgs. 231/2001)

Spendita di monete falsificate ricevute in buona fede (art. 457 cp)

Il reato si configura qualora un soggetto spenda o metta altrimenti in circolazione monete contraffatte o alterate, da lui ricevute in buona fede.

Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 cp)

La condotta criminosa in esame consiste nell'alterare, contraffare o introdurre nel territorio dello Stato, detenere o mettere in circolazione carta bollata, marche da bollo, francobolli contraffatti.

Uso di valori di bollo contraffatti o alterati (art. 464 cp)

Il reato punisce chi, pur non essendo incorso nella contraffazione o alterazione, fa uso di valori di bollo contraffatti o alterati.

Divulgazione, tramite reti telematiche, a disposizione del pubblico, o mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa (art. 171 comma 1, lett. a-bis, e comma 3, Legge 633/1941)

In relazione alla fattispecie delittuosa di cui all'art. 171 della Legge sul Diritto d'Autore, il Decreto 231 ha preso in considerazione esclusivamente due fattispecie:

- La messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore o parte di essa. La fattispecie di reato in oggetto si concretizza quando un soggetto viola il diritto di autore, diffondendo attraverso l'utilizzo di reti telematiche, in tutto o in parte, opere dell'ingegno protette (art. 171 comma 1, lett. a-bis);
- La messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera stessa, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Si tratta di reato comune, la cui condotta può essere realizzata da chiunque.

Nella prima ipotesi si tutela, dunque, l'interesse patrimoniale dell'autore dell'opera, mentre nella seconda ipotesi il bene giuridico protetto non è l'aspettativa di guadagno del titolare dell'oper,a ma il suo onore e la sua reputazione.

2. Aree di attività a rischio

Con riferimento ai reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento e in materia di violazione del diritto d'autore, le principali attività ritenute più specificamente a rischio sono le seguenti:

- Gestione dei valori e del denaro incassato;
- Gestione di finanziamenti, contributi ed erogazioni;
- Erogazione del corso.

3. Regole di carattere generale

Destinatari della presente parte speciale sono tutti i soggetti coinvolti nelle attività a rischio, affinchè gli stessi adottino regole di condotta conformi a quanto prescritto al fine di prevenire il verificarsi dei delitti considerati.
È fatto espresso divieto agli Organi Sociali (in via diretta), ai lavoratori dipendenti e ai consulenti di EQUASOFT di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate.
Nel rispetto del Codice Etico, dei principi e delle procedure aziendali applicabili alla presente parte speciale, i soggetti indicati devono rispettare scrupolosamente tutte le leggi vigenti ed in particolare a tali soggetti è fatto divieto di:

- detenere, ricevere e mettere in circolazione, in buona o mala fede, monete, banconote e marche da bollo falsificate;
- mantenere in circolazione, ovvero agevolare la circolazione di monete, banconote e marche da bollo in relazione alle quali si sia acquisita la certezza o si abbia anche solo il sospetto di falsità;
- duplicare o riprodurre opere protette dal diritto d'autore, in assenza di espressa autorizzazione da parte del titolare del diritto d'autore o degli aventi diritto;
- diffondere o modificare opere protette dal diritto d'autore, in assenza di espressa autorizzazione da parte del titolare del diritto d'autore o degli aventi diritto;
- concedere in locazione o detenere a scopo commerciale opere protette dal diritto d'autore, in assenza di espressa autorizzazione da parte del titolare del diritto d'autore o degli aventi diritto;

- tenere qualsivoglia ulteriore comportamento in grado di ledere gli altrui diritti di proprietà intellettuale.

4. Regole specifiche di condotta

Non sono state previste specifiche procedure e norme aziendali aventi ad oggetto la tutela di strumenti e segni di riconoscimento e del diritto d'autore, ritenendosi sufficienti le regole generali già dettagliate. È sufficiente stabilire che chiunque riceva banconote per conto dell'Ente debba verificarne l'autenticità e che chiunque rilevi all'interno della struttura qualsivoglia condotta anche solo potenzialmente integrante i reati in esame ne faccia prontamente denuncia all'OdV.
Nello svolgimento delle attività a rischio, tutti i destinatari del Modello e, in particolare, i soggetti aziendali coinvolti nelle aree a rischio, devono tenere un comportamento corretto e trasparente, in conformità a quanto disposto dalle previsioni di legge esistenti in materia, dal Codice Etico e dalle procedure aziendali.

5. Controlli dell'organismo di vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli, verifiche ed ispezioni, anche a campione o a seguito di segnalazione, delle operazioni a rischio al fine di verificare la corretta esplicazione delle stesse. A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo e libero accesso a tutta la documentazione aziendale rilevante che esso ritenga rilevante per la prevenzione e repressione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello. L'OdV dovrà evitare, per quanto possibile, di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione per prevenire e, se del caso, reprimere, ogni comportamento che sia in contrasto con le regole aziendali.

PARTE SPECIALE 6 – Reati di razzismo e xenofobia

1. Le fattispecie di reati di razzismo e xenofobia (art. 25-terdecies)

Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa (art. 604-bis cp)

La norma è diretta a tutelare il rispetto della dignità umana e del principio di uguaglianza etnica, nazionale, razziale e religiosa.

Essa punisce qualsiasi condotta di propaganda sulla superiorità o sull'odio razziale, nonchè l'istigazione e la propaganda di fatti o attività atte a provocare violenza per motivi etnici, razziali o religiosi.

Vengono inoltre vietate le associazioni istituite a tale scopo, punendo sia i meri partecipanti all'associazione, sia, in maniera più grave (analogamente alle norme sull'associazione a delinquere ex art. 416) gli organizzatori e promotori.

2. Aree di attività a rischio

Con riferimento ai reati di razzismo e xenofobia, considerate le attività svolte da Equasoft la probabilità di accadimento dei suddetti reati è considerata remota poiché la propaganda politica e le forme di discriminazione religiosa e razziale sono assolutamente vietate e condannate sia dalle regole contenute nel Codice Etico del gruppo che dai principi e dalle linee guida inclusi nel presente Modello. Inoltre, allo stato attuale appare alquanto improbabile che il Personale di Equasoft compia attività di propaganda ovvero di istigazione o di incitamento ai crimini di genocidio o contro l'umanità allo scopo di generare un vantaggio a favore della società. In ottica prudenziale, le principali attività ritenute più specificamente a rischio sono le seguenti:

- Gestione dell'assunzione del personale;
- Erogazione del corso.

3. Regole di carattere generale

Destinatari della presente parte speciale sono amministratori, dirigenti e dipendenti operanti nelle aree di attività a rischio, nonché a collaboratori esterni e partners commerciali, affinchè gli stessi adottino regole di condotta conformi a quanto prescritto al fine di prevenire il verificarsi del reato di razzismo e xenofobia.

È fatto espresso divieto a tali soggetti di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, il reato considerato.

Nel rispetto del Codice Etico, dei principi e delle procedure aziendali applicabili alla presente parte speciale, i soggetti indicati devono rispettare scrupolosamente tutte le leggi vigenti ed in particolare a tali soggetti è fatto divieto di:

- utilizzare anche occasionalmente la società, o una sua unità organizzativa, allo scopo di consentire o agevolare la commissione dei reati di cui sopra;
- nel corso dell'attività aziendale promuovere, costituire, organizzare o dirigere associazioni che si propongono il compimento di atti di razzismo e xenofobia;
- propagandare idee fondate sulla superiorità o sull'odio razziale o etnico
- istigare a commettere o commettere atti di discriminazione per motivi razziali, etnici, nazionali o religiosi;

4. Regole specifiche di condotta

Non sono state previste specifiche procedure e norme aziendali aventi ad oggetto la tutela di strumenti e segni di riconoscimento e del diritto d'autore, considerandosi la probabilità di accadimento dei suddetti reati remota e ritenendosi sufficienti le regole generali già dettagliate.
Nello svolgimento delle attività a rischio, tutti i destinatari del Modello e, in particolare, i soggetti aziendali coinvolti nelle aree a rischio, devono tenere un comportamento corretto e trasparente, in conformità a quanto disposto dalle previsioni di legge esistenti in materia, dal Codice Etico e dalle procedure aziendali.

5. Controlli dell'organismo di vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli, verifiche ed ispezioni, anche a campione o a seguito di segnalazione, delle operazioni a rischio al fine di verificare la corretta esplicazione delle stesse. A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo e libero accesso a tutta la documentazione aziendale rilevante che esso ritenga rilevante per la prevenzione e repressione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello. L'OdV dovrà evitare, per quanto possibile, di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione per prevenire e, se del caso, reprimere, ogni comportamento che sia in contrasto con le regole aziendali.