



**MODELLO STANDARD DI  
ORGANIZZAZIONE, GESTIONE E  
CONTROLLO**

**PARTE GENERALE**

**AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231**

	<b>DATA</b>	<b>APPROVATO</b>	<b>NOTE</b>
<b>ADOZIONE E REVISIONE</b>	Luglio 2021	Consiglio di Amministrazione	Prima adozione
	26 luglio 2022	Consiglio di Amministrazione	Aggiornamento normativo e inserimento nuova area di rischio (gestione delle vendite)
	26 febbraio 2024	Consiglio di Amministrazione	Aggiornamento al fine di recepire le novità legislative in materia di Responsabilità Amministrativa degli Enti

## Indice

DEFINIZIONI .....	5
1. IL DECRETO LEGISLATIVO 231/2001 .....	6
1.1 Principi generali della responsabilità amministrativa degli Enti.....	6
1.2 I presupposti della responsabilità amministrativa degli Enti.....	7
1.2.1 I soggetti attivi del reato-presupposto ed il loro “legame” con l’Ente.....	7
1.2.2 Interesse o vantaggio dell’Ente .....	7
1.2.3 I reati-presupposto della responsabilità amministrativa degli Enti .....	8
1.3 Le condizioni per l’esonero della responsabilità amministrativa degli Enti .....	8
1.3.1 Responsabilità amministrativa dell’Ente e reati-presupposto commessi da soggetti in posizione apicale .....	9
1.3.2 Responsabilità amministrativa dell’ente e reati-presupposto commessi da soggetti sottoposti all’altrui direzione .....	10
1.3.3 Le segnalazioni Whistleblowing .....	10
1.4 L’applicazione pratica del D. Lgs. n. 231/01 .....	12
1.4.1. Le Linee Guida di Confindustria.....	12
1.5. Le sanzioni amministrative applicabili agli Enti .....	14
1.5.1 Le sanzioni pecuniarie .....	15
1.5.2 Le sanzioni interdittive .....	15
1.5.3 La pubblicazione della sentenza di condanna .....	17
1.5.4 La confisca del prezzo o del profitto del reato .....	17
2. IL MODELLO DI GOVERNANCE E L’ASSETTO ORGANIZZATIVO .....	18
2.1 La Società.....	18
2.2 La storia di Yoroi S.r.l.....	19
2.3. L’assetto societario .....	20
2.4 Gli strumenti di governance della Società .....	25
2.4 Rapporti infragruppo .....	29
3. IL MODELLO DI ORGANIZZAZIONE E DI GESTIONE DELLA SOCIETA’.....	30
3.1 Obiettivi e funzione del Modello .....	30
3.2 Destinatari del Modello .....	31
3.3 Struttura del Modello: Parte Generale e Parte Speciale .....	31
3.4 Il progetto della Società per la definizione del proprio Modello .....	34
3.4.1 Individuazione delle aree, delle attività e dei processi sensibili.....	34
3.4.2 Identificazione dei Key Officer.....	35
3.4.3 Analisi dei processi e delle Attività Sensibili.....	35
3.4.4 Individuazione dei meccanismi correttivi: analisi di comparazione della situazione esistente rispetto al Modello a tendere.....	36
3.4.5 Predisposizione del Modello .....	37
3.4.6 Criteri di aggiornamento del Modello .....	37

3.5 Estensione dei principi del Modello di TINEXTA S.p.A. alla Società.....	38
4. ORGANISMO DI VIGILANZA.....	39
4.1 I requisiti dell’Organismo di Vigilanza.....	39
4.2 Reporting dell’Organismo di Vigilanza verso gli organi societari.....	43
4.3 Informativa verso l’Organismo di Vigilanza.....	44
4.4 Raccolta e conservazione delle informazioni.....	47
5. SISTEMA DISCIPLINARE E SANZIONATORIO.....	48
5.1 Principi generali.....	48
5.2 Condotte sanzionabili: categorie fondamentali.....	48
5.3 Soggetti.....	49
5.4 Violazioni del modello e relative sanzioni.....	49
5.5 Misure nei confronti dei dipendenti.....	50
5.6 Misure nei confronti dei dirigenti.....	50
5.7 Misure nei confronti di amministratori e sindaci.....	51
5.8 Misure nei confronti degli altri destinatari.....	51
6. COMUNICAZIONE E FORMAZIONE DEL PERSONALE.....	52
6.1 Formazione e diffusione del Modello.....	52
6.2 Componenti degli organi sociali, dipendenti, dirigenti e quadri.....	53
6.3 Altri Destinatari.....	53

## DEFINIZIONI

- **Codice Etico e di Condotta di Gruppo**: Documento adottato dal Gruppo TINEXTA volto ad indicare i valori cui le Società si ispirano nello svolgimento delle proprie attività;
- **Decreto**: Decreto Legislativo 8 giugno 2001, n. 231 e successive integrazioni e modifiche;
- **Organismo di Vigilanza** o **OdV**: organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo al quale, ai sensi del Decreto Legislativo n. 231/2001, è affidato compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento;
- **Consulenti**: coloro che agiscono in nome e/o per conto della Società sulla base di apposito mandato o di altro vincolo di consulenza o collaborazione;
- **Dirigenti**: i dirigenti della Società;
- **Dipendenti**: tutti i lavoratori subordinati della Società (impiegati, quadri, operai, ecc.);
- **Modello**: il modello di organizzazione, di gestione e controllo previsto dal D. Lgs. n. 231/2001, adottato ed efficacemente attuato sulla base dei principi di riferimento di cui al presente documento (di seguito denominato "Modello");
- **P.A.** o **Pubblica Amministrazione**: la Pubblica Amministrazione, inclusi i relativi funzionari nella loro veste di pubblici Ufficiali o incaricati di pubblico servizio (con la stessa definizione ci si riferisce a qualsiasi soggetto che rivesta le funzioni di pubblico ufficiale o incaricato di pubblico servizio anche se non alle dipendenze di una Pubblica Amministrazione);
- **Partner**: soggetti che intrattengono rapporti contrattuali con la Società, quali ad es. fornitori, sia persone fisiche sia persone giuridiche, ovvero soggetti con cui la società addivenga ad una qualunque forma di collaborazione contrattualmente regolata (consulenti, agenti, procacciatori, consorzi, ecc.), ove destinati a cooperare con l'azienda nell'ambito dei processi sensibili;
- **Reati**: i reati per i quali è applicabile la disciplina prevista dal D. Lgs. n. 231/2001;
- **Processi Sensibili**: attività della Società nel cui ambito ricorre il rischio di commissione dei reati per i quali è applicabile la disciplina prevista dal D. Lgs. n. 231/2001;
- **Area di rischio**: area/settore aziendale a rischio di commissione dei reati per i quali è applicabile la disciplina prevista dal D. Lgs. n. 231/2001;
- **Sistemi di controllo**: sistema di controllo predisposto dalla società al fine di prevenire, attraverso l'adozione di appositi protocolli, i rischi di commissione dei reati per i quali è applicabile la disciplina prevista dal D. Lgs. n. 231/2001;
- **Linee Guida Confindustria**: le Linee Guida emanate da Confindustria per la

costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. n. 231/2001, approvate dal Ministero della Giustizia in data 24 maggio 2004 e, da ultimo aggiornate, nel 2021.

## **1. IL DECRETO LEGISLATIVO 231/2001**

### **1.1 Principi generali della responsabilità amministrativa degli Enti**

Il Decreto Legislativo 8 giugno 2001, n. 231, emanato in esecuzione della delega contenuta nell'art. 11 della Legge 29 settembre 2000, n. 300, ha introdotto nell'ordinamento giuridico italiano la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato.

In particolare, il Decreto ha previsto che gli enti forniti di personalità giuridica, le società e le associazioni, anche prive di personalità giuridica, sono responsabili nel caso in cui i propri apicali, i propri dirigenti o coloro che operano sotto la direzione o la vigilanza di questi, commettano alcune fattispecie di reato, tassativamente individuate, nell'interesse o a vantaggio dell'ente stesso.

Il fine della norma è quello di sensibilizzare gli enti sulla necessità di dotarsi di una organizzazione interna idonea a prevenire la commissione di reati da parte dei propri apicali o delle persone che sono sottoposto al loro controllo.

Si noti che la responsabilità amministrativa dell'Ente non è sostitutiva di quella penale della persona fisica che ha realizzato materialmente il c.d. reato presupposto, ma si aggiunge ad essa.

Le fattispecie di reato cui si applica la disciplina in esame possono essere comprese, per comodità espositiva, nelle seguenti categorie:

- Reati commessi nei rapporti con la P.A e di corruzione. (artt. 24 e 25).
- Delitti informatici e trattamento illecito di dati (art. 24-bis).
- Delitti di criminalità organizzata (art. 24-ter).
- Reati di falsità in monete, carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis).
- Delitti contro l'industria e il commercio (art. 25-bis1).
- Reati societari (art. 25-ter).
- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater).
- Pratiche di mutilazione degli organi genitali femminili (art. 25-quater 1).
- Delitti contro la personalità individuale (art. 25-quinquies).
- Reati di abuso di mercato (art. 25-sexies).
- Reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies).
- Reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25-octies).
- Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies 1).
- Delitti in materia di violazione del diritto d'autore (art. 25-novies).

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies).
- Reati ambientali (art. 25-undecies).
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies).
- Reati di razzismo e xenofobia (art.25-terdecies).
- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art.25-quaterdecies).
- Reati transnazionali (Legge 16 marzo 2006, n. 146, artt. 3 e 10).
- Reati tributari (art. 25-quinquiesdecies).
- Reati di contrabbando (art. 25-sexiesdecies).
- Reati contro il patrimonio culturale (art. 25 septiesdecies).
- Reati di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25 duodevicies).

L'elenco completo dei reati suscettibili, in base al Decreto, di configurare la responsabilità amministrativa dell'ente e il dettaglio delle categorie di reato per le quali si può ipotizzare la commissione nel contesto operativo della Società, è riportato all'interno dell'Allegato alla Parte Speciale del Modello (All.to 2).

## **1.2 I presupposti della responsabilità amministrativa degli Enti**

### **1.2.1 I soggetti attivi del reato-presupposto ed il loro "legame" con l'Ente**

L'art. 5, comma 1, del Decreto, indica le persone fisiche il cui comportamento delittuoso fa derivare la responsabilità amministrativa degli Enti, in virtù della teoria della c.d. immedesimazione organica.

Ai sensi di tale articolo, difatti, l'Ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persona che esercitano, anche di fatto, la gestione e il controllo;
- b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

Con riferimento ai soggetti individuati *sub a)*, è bene evidenziare che, per il Legislatore, non è necessario che la posizione apicale sia rivestita "in via formale", ma è sufficiente che le funzioni esercitate, anche "di fatto" siano effettivamente di gestione e di controllo (come rilevato dalla Relazione Ministeriale al Decreto, difatti, devono essere esercitate entrambe).

### **1.2.2 Interesse o vantaggio dell'Ente**

Come si è detto, le persone fisiche dal cui comportamento delittuoso può

derivare la responsabilità amministrativa devono aver commesso il c.d. reato presupposto nell'interesse o a vantaggio dell'Ente.

L'interesse dell'Ente presuppone sempre una verifica ex ante del comportamento delittuoso tenuto dalla persona fisica, mentre il "vantaggio" richiede sempre una verifica ex post e può essere tratto dall'Ente anche quando la persona fisica non abbia agito nel suo interesse. I termini "interesse" e "vantaggio" hanno riguardo a concetti giuridicamente diversi e hanno ciascuno una specifica ed autonoma rilevanza, in quanto può ben accadere, ad esempio, che una condotta che inizialmente poteva sembrare di interesse per l'ente, poi, di fatto, a posteriori non porti il vantaggio sperato.

L'Ente non risponde, di converso, se le persone indicate sub 1.2.1 hanno agito nell'interesse esclusivo proprio o dei terzi: poiché, in tale evenienza, viene meno il requisito della commissione del reato nell'interesse o a vantaggio dell'Ente.

Nell'ipotesi in cui la persona fisica abbia commesso il c.d. reato presupposto nel "prevalente" interesse proprio o di terzi e l'Ente non abbia ricavato vantaggio alcuno o ne abbia ricavato un vantaggio minimo, vi sarà comunque responsabilità e l'applicazione ai sensi e per gli effetti dell'art. 12, comma 1, lett. a) del Decreto della sanzione pecuniaria ridotta della metà e comunque non superiore a € 103.291,38).

### ***1.2.3 I reati-presupposto della responsabilità amministrativa degli Enti***

La responsabilità amministrativa dell'Ente può essere configurata solo in relazione a quegli illeciti penali espressamente individuati come presupposto della responsabilità amministrativa dell'ente dal D. Lgs. n. 231/2001 e/o dalla Legge n. 146/2006.

Si noti, che l'Ente non può essere ritenuto responsabile per un fatto costituente reato se la sua responsabilità amministrativa, in relazione a quel reato e le relative sanzioni non sono espressamente previste da una legge che sia entrata in vigore prima della commissione del fatto (c.d. principio di legalità).

### **1.3 Le condizioni per l'esonero della responsabilità amministrativa degli Enti**

Gli articoli 6 e 7 del Decreto disciplinano le condizioni per l'esonero della responsabilità amministrativa dell'Ente.

Il Modello è un complesso di regole e strumenti finalizzato a dotare l'Ente di un efficace sistema organizzativo e di gestione, che sia anche idoneo ad individuare e prevenire le condotte penalmente rilevanti poste in essere da coloro che operano, a qualsiasi titolo, per conto della società.

Il Decreto delinea un differente trattamento per l'Ente a seconda che il reato-presupposto sia commesso:

- a. da persone che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, ovvero da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi;
- b. da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

### ***1.3.1 Responsabilità amministrativa dell'Ente e reati-presupposto commessi da soggetti in posizione apicale***

In base alle previsioni del d.lgs. 231/2001 – art. 6, comma 1, lett. a) e b) – l'ente può essere esonerato dalla responsabilità conseguente alla commissione di reati da parte dei soggetti qualificati ex art. 5 del d.lgs. 231/2001, se prova che:

- a) l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
- b) il compito di vigilare sul funzionamento, l'efficacia e sull'osservanza del Modello e di curarne l'aggiornamento sia stato affidato a un Organismo dell'ente dotato di autonomi poteri di iniziativa e controllo;
- c) le persone fisiche abbiano commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
- d) non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza, di cui alla lettera b).

In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i Modelli di organizzazione e gestione devono rispondere alle seguenti esigenze:

- a) individuare le attività nel cui ambito possono essere commessi reati;
- b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

In questa ipotesi, la disciplina di cui al Decreto prevede la c.d. "inversione dell'onere probatorio" riguardo all'adozione e all'efficace attuazione di un Modello idoneo a prevenire la commissione di reati- presupposto. Ciò significa che, qualora venga contestato un illecito amministrativo conseguente alla commissione di uno o più reati- presupposto da parte di un apicale, è l'Ente a dover dimostrare la propria estraneità dalla condotta delittuosa ("non risponde se prova" la sussistenza di tutto quanto richiesto dal Decreto).

### **1.3.2 Responsabilità amministrativa dell'ente e reati-presupposto commessi da soggetti sottoposti all'altrui direzione**

L'art. 7 del Decreto statuisce che se il reato-presupposto è stato commesso dalle persone indicate nell'art. 5, comma 1, lettera b), l'Ente è responsabile se la commissione del citato reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza.

L'inosservanza degli obblighi di direzione o vigilanza è esclusa se l'Ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

Il Modello dovrà prevedere, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

L'efficace attuazione del Modello, inoltre, richiede:

- a) una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;
- b) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

### **1.3.3 Le segnalazioni Whistleblowing**

Il D. Lgs. n. 24/2023, attuando la Direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, ha modificato quanto previsto dall'art. 6, comma 2 bis<sup>1</sup> del D. Lgs. n. 231/2001 in materia di segnalazioni Whistleblowing.

In particolare, il D. Lgs. n. 24/2023 ha previsto una specifica tutela rivolta alle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato.

I Modelli di Organizzazione, Gestione e Controllo devono conformarsi a quanto disposto dal D. Lgs. n. 24/2023 prevedendo canali di segnalazione interna che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

Ai sensi dell'art. 6 del D. Lgs. n. 24/2023 il segnalante può effettuare una segnalazione esterna attraverso il canale messo a disposizione da ANAC se, al

---

<sup>1</sup> Comma introdotto dalla Legge 30 novembre 2017, n. 179 in materia di Whistleblowing, G.U. n. 291 del 14 dicembre 2017.

momento della sua presentazione, ricorrano una delle seguenti condizioni:

- a. non è prevista, nell'ambito del suo contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto previsto dal Decreto;
- b. la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
- c. la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
- d. la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Qualora la segnalazione esterna dovesse essere presentata ad un soggetto diverso dall'ANAC questa deve essere trasmessa all'Autorità entro sette giorni dalla data del suo ricevimento, dando contestuale notizia della trasmissione alla persona segnalante.

Al fine di tutelare la riservatezza del segnalante l'art. 12 del D. Lgs. n. 24/2023 stabilisce che: "l'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del regolamento (UE) 2016/679 e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196"; l'identità delle persone coinvolte e delle persone menzionate nella segnalazione dovranno essere tutelate fino alla conclusione dei procedimenti avviati in ragione della segnalazione nel rispetto delle medesime garanzie previste in favore della persona segnalante. Qualora l'identità della persona segnalante dovesse essere stata rivelata dovrà essere dato avviso a quest'ultima, mediante comunicazione scritta, specificandone le ragioni.

Le misure di protezione si applicano quando:

- e. al momento della segnalazione o della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica, la persona segnalante o denunciante aveva fondato motivo di ritenere che le informazioni sulle violazioni segnalate, divulgate pubblicamente o denunciate fossero vere e rientrassero nell'ambito oggettivo di cui all'articolo 1 del predetto Decreto Legislativo;
- f. la segnalazione o divulgazione pubblica è stata effettuata sulla base di quanto previsto dal capo II dello stesso Decreto Legislativo.

I segnalanti non possono subire alcun tipo di ritorsione a seguito della segnalazione e, ove ciò invece dovesse accadere, è garantita loro la possibilità di denunciare eventuali comportamenti commessi nel contesto lavorativo

direttamente all'Autorità Nazionale Anticorruzione la quale procederà a informare immediatamente il Dipartimento della funzione pubblica presso la Presidenza del Consiglio dei ministri e gli eventuali organismi di garanzia o di disciplina, qualora il lavoratore rientrasse nel settore pubblico, ovvero l'Ispettorato Nazionale del Lavoro qualora la ritorsione si sia consumata nel contesto lavorativo di un soggetto privato.

L'obbligo di informare il datore di lavoro di eventuali comportamenti sospetti rientra già nel più ampio dovere di diligenza ed obbligo di fedeltà del prestatore di lavoro e, conseguentemente, il corretto adempimento dell'obbligo di informazione non può dare luogo all'applicazione di sanzioni disciplinari, ad eccezione dei casi in cui l'informazione sia connotata da intenti calunniosi o sorretta da cattiva fede, dolo o colpa grave. Al fine di garantire l'efficacia del sistema di whistleblowing, è quindi necessaria una puntuale informazione da parte dell'Ente di tutto il personale e dei soggetti che con lo stesso collaborano non soltanto in relazione alle procedure e ai regolamenti adottati dalla Società e alle attività a rischio, ma anche con riferimento alla conoscenza, comprensione e diffusione degli obbiettivi e dello spirito con cui la segnalazione deve essere effettuata.

Con l'obiettivo di dare attuazione alle disposizioni in materia di obbligo di fedeltà del prestatore di lavoro e della legge sul Whistleblowing, si rende dunque necessaria l'introduzione nel Modello di Organizzazione, Gestione e Controllo di un sistema di gestione delle segnalazioni di illeciti che consenta di tutelare l'identità del segnalante e il connesso diritto alla riservatezza di quest'ultimo, nonché l'introduzione di specifiche previsioni all'interno del sistema disciplinare volte a sanzionare eventuali atti di ritorsione e atteggiamenti discriminatori in danno del segnalante.

## **1.4 L'applicazione pratica del D. Lgs. n. 231/01**

### **1.4.1. Le Linee Guida di Confindustria**

Ai sensi dell'art. 6 del Decreto, i Modelli possono essere adottati, garantendo le suindicate esigenze, anche sulla base di codici di comportamento redatti dalle associazioni rappresentative degli Enti, comunicati al Ministero della Giustizia ai sensi dell'art. 6, comma 3, del Decreto.

Confindustria si propone, per Statuto, di contribuire, insieme alle istituzioni politiche e alle organizzazioni economiche, sociali e culturali, nazionali ed internazionali, alla crescita economica e al progresso sociale del paese.

Anche in tale ottica, e per essere d'aiuto alle imprese associate, Confindustria ha emanato le "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. 231/2001".

La prima versione delle Linee Guida, elaborata nel 2002 dal Gruppo di lavoro sulla "Responsabilità amministrativa delle persone giuridiche", costituito nell'ambito del Nucleo Affari Legali, Finanza e Diritto d'Impresa di Confindustria,

è stata approvata dal Ministero della Giustizia nel giugno 2004.

A seguito dei numerosi interventi legislativi che, nel frattempo, hanno modificato la disciplina sulla responsabilità amministrativa degli Enti, estendendone l'ambito applicativo a ulteriori fattispecie di reato, il Gruppo di lavoro di Confindustria ha provveduto ad aggiornare le Linee Guida per la costruzione dei modelli organizzativi.

L'ultimo aggiornamento delle Linee Guida, del giugno 2021, è stato approvato dal Ministero della Giustizia in data 8 giugno 2021.

Le nuove Linee Guida di Confindustria per la costruzione dei modelli organizzativi adeguano i precedenti testi alle novità legislative, giurisprudenziali e alla prassi applicativa nel frattempo intervenute, con il fine di fornire indicazioni in merito alle misure idonee a prevenire la commissione dei reati-presupposto previsti dal Decreto.

Le Linee Guida di Confindustria per la costruzione dei Modelli forniscono alle associazioni e alle imprese – affiliate o meno all'Associazione – indicazioni di tipo metodologico su come predisporre un modello organizzativo idoneo a prevenire la commissione dei reati indicati nel Decreto.

Le indicazioni di tale documento, avente una valenza riconosciuta anche dal Decreto, possono essere schematizzate secondo i seguenti punti fondamentali:

- individuazione delle aree di rischio, volte a verificare in quale area/settore aziendale sia possibile la realizzazione dei reati previsti dal D. Lgs. 231/2001;
- individuazione delle modalità di commissione degli illeciti;
- esecuzione del *risk assessment*, *in un'ottica integrata*;
- individuazione dei punti di controllo tesi a mitigare il rischio reato;
- *gap analysis*.

Le componenti più rilevanti del sistema di controllo ideato da Confindustria sono:

- Codice Etico;
- sistema organizzativo;
- procedure manuali ed informatiche;
- poteri autorizzativi e di firma;
- sistemi di controllo e gestione;
- comunicazione al personale e sua formazione.
- disciplina delle modalità per effettuare segnalazioni whistleblowing e modalità di gestione delle stesse.

Le componenti del sistema di controllo devono essere orientate ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- applicazione del principio di separazione delle funzioni (nessuno può gestire in autonomia un intero processo);
- documentazione dei controlli;
- previsione di un adeguato sistema sanzionatorio per la violazione delle procedure previste dal modello;

- individuazione dei requisiti dell'organismo di vigilanza, riassumibili come segue:
  - autonomia e indipendenza;
  - professionalità;
  - continuità di azione.
- obblighi di informazione dell'Organismo di Vigilanza ed individuazione dei criteri per la scelta di tale Organismo.

È opportuno evidenziare che:

- 1) la mancata conformità a punti specifici delle Linee Guida non inficia di per sé la validità del Modello;
- 2) le indicazioni fornite nelle Linee Guida richiedono un successivo adattamento da parte delle imprese.

Ogni modello organizzativo, infatti, per poter esercitare la propria efficacia preventiva, va costruito tenendo presenti le caratteristiche proprie dell'impresa cui si applica. Il rischio reato di ogni impresa, difatti, è strettamente connesso al settore economico, dalla complessità organizzativa - non solo dimensionale - dell'impresa e dell'area geografica in cui essa opera.

### **1.5. Le sanzioni amministrative applicabili agli Enti**

Il Decreto disciplina quattro tipi di sanzioni amministrative applicabili agli Enti per gli illeciti amministrativi dipendenti da reato:

- 1) le sanzioni pecuniarie (e sequestro conservativo in sede cautelare), applicabili a tutti gli illeciti;
- 2) le sanzioni interdittive, applicabili anche come misura cautelare e comunque soltanto nei casi di particolare gravità di durata non inferiore a tre mesi e non superiore a due anni che, a loro volta, possono consistere in:
  - interdizione dall'esercizio dell'attività;
  - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
  - divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
  - esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi;
  - divieto di pubblicizzare beni o servizi;
  - la confisca ;
  - pubblicazione della sentenza (in caso di applicazione di una sanzione interdittiva).

La ratio della disciplina predisposta in ambito sanzionatorio è evidente: si intende perseguire sia il patrimonio dell'ente che la sua operatività, mentre, con l'introduzione della confisca del profitto, si vuole fronteggiare l'ingiusto ed ingiustificato arricchimento dell'Ente tramite la commissione di reati.

### **1.5.1 Le sanzioni pecuniarie**

La sanzione pecuniaria è la sanzione fondamentale, applicabile sempre e a tutti gli illeciti amministrativi dipendenti da reato.

La sanzione pecuniaria viene applicata per quote in un numero non inferiore a cento né superiore a mille.

Il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'ente, nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

L'importo di una quota va da un minimo di € 258,23 ad un massimo di € 1.549,37 ed è fissato sulla base delle condizioni economiche e patrimoniali dell'ente allo scopo di assicurare l'efficacia della sanzione.

In ogni modo, la pena è ridotta della metà e non può superare, comunque Euro 103.291,38 se:

- a) l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo (art. 12, comma 1, lett. A, del Decreto);
- b) il danno patrimoniale cagionato è di particolare tenuità (art. 12, comma 1, lett. B, del Decreto).

La sanzione pecuniaria, inoltre, è ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado:

- a) l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;
- b) è stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.

Nel caso in cui concorrono entrambe le condizioni, la sanzione è ridotta dalla metà ai due terzi.

In ogni caso, la sanzione pecuniaria non può essere inferiore a euro 10.329,14. Per quantificare il valore monetario della singola quota, pertanto, il giudice penale deve operare una "duplice operazione": deve dapprima determinare l'ammontare del numero delle quote sulla scorta dei citati indici di gravità dell'illecito, del grado di responsabilità dell'ente e dell'attività svolta per attenuare le conseguenze del reato e, successivamente, determinare il valore monetario della singola quota tenendo conto delle condizioni economiche e patrimoniali dell'ente, allo scopo di assicurare l'efficacia della sanzione.

### **1.5.2 Le sanzioni interdittive**

Le sanzioni interdittive si applicano unitamente alla sanzione pecuniaria, ma solamente in relazione ai reati-presupposto per i quali sono espressamente previste.

La loro durata non può essere inferiore a tre mesi e non può essere superiore a due anni.

Le sanzioni interdittive previste dal Decreto sono:

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

Se necessario, le sanzioni interdittive possono essere applicate congiuntamente. La loro applicazione, pertanto, può, da un lato, paralizzare lo svolgimento dell'attività dell'Ente, dall'altro, condizionarla sensibilmente attraverso la limitazione della sua capacità giuridica o la sottrazione di risorse finanziarie.

Trattandosi di sanzioni particolarmente gravose, nel Decreto è stabilito che possano essere applicate solo se ricorre almeno una delle seguenti condizioni:

- a) l'ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
- b) in caso di reiterazione degli illeciti.

Le sanzioni interdittive, salvo quanto disposto dall'art. 25, comma 5 del Decreto, hanno una durata non inferiore a tre mesi e non superiore a due anni; tuttavia, può essere disposta:

- a) l'interdizione definitiva dall'esercizio dell'attività se l'Ente ha tratto dal reato un profitto di rilevante entità ed è già stato condannato, almeno tre volte negli ultimi sette anni, alla interdizione temporanea dall'esercizio dell'attività;
- b) in via definitiva, la sanzione del divieto di contrattare con la pubblica amministrazione ovvero del divieto di pubblicizzare beni o servizi quando è già stato condannato alla stessa sanzione almeno tre volte negli ultimi sette anni;
- c) l'interdizione definitiva dall'esercizio dell'attività se l'Ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di reati in relazione ai quali è prevista la sua responsabilità.

Tali sanzioni, in ogni modo, non si applicano qualora:

- l'autore del reato abbia commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne abbia ricavato vantaggio o ne abbia ricavato un vantaggio minimo;
- il danno patrimoniale cagionato è di particolare tenuità.

Non si applicano, inoltre, quando, prima della dichiarazione di apertura del

dibattimento di primo grado, “concorrono” le seguenti condizioni (c.d. riparazione delle conseguenze del reato):

- a) l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;
- b) l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi;
- c) l'ente ha messo a disposizione il profitto conseguito ai fini della confisca.

Infine, in ogni caso, le sanzioni interdittive non possono essere applicate quando pregiudicano la continuità dell'attività svolta in stabilimenti industriali o parti di essi dichiarati di interesse strategico nazionale (ex articolo 1 del D. L. 3 dicembre 2012, n. 207), se l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi. Il modello organizzativo si considera sempre idoneo a prevenire reati della specie di quello verificatosi quando nell'ambito della procedura di riconoscimento dell'interesse strategico nazionale sono stati adottati provvedimenti diretti a realizzare, anche attraverso l'adozione di modelli organizzativi, il necessario bilanciamento tra le esigenze di continuità dell'attività produttiva e di salvaguardia dell'occupazione e la tutela della sicurezza sul luogo di lavoro, della salute, dell'ambiente e degli altri eventuali beni giuridici lesi dagli illeciti commessi.

### ***1.5.3 La pubblicazione della sentenza di condanna***

La pubblicazione della sentenza di condanna può essere disposta quando nei confronti dell'ente viene applicata una sanzione interdittiva.

La sentenza è pubblicata una sola volta, per estratto o per intero, in uno o più giornali indicati dal giudice, i quali, si può ipotizzare, saranno giornali “specializzati” o di “settore”, ovvero potrà essere pubblicata mediante affissione nel comune ove l'ente ha la sede principale, il tutto a complete spese dell'ente.

Tale sanzione ha una natura meramente afflittiva ed è volta ad incidere negativamente sull'immagine dell'Ente.

### ***1.5.4 La confisca del prezzo o del profitto del reato***

Nei confronti dell'ente, con la sentenza di condanna, è sempre disposta la confisca del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato e fatti salvi i diritti acquisiti dai terzi in buona fede.

Quando non è possibile eseguire la confisca del prezzo o del profitto del reato, la stessa può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato (c.d. confisca per equivalente).

Per “prezzo” del reato, si intendono le cose, il denaro o le altre utilità date o promesse per determinare o istigare alla commissione della condotta criminosa.

Per “profitto” del reato, si intende la conseguenza economica immediata ricavata dall'illecito.

La confisca per equivalente è divenuta, recentemente, uno degli strumenti più utilizzati per contrastare la c.d. criminalità del profitto.

Anche tale sanzione, come la precedente di cui *sub* 1.5.3 ha una diretta matrice penalistica.

## **2. IL MODELLO DI GOVERNANCE E L'ASSETTO ORGANIZZATIVO**

### **2.1 La Società**

La Società, al fine di assicurare sempre più condizioni di correttezza e di trasparenza nella conduzione delle attività aziendali, ha ritenuto conforme alle proprie politiche aziendali procedere all'adozione del Modello, alla luce delle prescrizioni del Decreto.

L'iniziativa intrapresa dalla Società di adottare il Modello è stata assunta nella convinzione che l'adozione di tale Modello, al di là delle prescrizioni del Decreto che indicano il Modello quale elemento facoltativo e non obbligatorio, possa costituire un valido strumento di sensibilizzazione dei Dipendenti.

YOROI S.r.l. ha per oggetto sociale:

La fornitura di prodotti, servizi, consulenza, formazione in ambito di sicurezza informatica con un'offerta integrata per supportare i propri clienti nella definizione delle strategie e nell'implementazione delle soluzioni di sicurezza delle informazioni, che si articola negli ambiti principali della security governance e della security technology ovvero:

- l'installazione e l'esercizio con qualsiasi tecnica, mezzo e sistema, di sistemi, impianti, e servizi per la realizzazione di sistemi di Sicurezza in ambito Information e Communication Technology (ICT), per l'espletamento, la gestione e la commercializzazione, senza limiti territoriali, dei sistemi e servizi di sicurezza a protezione dei dati e delle comunicazioni, quali anche risultanti dall'evoluzione delle tecnologie, e per lo svolgimento delle attività ad essi anche indirettamente connesse, comprese quelle di progettazione, realizzazione, gestione, manutenzione, monitoraggio, telecontrollo, integrazione e commercializzazione di prodotti, servizi, per la sicurezza informatica;
- la fornitura, installazione e manutenzione di apparati software e/o hardware atti al miglioramento della sicurezza aziendale quali: Firewall, Proxy, URL Filtering, Intrusion Detection Systems, Intrusion Prevention Systems, Anti Malware Prevention e soluzioni software come AntiVirus, AntiMalware, Data Loss Prevention, Mobile Device Management;
- la fornitura di servizi di analisi delle vulnerabilità di un sistema informativo, Penetration Testing, Targeted Attack Simulation e Security Audit; monitoraggio dello stato di sicurezza dell'infrastruttura finalizzata a prevenire possibili intrusioni evitando perdite o corruzione di dati;

- la fornitura di prodotti e servizi debitamente orchestrati per erogare Managed Security Service Provider per la protezione contro i cyber attacks;
- la fornitura di attività difensiva che può riguardare l'intera rete aziendale e/o parte di essa, sistemi server e/o sistemi client e può sfociare in attività mirata su ambienti SCADA e mobile;
- lo svolgimento di attività connesse o strumentali, ivi comprese le attività editoriali, pubblicitarie, informatiche, telematiche e multimediali ed in genere le attività commerciali, finanziarie, noleggio, immobiliari, di ricerca, formazione e consulenza.

La Società può anche assumere rappresentanze di ditte produttrici e rivenditrici di software e hardware per la Sicurezza Informatica, sia con deposito che senza, e partecipare ad appalti pubblici e privati e subappaltare a sua volta in tutto o in parte i lavori appaltati.

La Società può altresì svolgere corsi di formazione standard e personalizzati che possano soddisfare ogni livello di esigenza formativa in ambito di Sicurezza Informatica.

In via residuale, quando sia svolta in via strettamente strumentale al conseguimento dell'oggetto sociale, la Società può rilasciare garanzie anche ipotecarie e fideiussioni.

YOROI S.r.l. è strutturata in 4 Business Unit:

- Advisory Area
- Managed Security Services Area, costituita dall'Unità Resident Consulting e dall'Unità CSDC (Cyber Security Defence Center)
- Product Area
- Implementation Services Area

## **2.2 La storia di Yoroi S.r.l.**

YOROI S.r.l. nasce nel 2014, come startup nell'ambito della cyber security, occupandosi di sviluppare e gestire innovativi Sistemi Integrati Adattivi e Dinamici di Difesa Cibernetica. Tra la fine del 2020 e gli inizi del 2021 YOROI acquista il ramo di azienda "Cybersecurity" della Cybaze S.p.A. (ex Emaze S.p.A) ed incorpora, mediante un'operazione di fusione, @Mediaservice.net s.r.l., due società pioniere del mercato della cyber security in Italia con oltre vent'anni di esperienza. In tal modo YOROI S.r.l. ha coniugato, da un lato, l'esperienza più significativa del mercato italiano in ambito cyber security e, dall'altro, la vocazione all'innovazione tecnologica più all'avanguardia. L'ultimo passaggio relativo alla crescita e all'affermazione di YOROI S.r.l. come punto di riferimento della cyber security in Italia è stata l'acquisizione, nel gennaio 2021, della maggioranza delle partecipazioni della società da parte di TINEXTA CYBER S.p.A., società con socio unico TINEXTA S.P.A.

YOROI S.r.l. è, pertanto, entrata a far parte del Gruppo TINEXTA, quotato sul segmento STAR di Borsa Italiana.

### **2.3. L'assetto societario**

Il sistema di amministrazione adottato dalla Società è il sistema tradizionale, pertanto presenta un'Assemblea dei Soci, un Organo amministrativo che si esplicita nel Consiglio d'Amministrazione e un Organo di controllo costituito dal Collegio Sindacale.

#### **Assemblea**

L'Assemblea delibera sulle materie riservate alla propria competenza dalla legge, dallo statuto, nonché sugli argomenti che uno o più amministratori o tanti soci che rappresentino almeno un terzo del capitale sociale sottopongono alla sua approvazione.

Devono essere adottate, in prima, in seconda e in ogni successiva convocazione, dall'Assemblea dei soci e con la presenza e il voto favorevole, in prima e in ogni eventuale successiva convocazione, di uno dei Soci di Minoranza, le deliberazioni aventi ad oggetto le materie di seguito elencate:

- a) modifiche statutarie relative all'oggetto sociale che hanno impatto sostanziale sull'attività della Società;
- b) modifiche statutarie che pregiudichino i diritti attribuiti ai Soci di Minoranza;
- c) fusioni, scissioni e trasformazioni, tali da pregiudicare il valore della partecipazione dei Soci di Minoranza.

Possono essere adottate dal consiglio di amministrazione, solo a seguito di autorizzazione da parte dell'assemblea dei soci, da adottarsi a maggioranza semplice del capitale sociale, le deliberazioni aventi ad oggetto le materie di seguito elencate:

- a) approvazione e modifica del business plan della Società;
- b) approvazione del budget annuale della Società;
- c) approvazione del piano di investimenti della Società;
- d) nomina dei responsabili di funzioni di primo livello della Società, ovvero di direttori generali, responsabili di funzioni di controllo di gestione e amministrazione;
- e) compravendita di partecipazioni (sia di controllo sia di minoranza) di valore eccedente la soglia di Euro 250.000,00 (duecentocinquantamila/00) e
- f) concessione di garanzie.

#### **Consiglio di Amministrazione**

La Società è amministrata da un Consiglio di Amministrazione composto da un numero di membri pari a 5 (cinque) - nominati dall'Assemblea.

Gli amministratori possono essere anche non soci, durano in carica per il periodo indicato in occasione della nomina, salvo revoca o dimissioni e sono rieleggibili.

La gestione, sia ordinaria che straordinaria dell'impresa, spetta esclusivamente agli amministratori, i quali compiono tutti gli atti e le operazioni necessarie per l'attuazione dell'oggetto sociale, ferma restando la necessità di specifica autorizzazione nei casi richiesti dalla legge.

Il Consiglio di Amministrazione può delegare, nei limiti di cui all'art. 2381 c.c., parte delle proprie attribuzioni ad uno o più dei suoi componenti, determinandone i poteri e la relativa remunerazione.

Il Consiglio di Amministrazione può altresì disporre che venga costituito un comitato esecutivo del quale fanno parte di diritto, oltre ai consiglieri nominati a farne parte, anche il Presidente, nonché tutti i consiglieri muniti di delega.

Il Consiglio, con la propria delibera di istituzione del comitato esecutivo, può determinare gli obiettivi e le modalità di esercizio dei poteri delegati.

Al Consiglio spetta, comunque, il potere di controllo e di avocare a sé le operazioni rientranti nella delega, oltre che il potere di revocare le deleghe.

Possono essere altresì nominati direttori generali e procuratori, determinandone i poteri.

Al Presidente del Consiglio di Amministrazione, ed in caso di sua assenza od altro impedimento di quest'ultimo al Vice Presidente, se nominato, o eventualmente ad uno o più Consiglieri delegati se nominati, spetta, con firma libera, la rappresentanza legale della Società.

### **Collegio Sindacale**

Il Collegio Sindacale vigila sull'osservanza della legge e dello Statuto e sul rispetto dei principi di corretta amministrazione ed in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla Società e sul suo funzionamento. Il Collegio Sindacale si compone di tre membri effettivi e di due supplenti.

Tutti i sindaci devono essere revisori legali dei conti, iscritti nel registro istituito presso il Ministero di Giustizia.

I sindaci sono nominati dai soci. Essi restano in carica per tre esercizi e scadono alla data della decisione dei soci di approvazione del bilancio relativo al terzo esercizio della carica.

### **DPO e Privacy Officer**

In adempimento a quanto previsto dal Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679 è stato nominato, anche quale DPO di Yoroì S.r.l., il DPO del Gruppo Tinexta con il compito di:

a) sorvegliare l'osservanza del GDPR, valutando i rischi di ogni Trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;

- b) condurre una valutazione di impatto sulla protezione dei dati (DPIA);
- c) informare e sensibilizzare la Società riguardo agli obblighi derivanti dal Regolamento e da altre disposizioni in materia di protezione dei dati;
- d) cooperare con l'Autorità di Controllo e fungere da punto di contatto per la medesima su ogni questione connessa al trattamento;
- e) fungere da punto di contatto con l'Interessato per l'esercizio dei diritti di cui agli art. 15-22 del GDPR;
- f) supportare il Titolare o il Responsabile in ogni attività connessa al trattamento di Dati Personali, anche con riguardo all'eventuale tenuta di un registro delle attività di trattamento (art. 30 GDPR);
- g) coordinare e supervisionare l'attività dei Privacy Officer che, in ossequio a quanto stabilito dalla Data Protection Policy di Gruppo, presidiano il tema della protezione dei dati personali nelle società controllate.

Nell'ambito delle funzioni di supporto al DPO, il Privacy Officer della Società ha il compito di presidiare l'attuazione degli adempimenti previsti per ottemperare alle prescrizioni del GDPR, della normativa nazionale e delle policy emanate dal Gruppo Tinexta, segnalando senza ritardo al Titolare e al DPO tutte le situazioni di non conformità. Il Privacy Officer svolge, inoltre, attività di supporto al DPO e, in particolare, in collaborazione con il DPO medesimo, deve:

- a) informare e fornire consulenza agli Utenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni relative alla protezione dei dati personali;
- b) predisporre, direttamente o per tramite e con l'ausilio delle appropriate Funzioni aziendali:
  - i. il registro dei trattamenti, ove richiesto,
  - ii. le Informative,
  - iii. le formule del consenso,
  - iv. le nomine a responsabile del trattamento,
  - v. ogni altra documentazione relativa al trattamento dei dati personali,
- c) assicurarsi che la documentazione di cui al punto precedente sia correttamente inserita nei processi e nei prodotti aziendali;
- d) tenere aggiornato:
  - i. il registro dei trattamenti, alla luce delle informazioni funzionali alla mappatura dei trattamenti,
  - ii. il registro dei data breach sulla base delle informazioni notificate tramite l'indirizzo e-mail dedicato o in altro modo,
  - iii. l'elenco dei responsabili del trattamento nelle modalità definite dalla specifica organizzazione aziendale,
- e) mantenere un archivio storico delle versioni delle informative sul trattamento

dati personali in uso e delle nomine a responsabile del trattamento;

f) in conformità con gli obblighi in materia di trattamento dei dati personali, favorire la sensibilizzazione e la formazione del personale in ambito Privacy al fine di evitare eventuali violazioni e conseguenti rischi e responsabilità per la Società;

g) predisporre, con l'ausilio delle appropriate Funzioni aziendali, la valutazione d'impatto sulla protezione dei dati ("DPIA") e farne approvare il contenuto al Legale Rappresentante della Società;

h) collaborare con le Funzioni aziendali competenti al fine di garantire l'osservanza dei principi di *privacy by design* e *by default*;

i) coordinare la condotta delle eventuali articolazioni a supporto privacy, fornendo, di concerto con il DPO, le indicazioni su questioni relative al trattamento dei dati personali;

j) assicurare che vengano soddisfatti gli obblighi di reportistica circa le modalità di trattamento dei dati personali;

k) collaborare con il DPO al fine di procedere alla contestazione delle violazioni poste in essere dal Personale della Società autorizzato ai trattamenti, che non si conformi agli obblighi su di esso gravanti;

l) sottoporre all'attenzione del DPO e collaborare con lo stesso in relazione alle problematiche più rilevanti in materia di trattamento dei dati personali;

m) svolgere le altre attività di competenza previste dalla *Data Protection Policy*.

Al fine di consentire al DPO l'attività di controllo, il Privacy Officer ha inoltre la responsabilità:

a) di inviare al DPO con cadenza almeno trimestrale entro il 15 gennaio, il 15 aprile, il 15 luglio e il 15 ottobre di ogni anno solare e in caso di emergenze (i.e. qualora si verifichi un *data breach*), un report relativo alle modalità di trattamento dei dati personali;

b) di effettuare, di concerto con il DPO, con cadenza almeno semestrale, controlli periodici presso le funzioni aziendali in cui si ritenga opportuno, richiedendo copia della documentazione a supporto delle proprie attività di audit;

c) di adottare, di concerto con il DPO, le misure volte a correggere eventuali mancate conformità con la Normativa Privacy applicabile o i rischi di mancata conformità, sulla base delle informazioni contenute nei report, derivanti dagli audit o in altro modo acquisite.

### **Referente Legge 262/2005**

La Legge 262/2005 ha istituito la figura del "Dirigente preposto alla redazione dei documenti contabili societari", attribuendole, tra l'altro, la responsabilità di contribuire a garantire "l'affidabilità dell'informativa finanziaria".

La disciplina del Dirigente preposto è prevista nella sezione V bis del Testo Unico della Finanza, dedicata alla redazione dei documenti contabili, all'art. 154 bis che detta le norme generali sulla designazione, i compiti e i poteri del Dirigente preposto, nonché sulle responsabilità civili e penali che conseguono all'incarico. Il Gruppo Tinexta ha nominato un unico Dirigente preposto, la cui missione ha come obiettivi per il Gruppo:

- assicurare l'attendibilità dell'informativa finanziaria del bilancio consolidato;
- assicurare che le segnalazioni di vigilanza su base consolidata si basino sui dati della contabilità e del sistema informativo aziendale, nonché su quelli forniti dalle Società e dagli enti partecipati inclusi nella vigilanza consolidata.

Il Dirigente preposto si avvale, per lo svolgimento della propria missione, di un Referente identificato presso la Società (individuato nel ruolo del CFO), che dipende funzionalmente dal Dirigente preposto per quanto attiene metodologie, strumenti, reportistica e processi di lavoro relativi

### **Referente ERM**

Garantisce l'applicazione delle Linee Guida di Enterprise Risk Management della Capogruppo all'interno della Società.

### **Compliance**

Gestisce ed aggiorna la documentazione relativa al D.Lgs. 231/01, basandosi sulle linee guida definite dalla Capogruppo; garantisce inoltre l'adesione al Codice Etico e di Condotta di gruppo; identifica le norme applicabili in materia regolatoria e misura il loro impatto su processi e procedure aziendali, proponendo modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio dei rischi di non conformità e di reputazione.

### **Internal Audit di Gruppo**

Il Gruppo Tinexta dispone di una funzione di Internal Audit la cui missione è quella di proteggere ed accrescere il valore del Gruppo, fornendo assurance obiettiva e risk – based e consulenza interna, finalizzate a valutare e migliorare i processi di controllo, di gestione dei rischi e di corporate governance.

La funzione si articola in 3 unità organizzative, distinte per BU (Digital Trust ed Estero, Cybersecurity e Business Innovation), risponde gerarchicamente al C.d.A. della Capogruppo, riportando le risultanze dei lavori svolti anche agli organi amministrativi, di controllo e vigilanza delle controllate interessate.

La Società, in forza di apposito contratto di service con la Capogruppo, si avvale dell'attività di controllo di terzo livello della menzionata funzione che, pertanto, può essere chiamata a svolgere le suddette attività di assurance e consulenza su specifiche aree aziendali.

### **Società di revisione**

La Società ha affidato la revisione legale ad una società esterna incaricata dall'Assemblea dei soci su proposta motivata del Collegio Sindacale in conformità con le prescrizioni di legge al tempo vigenti.

### **Le altre Funzioni aziendali**

Nell'organigramma vengono individuate le aree, le direzioni, nonché i responsabili delle relative funzioni.

Più specificamente, nell'organigramma è precisato che operano alle dirette dipendenze del Presidente del Consiglio di amministrazione e dell'Amministratore Delegato i Responsabili delle seguenti funzioni:

- Administration, Finance, Control & Procurement
- HR;
- Legal, Privacy Officer, Compliance Interna;
- Operation;
- Marketing;
- Sales;
- IT

Si precisa che le attività in ambito AF (amministrazione, tesoreria, bilancio etc) sono svolte in service da Tinexta Cyber mentre le attività di registrazione delle fatture passive e di gestione delle anagrafiche fornitori vengono svolte in service dalla capogruppo Tinexta S.p.A., tramite lo Shared Services Accounts Payable.

## **2.4 Gli strumenti di governance della Società**

Statuto: In conformità con le disposizioni di legge vigenti, contempla diverse previsioni relative al governo societario volte ad assicurare il corretto svolgimento dell'attività di gestione.

Codice Etico e di Condotta di Gruppo: Come indicato al punto 2.2, YOROI S.r.l. nel gennaio 2021 è entrata a far parte del Gruppo TINEXTA, recependo, tra l'altro, il Codice Etico e di Condotta di Gruppo, che regola il complesso di diritti, doveri e responsabilità che le Società del Gruppo riconoscono come propri e assumono nei confronti dei propri interlocutori, cui devono conformarsi tutti i destinatari del presente Modello. Il Codice Etico e di Condotta di Gruppo fissa i principi etici nei quali le Società del Gruppo Tinexta si rispecchiano e ai quali, coerentemente, si devono ispirare tutti i soggetti con i quali esse operano.

In particolare, la Società si ispira ai seguenti principi:

- osservanza delle leggi vigenti nazionali, comunitarie e in generale la normativa internazionale dei Paesi in cui opera, i regolamenti o codici interni e, ove applicabili, le norme di deontologia professionale;
- onestà, correttezza e trasparenza delle azioni, poste in essere nel perseguimento dei propri obiettivi;
- rispetto dei Diritti Umani nello svolgimento delle nostre operazioni e lungo la catena del valore è un fattore imprescindibile nella gestione aziendale;
- diversità e inclusione all'interno delle politiche societarie;
- valorizzazione delle capacità e delle competenze delle persone, in modo che ognuno possa esprimere al meglio il proprio potenziale;
- fedeltà nei rapporti con le controparti di qualsiasi natura;
- tutela della privacy e delle informazioni sensibili in rispetto di quanto previsto dalla normativa in materia di privacy;
- prevenzione della corruzione, anche internazionale, sia dal lato attivo che passivo. A tal fine, a titolo esemplificativo: sono vietati favori, comportamenti collusivi, sollecitazioni dirette e/o attraverso terzi, al fine di ottenere vantaggi per la Società, per sé o per altri; il personale non deve cercare di influenzare impropriamente le decisioni della controparte (funzionari pubblici/esponenti degli Enti Privati che trattano o prendono decisioni per conto rispettivamente delle Pubbliche Amministrazioni e degli Enti Privati); non è mai consentito corrispondere né offrire, direttamente o indirettamente, denaro, omaggi o qualsiasi utilità alla Pubblica Amministrazione e agli Enti Privati o a loro familiari, per compensare un atto del proprio ufficio;
- mantenimento di un rapporto corretto e trasparente con l'amministrazione finanziaria, di una gestione etica del tema fiscale, nonché rispettare la normativa in materia fiscale;
- trasparenza verso il mercato, le Autorità di Vigilanza, gli Enti e le Istituzioni assicurando la veridicità, completezza e tempestività nelle comunicazioni sociali di qualsiasi natura
- contrasto a qualsiasi restrizione del confronto competitivo e astensione da pratiche commerciali collusive che favoriscano la conclusione di affari a vantaggio della Società e che comportino una violazione della normativa vigente in materia di concorrenza leale;
- imparzialità che prevede l'obbligo di evitare situazioni di conflitto d'interesse;
- ripudio del terrorismo che trova attuazione anche attraverso l'esecuzione di verifiche circa la non appartenenza dei potenziali partner alle Liste di Riferimento, pubblicate dall'Unità di Informazione Finanziaria (UIF), istituita presso la Banca d'Italia ex art. 6 c. 1 del D.Lgs. 231/2007, per la prevenzione e il contrasto del riciclaggio del denaro e del finanziamento del terrorismo;
- tutela dell'ambiente e della salute e sicurezza sui luoghi di lavoro e del patrimonio aziendale;

- imparzialità, che prevede l'obbligo di evitare situazioni di conflitto d'interesse.

L'adozione del Codice Etico e di Condotta di Gruppo costituisce altresì uno dei presupposti per l'efficace funzionamento del Modello. Il Codice Etico e di Condotta di Gruppo ed il Modello realizzano una stretta integrazione di norme interne con l'intento di incentivare la cultura dell'etica e della trasparenza aziendale ed evitare il rischio di commissione dei reati-presupposto della responsabilità amministrativa dell'Ente.

Comunicazioni organizzative e organigramma aziendale: riporta la struttura organizzativa della Società, le responsabilità e le finalità delle varie Funzioni e Unità Organizzative in cui essa si articola.

Sistema di deleghe e procure: La Società ha adottato un sistema di deleghe e procure caratterizzato da elementi di "sicurezza" ai fini della prevenzione dei reati (rintracciabilità ed evidenziabilità delle attività sensibili) che, nel contempo, consente la gestione efficiente dell'attività della Società.

Per "delega" si intende il trasferimento, non occasionale, all'interno della Società, di responsabilità e poteri da un soggetto all'altro in posizione a questo subordinata. Per "procura" si intende il negozio giuridico con il quale una parte conferisce all'altra il potere di rappresentarla (ossia ad agire in nome e per conto della stessa). La procura, a differenza della delega, assicura alle controparti di negoziare e contrarre con le persone preposte ufficialmente a rappresentare la Società.

Al fine di un'efficace prevenzione dei reati, il sistema di deleghe e procure deve rispettare i seguenti requisiti essenziali:

- a) le deleghe devono coniugare ciascun potere alla relativa responsabilità e ad una posizione adeguata nell'organigramma;
- b) ciascuna delega deve definire in modo specifico ed inequivocabile i poteri del delegato e il soggetto (organo o individuo) cui il delegato riporta gerarchicamente;
- c) i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi della Società;
- d) il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli;
- e) tutti coloro che intrattengono per conto della Società rapporti con la P.A. e/o con soggetti privati devono essere dotati di specifica procura in tal senso;
- f) a ciascuna procura che comporti il potere di rappresentanza della Società nei confronti dei terzi si deve accompagnare una delega interna che ne descriva il relativo potere di gestione;
- g) copie delle deleghe e procure e dei relativi aggiornamenti saranno trasmesse all'OdV.

L'OdV verifica periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore e la loro coerenza con le disposizioni organizzative, raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al delegato o vi siano altre anomalie.

Sistema procedurale: documenti organizzativi che definiscono responsabilità, ambiti di applicazione e modalità operative dei processi aziendali.

Portale intranet: è la porta d'accesso a servizi software, informativi e documentali (comunicati e manuali) oppure a specifiche risorse esterne in Internet.

Modello di governance in ambito Risk Management: Yoroi in quanto Società del Gruppo Tinexta, aderisce al processo di Enterprise Risk Management definito secondo lo standard internazionale denominato "Co.S.O. – Enterprise Risk Management", finalizzato a identificare, valutare e gestire tutti i rischi che possono avere impatto sull'attività d'impresa e così influire sul raggiungimento degli obiettivi strategici e di business, in linea con la propensione al rischio definita nel risk appetite statement dal Consiglio di Amministrazione.

Modello di governance in ambito Privacy: Yoroi, in quanto Società del Gruppo Tinexta, provvede alla costituzione del Modello di Compliance della privacy attraverso l'adozione e l'implementazione di specifici documenti, quali la Data Protection Policy Gruppo Tinexta e relativi Allegati.

Modello di governance in ambito compliance: Yoroi, in quanto Società del Gruppo Tinexta, aderisce al modello di gestione delle tematiche di compliance finalizzato a controllare e valutare periodicamente l'adeguatezza e l'efficacia delle misure, delle politiche e delle procedure adottate per individuare e minimizzare il rischio di mancata osservanza degli obblighi normativi.

Modello di governance in ambito cyber security: la Società adotta gli strumenti di Gruppo finalizzati al presidio delle tematiche di cyber security e dei relativi rischi connessi.

Modello di governance in ambito market abuse: la Società adotta gli strumenti della Capogruppo ai fini dell'adeguamento alle previsioni della normativa europea in materia di market abuse.

Modello di governance in ambito ESG: la Società adotta specifiche policy definite dalla Capogruppo in cui definisce il proprio impegno nella gestione della sostenibilità e delle tematiche ESG rilevanti, in modo sempre più integrato alla strategia e alle attività operative aziendali.

Si riporta di seguito l'elenco di tali policy:

- Policy Sostenibilità;
- Policy Diversity & Inclusion;
- Policy Diritti Umani;
- Policy Anticorruzione;
- Policy Fiscale;
- Policy Ambiente.

Il sistema di controllo sull'informativa finanziaria: La Società si attiene alle prescrizioni della Legge 262/05 finalizzate a documentare il modello di controllo contabile-amministrativo adottato, nonché ad eseguire specifiche verifiche sui controlli rilevati, per supportare il processo di attestazione del Dirigente Preposto del Gruppo Tinexta alla redazione dei documenti contabili societari. In particolare, al fine di garantire che le esigenze di copertura dei rischi e la relativa struttura dei controlli siano adeguati, con cadenza semestrale sono svolte attività di test sui controlli amministrativo-contabili per verificarne, nel corso del periodo di riferimento, l'effettiva applicazione e operatività, nonché attività di monitoraggio per accertare l'implementazione dei correttivi definiti.

Il Referente della Società in materia di Legge 262/2005 (individuato nel CFO) è incaricato del coordinamento della stesura e/o aggiornamento delle procedure amministrativo-contabili e fiscali per garantire il rispetto della Compliance alla suddetta Legge.

Le attività di testing e monitoraggio del sistema di controllo interno sono svolte dalla Direzione Internal Audit della Capogruppo. Gli esiti delle attività sono comunicati dal Responsabile della Direzione Internal Audit al Referente della Società ed al Dirigente preposto del Gruppo, per le valutazioni di competenza.

Modello di Dialogo e Controllo di Gruppo: al fine di assicurare che le Società del Gruppo operino sulla base di valori condivisi, è stato definito il "Modello di Dialogo e Controllo di Gruppo" che:

- regola le modalità di funzionamento del Gruppo Tinexta e costituisce la disciplina di riferimento alla quale ricondurre i rapporti fra la capogruppo e le Società controllate;
- garantisce livelli di integrazione coerenti con la realizzazione del comune progetto strategico, nel rispetto dell'autonomia giuridica delle Società del Gruppo;
- ottimizza le sinergie determinate dall'appartenenza al Gruppo, valorizzando le caratteristiche delle diverse società;
- indica le interazioni tra la Società controllante e le Società controllate dirette e indirette.

## **2.4 Rapporti infragruppo**

Le prestazioni dei servizi infragruppo devono essere disciplinate da un contratto

scritto, di cui copia deve essere inviata, su richiesta, all'Organismo di Vigilanza della Società. In particolare, il contratto di prestazione di servizi deve:

- disciplinare i ruoli, le responsabilità, le modalità operative e i flussi informativi per lo svolgimento dei servizi oggetto del contratto.
- Prevedere specifici presidi di controllo per il monitoraggio della corretta esecuzione delle attività affidate in service;
- definire una clausola con cui le parti si impegnano al rispetto dei principi di organizzazione, gestione e controllo idonei a prevenire la commissione di atti illeciti di cui al d.lgs. 231/01, definiti nel Modello di Organizzazione, Gestione e Controllo adottato o altro modello di compliance, ove non sia vigente la disciplina 231, contenente presidi di controllo coerenti con quelli previsti nel Modello di organizzazione, gestione e controllo adottato dalla Società.

### **3. IL MODELLO DI ORGANIZZAZIONE E DI GESTIONE DELLA SOCIETA'**

#### **3.1 Obiettivi e funzione del Modello**

YOROI S.r.l. è particolarmente sensibile all'esigenza di diffondere e consolidare la cultura della trasparenza e dell'integrità, poiché, anche prescindendo dall'aspetto strettamente giuridico-sanzionatorio sin qui illustrato, tali valori costituiscono il fulcro del credo della società e del Gruppo Tinexta di cui è entrata a far parte. Il raggiungimento delle predette finalità si concretizza in un sistema coerente di principi, procedure organizzative, gestionali e di controllo e disposizioni che danno vita al Modello che la Società ha predisposto e adottato. Tale Modello ha quali obiettivi quelli di:

- sensibilizzare i Destinatari richiedendo loro, nei limiti delle attività svolte nell'interesse della Società, di adottare comportamenti corretti e trasparenti, in linea con i valori etici a cui la stessa si ispira nel perseguimento del proprio oggetto sociale e tali da prevenire il rischio di commissione degli illeciti contemplati nel Decreto;
- determinare nei predetti soggetti la consapevolezza di potere incorrere, in caso di violazione delle disposizioni impartite dalla Società, in conseguenze disciplinari e/o contrattuali, oltre che in sanzioni penali e amministrative comminabili nei loro confronti;
- istituire e/o rafforzare controlli che consentano alla Società di prevenire o di reagire tempestivamente per impedire la commissione di illeciti da parte dei soggetti apicali e delle persone sottoposte alla direzione o alla vigilanza dei primi che comportino la responsabilità amministrativa della Società;
- consentire alla Società, grazie a una azione di monitoraggio sulle aree di attività a rischio, di intervenire tempestivamente, al fine di prevenire o contrastare la commissione dei reati stessi e sanzionare i comportamenti contrari al proprio Modello;

- migliorare l'efficacia e la trasparenza nella gestione delle attività;
- determinare una piena consapevolezza nel potenziale autore dell'illecito che la commissione di un eventuale illecito è fortemente condannata e contraria – oltre che alle disposizioni di legge – sia ai principi etici ai quali la Società intende attenersi, sia agli stessi interessi della Società anche quando apparentemente potrebbe trarne un vantaggio.

### **3.2 Destinatari del Modello**

Le regole contenute nel Modello si applicano in primo luogo a coloro che svolgono funzioni di rappresentanza, amministrazione o direzione della Società nonché a chi esercita, anche di fatto, la gestione e il controllo della Società.

Il Modello si applica, inoltre, a tutti i dipendenti della Società, ivi compresi eventuali distaccati, i quali sono tenuti a rispettare, con la massima correttezza e diligenza, tutte le disposizioni e i controlli in esso contenuti, nonché le relative procedure di attuazione.

Il Modello si applica altresì, nei limiti del rapporto in essere, a coloro i quali, pur non appartenendo alla Società, operano su mandato o per conto della stessa o sono comunque legati alla Società da rapporti giuridici rilevanti. A tal fine, nei contratti o nei rapporti in essere con i suddetti soggetti, è espressamente previsto il riferimento al Codice Etico e di Condotta di Gruppo e al Modello.

In particolare con riferimento ad eventuali partners, in Italia e all'estero, con cui la Società può operare, pur nel rispetto dell'autonomia delle singole entità giuridiche, la Società si farà promotrice dell'adozione di un sistema di controllo interno atto a prevenire anche i reati presupposto del d.lgs.231/01 adoperandosi, attraverso la previsione di specifiche clausole contrattuali, per garantire che gli stessi uniformino la propria condotta ai principi posti dal Decreto e sanciti nel Codice Etico e di Condotta di Gruppo.

### **3.3 Struttura del Modello: Parte Generale e Parte Speciale**

Il Modello è articolato nella presente "Parte Generale", che ne contiene i principi fondamentali e in una "Parte Speciale", suddivisa in capitoli, il cui contenuto fa riferimento alle tipologie di reato previste dal Decreto e ritenute potenzialmente verificabili all'interno della Società.

La Parte Generale, dopo aver fornito le "definizioni" dei principali istituti e concetti presi in considerazione nel Modello, illustra dapprima i principi generali, i criteri ed i presupposti per l'attribuzione della responsabilità amministrativa degli Enti (individuazione dei soggetti attivi del reato-presupposto; loro "legame" con l'Ente; concetti di "interesse" o "vantaggio" dell'Ente; catalogo dei reati-presupposto della responsabilità amministrativa degli Enti; etc.), per poi chiarire quali sono le condizioni per l'esonero della responsabilità amministrativa degli Enti e, in assenza di quest'ultime, le gravi sanzioni amministrative applicabili all'Ente. Nella redazione del Modello si è

cercato di renderne il contenuto fruibile a tutti i livelli aziendali, al fine di determinare una piena consapevolezza in tutti coloro che operano in nome e per conto della Società, sia in relazione alla materia della responsabilità da reato degli Enti, sia con riferimento alle gravi conseguenze sanzionatorie in cui incorrerebbe la Società qualora venga commesso uno dei reati contemplati dal Decreto e dalla Legge 146/06.

Calandosi nel contesto aziendale, sono stati poi analizzati gli strumenti di governance, il sistema di controllo interno e l'assetto della Società.

Inoltre, vengono descritti gli obiettivi, la funzione e i destinatari del Modello, nonché la metodologia adottata per l'attività di redazione/aggiornamento del Modello di organizzazione, gestione e controllo.

La Parte Generale, infine, tratta dell'Organismo di Vigilanza e dei flussi informativi nei confronti di quest'ultimo, del sistema disciplinare e sanzionatorio dei principi di riferimento per la comunicazione e la formazione.

Nella "Parte Speciale" vengono affrontate le aree di attività della Società considerate a rischio in relazione alle diverse tipologie di reato previste dal Decreto e dalla Legge n. 146/2006 ritenute potenzialmente verificabili all'interno della Società.

In particolare, la Parte Speciale contiene una descrizione relativa a:

- le Attività Sensibili, ovvero quelle attività presenti nella realtà aziendale nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati di cui al punto precedente;
- i reati previsti dal D.Lgs. 231/01, astrattamente applicabili all'attività sensibile;
- gli standard di controllo generali delle attività posti alla base degli strumenti e delle metodologie utilizzate per strutturare gli standard di controllo specifici, che devono essere sempre presenti in tutte le Attività Sensibili prese in considerazione dal Modello;
- gli standard di controllo specifici, applicabili a singole attività sensibili, elaborati sulla base degli standard di controllo generali sopra riportati, quali misure di presidio individuate per mitigare il rischio specifico di commissione del singolo reato/categoria di reato.

In relazione alla descrizione normativa delle fattispecie e alla tipologia di attività svolta dalla Società, l'analisi delle aree potenzialmente a rischio consente ragionevolmente di escludere in astratto la rilevanza dei delitti in materia di falsità in monete, in carte di pubblico credito in valori in bollo e in strumento o segni di riconoscimento (ex art. 25-bis), dei reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (ex art. 25-quaterdecies), e dei reati contro la personalità individuale (di cui all'art. 25-quinquies) ad eccezione del reato di intermediazione

illecita e sfruttamento del lavoro. Infine, in alcun modo riferibile all'attività di YOROI S.r.l. è il delitto di mutilazione organi genitali femminili (art. 25-quater.1), i reati di razzismo e xenofobia (art. 25-terdecies), i reati di contrabbando (art. 25-sexiesdecies), nonché quelli contro il patrimonio culturale (art. 25-septiesdecies) e quelli di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-duodevicies).

Per quanto riguarda i reati associativi (anche transnazionali), si ritiene - sotto un profilo strettamente gestionale - che essi possano rappresentare, sempre in linea teorica, una particolare modalità di commissione dei reati individuati come rilevanti nella mappatura contenuta nel presente Modello. Di conseguenza i presidi previsti in relazione all'ipotetica realizzazione monosoggettiva degli stessi possono servire alla prevenzione della loro commissione in forma plurisoggettiva, stabile e organizzata.

Nell'eventualità in cui si rendesse necessario procedere all'emanazione di ulteriori specifici capitoli della Parte Speciale, relativamente a nuove fattispecie di reato che in futuro venissero ricomprese nell'ambito di applicazione del Decreto è demandato al Consiglio di Amministrazione della Società il potere di integrare il presente Modello mediante apposita delibera, anche su segnalazione e/o previa consultazione dell'Organismo di Vigilanza.

Le aree sensibili nel cui ambito possono essere commessi, in linea teorica, i reati presupposto sono le seguenti:

- Gestione dei rapporti con la Pubblica Amministrazione e le Autorità di Vigilanza;
- Erogazione servizi cybersecurity in favore di clienti;
- Gestione delle vendite;
- Gestione dei sistemi informativi;
- Comunicazioni verso l'esterno;
- Gestione delle informazioni privilegiate;
- Acquisti beni e servizi;
- Consulenze e incarichi professionali ai terzi;
- Gestione di sponsorizzazioni e di donazioni, omaggi e di altre liberalità;
- Gestione adempimenti in materia di salute e sicurezza sui luoghi di lavoro;
- Gestione della contabilità e delle attività di predisposizione del bilancio;
- Gestione degli adempimenti fiscali;
- Gestione finanza e tesoreria;
- Gestione del contenzioso;
- Affari societari;
- Gestione delle attività di merger & acquisition;
- Gestione delle risorse umane;
- Sistema di gestione ambientale;
- Gestione delle operazioni con parti correlate e dei rapporti infragruppo;
- Gestione dei rapporti con la società di revisione.

### **3.4 Il progetto della Società per la definizione del proprio Modello**

La Società ha deciso di procedere alla predisposizione e adozione del Modello in quanto consapevole che tale sistema, seppur costituendo una “facoltà” e non un obbligo, rappresenta un’opportunità per rafforzare la sua cultura di governance, cogliendo al contempo l’occasione dell’attività svolta (inventariazione delle Attività Sensibili, analisi dei rischi potenziali, valutazione e adeguamento del sistema dei controlli già esistenti sulle Attività Sensibili) per sensibilizzare le risorse impiegate rispetto ai temi del controllo dei processi, finalizzati a una prevenzione “attiva” dei reati.

La metodologia scelta per eseguire il progetto, in termini di organizzazione, definizione delle modalità operative, strutturazione in fasi, assegnazione delle responsabilità tra le varie funzioni, è stata elaborata al fine di garantire la qualità e l’autorevolezza dei risultati.

Il progetto è articolato nelle fasi sinteticamente di seguito riassunte, che esclusivamente per una spiegazione metodologica, sono evidenziate autonomamente.

#### **3.4.1 Individuazione delle aree, delle attività e dei processi sensibili**

L’art. 6, comma 2, lett. a) del d.lgs. 231/2001 indica, tra i requisiti del Modello, l’individuazione dei processi e delle attività nel cui ambito possono essere commessi i reati espressamente richiamati dal Decreto. Si tratta, in altri termini, di quelle attività e processi che comunemente vengono definiti “sensibili” (di seguito, “Attività Sensibili”, identificate nell’ambito delle cosiddette “Aree a Rischio”).

Scopo della prima fase è stato identificare gli ambiti oggetto dell’intervento e individuare preliminarmente le Attività Sensibili.

Propedeutica all’individuazione delle Attività Sensibili è l’analisi della struttura organizzativa della Società, svolta al fine di meglio comprendere l’attività della Società e di identificare gli ambiti oggetto dell’intervento.

L’analisi della struttura organizzativa della Società ha consentito l’individuazione dei processi / Attività Sensibili e la preliminare identificazione delle funzioni responsabili di tali processi/attività.

Qui di seguito sono elencate le attività svolte nella prima fase:

- raccolta della documentazione relativa alla struttura organizzativa della Società;
- analisi della documentazione raccolta per comprendere le attività svolte dalla Società;
- analisi storica (“case history”) dei casi già emersi nel passato relativi a precedenti penali, civili, o amministrativi nei confronti della Società o suoi dipendenti che abbiano eventuali punti di contatto con la normativa introdotta dal d.lgs. 231/2001;
- rilevazione degli ambiti di attività e delle relative responsabilità funzionali;

- individuazione preliminare dei processi / Attività Sensibili ex d.lgs. 231/2001;
- individuazione preliminare delle direzioni/funzioni responsabili delle Attività Sensibili identificate.

### **3.4.2 Identificazione dei Key Officer**

Scopo della seconda fase è stato identificare i responsabili dei processi / Attività Sensibili, ovvero le risorse con una conoscenza approfondita dei processi / Attività Sensibili e dei meccanismi di controllo attualmente in essere (di seguito, “key officer”), completando e approfondendo l’inventario preliminare dei processi / Attività Sensibili nonché delle funzioni e dei soggetti coinvolti.

Le attività operative per l’esecuzione della fase in oggetto presupponevano la raccolta delle informazioni necessarie per i) comprendere ruoli e responsabilità dei soggetti partecipanti alle Attività Sensibili e ii) identificare i key officer in grado di fornire il supporto operativo necessario a dettagliare le Attività Sensibili ed i relativi meccanismi di controllo.

In particolare, i key officer sono stati identificati nelle persone di più alto livello organizzativo in grado di fornire le informazioni di dettaglio sui singoli processi e sulle attività delle singole funzioni.

### **3.4.3 Analisi dei processi e delle Attività Sensibili**

Obiettivo della terza fase è stato analizzare e formalizzare, per ogni processo / Attività Sensibile individuato nelle fasi prima e seconda, le attività principali, le funzioni e i ruoli/responsabilità dei soggetti interni ed esterni coinvolti, gli elementi di controllo esistenti, al fine di verificare in quali aree/settori di attività e secondo quali modalità si potessero astrattamente realizzare le fattispecie di reato di cui al d.lgs. 231/2001.

L’attività che ha caratterizzato la terza fase ha riguardato l’esecuzione di interviste strutturate con i key officer al fine di raccogliere, per i processi / Attività Sensibili individuati nelle fasi precedenti, le informazioni necessarie a comprendere:

- i processi /attività svolte;
- le funzioni/soggetti interni/esterni coinvolti;
- i relativi ruoli/responsabilità;
- il sistema dei controlli esistenti.

In particolare, le interviste con i key officer hanno avuto lo scopo di:

- acquisire una visione sistematica di tutte le aree/settori di attività della società e del loro effettivo funzionamento;
- verificare l’effettività dei protocolli e delle procedure esistenti, ossia la rispondenza tra i comportamenti concreti e quelli previsti nei protocolli;
- identificare i rischi astratti dell’area/settore di attività oggetto di analisi, nonché i potenziali fattori di rischio;
- determinare l’esposizione al rischio (c.d. rischio inerente) mediante la

- valutazione dell'impatto dell'evento per la Società ("I") e della probabilità che l'illecito possa effettivamente verificarsi ("P");
- identificare i presidi e le attività esistenti a mitigazione dei rischi rilevanti, prendendo, tra l'altro, come riferimento, i seguenti principi di controllo:
    - esistenza di procedure formalizzate;
    - tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informativi;
    - segregazione dei compiti;
    - esistenza di deleghe formalizzate coerenti con le responsabilità organizzative assegnate;
  - valutare l'adeguatezza dei protocolli e delle procedure esistenti, ossia la loro capacità di prevenire il verificarsi di condotte illecite (o comunque di ridurre il rischio ad un livello accettabile) e di evidenziarne le modalità di eventuale realizzazione sulla base della rilevazione della situazione esistente in azienda (in relazione alle aree/attività "sensibili", alle aree/funzioni aziendali coinvolte ed ai controlli ed alle procedure esistenti);
  - determinare il livello di rischio residuo in considerazione dell'esistenza e dell'adeguatezza dei controlli rilevati. In particolare, la valutazione dell'adeguatezza del sistema di controllo interno esistente è stata esaminata in relazione al livello auspicabile e ritenuto ottimale di efficacia ed efficienza di protocolli e standard di controllo;
  - definire le eventuali aree di miglioramento.

Le informazioni acquisite nel corso delle interviste sono state poi sottoposte agli intervistati affinché gli stessi potessero condividere formalmente l'accuratezza e completezza delle stesse.

Al termine di tale fase è stata definita una "mappa dei processi / Attività Sensibili" che, in considerazione degli specifici contenuti, potrebbero essere esposte alla potenziale commissione dei reati richiamati dal d.lgs. 231/2001.

#### **3.4.4 Individuazione dei meccanismi correttivi: analisi di comparazione della situazione esistente rispetto al Modello a tendere**

Lo scopo della quarta fase è consistito nell'individuazione i) dei requisiti organizzativi caratterizzanti un modello organizzativo idoneo a prevenire i reati richiamati dal d.lgs. 231/2001 e ii) dei meccanismi correttivi intesi come le azioni di miglioramento del modello organizzativo esistente.

Al fine di rilevare ed analizzare in dettaglio il modello di controllo esistente a presidio dei rischi riscontrati e di valutare la conformità del modello stesso alle previsioni del d.lgs. 231/2001, è stata effettuata un'analisi comparativa tra il modello organizzativo e di controllo esistente e un modello astratto di riferimento valutato sulla base delle esigenze manifestate dalla disciplina di cui al d.lgs. 231/2001.

In particolare, il confronto è stato condotto in termini di compatibilità al sistema delle deleghe e dei poteri, al sistema delle procedure, al Codice Etico e di

Condotta di Gruppo.

Attraverso il confronto operato, è stato possibile desumere le aree di miglioramento del sistema di controllo interno esistente e i relativi meccanismi correttivi. Sulla scorta di quanto emerso, è stato predisposto un piano di attuazione, teso a individuare i requisiti organizzativi caratterizzanti un modello di organizzazione, gestione e controllo conforme a quanto disposto dal d.lgs. 231/2001, e le azioni di miglioramento dell'attuale sistema di controllo (processi e procedure).

#### **3.4.5 Predisposizione del Modello**

Terminate le fasi precedenti, è stato predisposto il presente documento che individua gli elementi costitutivi essenziali del Modello di organizzazione, gestione e controllo, articolato secondo le disposizioni del d.lgs. 231/2001 e le linee guida emanate da Confindustria.

Il Modello comprende i seguenti elementi costitutivi:

- individuazione delle attività della Società nel cui ambito possono essere commessi i reati richiamati dal d.lgs. 231/2001;
- standard dei controlli, generali e specifici, concernenti essenzialmente modalità di formazione e attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individuazione delle modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
- ruolo e compiti dell'Organismo di Vigilanza;
- flussi informativi da e verso l'Organismo di Vigilanza e specifici obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- sistema disciplinare atto a sanzionare la violazione delle disposizioni contenute nel Modello;
- principi generali per l'adozione del piano di formazione e comunicazione ai destinatari;
- criteri di aggiornamento del Modello.

L'aggiornamento del Modello organizzativo è stata effettuata sulla base dei risultati ottenuti e dall'analisi delle informazioni raccolte così da renderlo coerente al contesto aziendale.

#### **3.4.6 Criteri di aggiornamento del Modello**

L'Organismo di Vigilanza suggerisce al Consiglio di Amministrazione l'opportunità di procedere ad aggiornare il Modello, qualora gli elementi di novità – normativa o organizzativa e/o di assetto societario – siano tali da poter incidere sull'efficacia e sull'effettività dello stesso.

In particolare, il Modello potrà essere aggiornato qualora:

- si riscontrino violazioni delle prescrizioni del Modello;
- intervengano modifiche dell'assetto interno della Società;
- siano emanate modifiche alla normativa di riferimento.

In particolare, al fine di garantire che le variazioni del Modello siano operate con la necessaria tempestività ed efficacia, senza al contempo incorrere in difetti di coordinamento tra i processi operativi, le prescrizioni contenute nel Modello e la diffusione delle stesse, il Consiglio di Amministrazione ha ritenuto di delegare alla Funzione Legale il compito di apportare con cadenza periodica, ove risulti necessario, le modifiche al Modello che attengano ad aspetti di carattere descrittivo.

Si precisa che con l'espressione "aspetti descrittivi" si fa riferimento a elementi e informazioni che derivano da atti deliberati dal Consiglio di Amministrazione (come, ad esempio la ridefinizione dell'organigramma) o da funzioni munite di specifica delega (es. nuove procedure).

La Funzione Legale comunica tempestivamente all'OdV le eventuali modifiche apportate al Modello relative ad aspetti di carattere descrittivo e ne informa il Consiglio di Amministrazione, in occasione della prima riunione utile, al fine di farne oggetto di ratifica da parte dello stesso.

Rimane, in ogni caso, di esclusiva competenza del Consiglio di Amministrazione la delibera di aggiornamenti e/o di adeguamenti del Modello dovuti ai seguenti fattori:

- intervento di modifiche normative in tema di responsabilità amministrativa degli enti;
- identificazione di nuove Attività Sensibili, o variazione di quelle precedentemente identificate, anche eventualmente connesse all'avvio di nuove attività;
- commissione dei reati richiamati dal D.Lgs. 231/2001 da parte dei destinatari delle previsioni del Modello o, più in generale, di significative violazioni del Modello;
- riscontro di carenze e/o lacune nelle previsioni del Modello a seguito di verifiche sull'efficacia del medesimo.

L'OdV conserva, in ogni caso, precisi compiti e poteri in merito alla promozione del costante aggiornamento del Modello. A tal fine, formula osservazioni e proposte, attinenti all'organizzazione e il sistema di controllo, alle strutture a ciò preposte o, in casi di particolare rilevanza, al Consiglio di Amministrazione.

### **3.5 Estensione dei principi del Modello di TINEXTA S.p.A. alla Società**

La Società, al fine di evitare discrasie negli indirizzi e nei criteri adottati, nel predisporre e/o adeguare il proprio Modello, pur nel rispetto delle esigenze operative e con gli opportuni adattamenti resi necessari dalle proprie dimensioni e dalla realtà in cui opera, si attiene alle Linee Guida e si ispira ai principi del Modello adottato dalla controllante, recependone i contenuti, coerentemente con gli ambiti entro i quali si esplica l'attività di Direzione e Coordinamento svolta da TINEXTA S.p.A., in qualità di Capogruppo, relativamente alle tematiche del D.Lgs. 231/01.

## **4. ORGANISMO DI VIGILANZA**

### **4.1 I requisiti dell'Organismo di Vigilanza**

In base alle previsioni del Decreto, l'ente può essere esonerato dalla responsabilità conseguente alla commissione di reati da parte dei soggetti apicali o sottoposti alla loro vigilanza e direzione, se l'organo dirigente - oltre ad aver adottato ed efficacemente attuato un Modello di organizzazione idonei a prevenire i reati - ha affidato il compito di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo.

L'affidamento dei suddetti compiti ad un organismo dotato di autonomi poteri di iniziativa e controllo, unitamente al corretto ed efficace svolgimento degli stessi, rappresenta, quindi, presupposto indispensabile per l'esonero dalla responsabilità prevista dal Decreto.

I requisiti principali dell'Organismo di Vigilanza (quali richiamati anche dalla Linee Guida di Confindustria) possono essere così identificati:

- autonomia e indipendenza: l'organismo deve essere inserito come unità di staff in una posizione gerarchica la più elevata possibile e deve essere previsto un riporto al massimo vertice aziendale operativo. Inoltre, in capo al medesimo organismo non devono essere attribuiti compiti operativi che, per la loro natura, ne metterebbero a repentaglio l'obiettività di giudizio. Infine, deve poter svolgere la propria funzione in assenza di qualsiasi forma di interferenza e condizionamento da parte dell'ente, e, in particolare, del *management* aziendale;
- professionalità: l'organismo deve avere un bagaglio di conoscenze, strumenti e tecniche necessari per svolgere efficacemente la propria attività;
- continuità di azione: per un'efficace e costante attuazione del modello organizzativo, attraverso l'espletamento di verifiche periodiche. La continuità di azione può essere favorita, ad esempio, dalla partecipazione alle riunioni dell'Organismo di Vigilanza di un dipendente della società che, per le mansioni svolte, sia in grado di garantire una presenza costante all'interno della società, pur senza svolgere, ovviamente, funzioni soggette al controllo dell'Organismo di Vigilanza.

L'Organismo di Vigilanza di YOROI S.r.l. è un organismo pluripersonale composto da tre soggetti, interni ed esterni alla Società, esperti nelle materie connesse alle discipline previste dal Decreto (quali, a titolo esemplificativo, materie giuridiche, aziendali, contabili, fiscali e conoscenza delle tecniche di conduzione di audit interni).

L'Organismo di Vigilanza è istituito con delibera del Consiglio di Amministrazione. I suoi membri restano in carica per la durata del mandato del Consiglio di Amministrazione che lo ha nominato.

Alla scadenza del termine, i membri dell'Organismo di Vigilanza rimangono in carica fino a quando intervengano nuove nomine deliberate dal Consiglio di

Amministrazione. Se nel corso della carica, uno o più membri dell'Organismo di Vigilanza cessano per qualsiasi motivo dal loro incarico, il Consiglio di Amministrazione provvede senza indugio alla loro sostituzione con propria delibera.

Il compenso per la carica di membro dell'Organismo di Vigilanza, per tutta la durata del mandato, è stabilito nella delibera del Consiglio di Amministrazione che ha provveduto alla nomina.

La nomina quale componente dell'Organismo di Vigilanza è condizionata alla presenza dei requisiti soggettivi di eleggibilità. All'atto del conferimento dell'incarico, il soggetto designato a ricoprire la carica di componente dell'Organismo di Vigilanza deve rilasciare una dichiarazione nella quale attesta l'assenza delle seguenti cause di ineleggibilità e/o incompatibilità, oltre a quelle eventualmente previste da norme applicabili:

- conflitti di interesse, anche potenziali, con la società tali da pregiudicare l'indipendenza richiesta dal ruolo e dai compiti propri quale membro dell'Organismo di Vigilanza;
- i soggetti legati da relazioni di parentela, coniugio (o situazioni di convivenza di fatto equiparabili al coniugio) o affinità entro il quarto grado degli amministratori, sindaci e revisori delle Società, dei soggetti apicali, nonché degli amministratori di società controllanti o di società controllate;
- titolarità, diretta o indiretta, di partecipazioni azionarie di entità tale da permettere di esercitare una notevole influenza sulla società;
- i soggetti con funzioni di amministrazione, con deleghe o incarichi esecutivi presso le Società o presso altre società del gruppo;
- sentenza di condanna, anche non passata in giudicato, ovvero sentenza di applicazione della pena su richiesta (il c.d. patteggiamento) per i delitti richiamati dal Decreto, o che per la loro particolare gravità incidano sull'affidabilità morale e professionale del soggetto;
- condanna, con sentenza, anche non passata in giudicato, a una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

I sopra richiamati motivi di incompatibilità e/o ineleggibilità e la connessa autocertificazione devono essere considerati anche con riferimento ad eventuali consulenti esterni coinvolti nell'attività e nello svolgimento dei compiti propri dei membri dell'Organismo di Vigilanza.

La cessazione della carica è determinata da rinuncia, decadenza, revoca e, per quanto riguarda i componenti nominati in ragione della funzione di cui siano titolari in ambito aziendale, dal venir meno della titolarità di questa.

La rinuncia da parte dei componenti dell'OdV può essere esercitata in qualsiasi momento e deve essere comunicata al Consiglio di Amministrazione per iscritto, unitamente alle motivazioni che l'hanno determinata.

I componenti dell'Organismo di Vigilanza possono essere revocati

esclusivamente per giusta causa, sentito il parere non vincolante del Collegio Sindacale, mediante un'apposita delibera del Consiglio di Amministrazione. A tale proposito, per giusta causa di revoca dovrà intendersi, a titolo esemplificativo:

- l'interdizione o l'inabilitazione, ovvero una grave infermità che renda il componente dell'Organismo di Vigilanza inidoneo a svolgere le proprie funzioni di vigilanza, o un'infermità che, comunque, comporti la sua assenza per un periodo superiore a sei mesi;
- l'attribuzione al componente dell'Organismo di Vigilanza di funzioni e responsabilità operative, ovvero il verificarsi di eventi, incompatibili con i requisiti di autonomia di iniziativa e di controllo, indipendenza e continuità di azione, che sono propri dell'Organismo di Vigilanza;
- la perdita dei requisiti soggettivi di onorabilità, integrità, rispettabilità e indipendenza presenti in sede di nomina;
- la sussistenza di una o più delle citate cause di ineleggibilità e incompatibilità;
- un grave inadempimento dei doveri propri dell'Organismo di Vigilanza.

In tali ipotesi, il Consiglio di Amministrazione provvede tempestivamente a nominare il nuovo componente dell'Organismo di Vigilanza in sostituzione di quello revocato. Qualora, invece, la revoca venga esercitata nei confronti di tutti i componenti dell'Organismo di Vigilanza, il Consiglio di amministrazione provvederà a nominare contestualmente un nuovo Organismo di Vigilanza, al fine di assicurare continuità di azione allo stesso.

L'Organismo di Vigilanza potrà giovare – sotto la sua diretta sorveglianza e responsabilità – nello svolgimento dei compiti affidatigli, della collaborazione di tutte le funzioni e strutture della società ovvero di consulenti esterni – previa sottoscrizione di apposito contratto – avvalendosi delle rispettive competenze e professionalità. L'Organismo di Vigilanza si dota di un Regolamento. Le riunioni dell'organismo devono constare di verbali debitamente registrati in un libro verbali custodito dallo stesso Organismo di Vigilanza presso la sede della Società

All'Organismo di Vigilanza è affidato il compito di:

1. vigilare sull'osservanza delle prescrizioni del Modello, in relazione alle diverse tipologie di reati contemplate dal Decreto e dalle successive leggi che ne hanno esteso il campo di applicazione, attraverso la definizione di un piano delle attività finalizzato anche alla verifica della rispondenza tra quanto astrattamente previsto dal Modello ed i comportamenti concretamente tenuti dai soggetti obbligati al suo rispetto;
2. verificare l'adeguatezza del Modello sia rispetto alla prevenzione della commissione dei reati richiamati dal d.lgs. 231/2001 sia con riferimento alla capacità di far emergere il concretizzarsi di eventuali comportamenti illeciti;
3. verificare l'efficienza e l'efficacia del Modello anche in termini di rispondenza tra le modalità operative adottate in concreto e le procedure formalmente

previste dal Modello stesso;

4. verificare il mantenimento nel tempo dei requisiti di efficienza ed efficacia del Modello;
5. svolgere, anche attraverso le funzioni preposte, periodica attività ispettiva e di controllo, di carattere continuativo e a sorpresa, in considerazione dei vari settori di intervento o delle tipologie di attività e dei loro punti critici al fine di verificare l'efficienza e l'efficacia del Modello;
6. segnalare l'eventuale necessità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione alle mutate condizioni aziendali, all'evoluzione normativa o ad ipotesi di violazione dei suoi contenuti;
7. monitorare il periodico aggiornamento del sistema di identificazione, mappatura e classificazione delle Attività Sensibili;
8. rilevare gli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie funzioni;
9. con riferimento alla segnalazione degli illeciti verificare l'adeguatezza dei canali informativi predisposti in applicazione della disciplina sul whistleblowing affinché gli stessi siano tali da assicurare la compliance alla normativa di riferimento;
10. con riferimento alle segnalazioni degli illeciti il ruolo di Gestore delle segnalazioni, mediante designazione apposita da parte dell'organo amministrativo;
11. promuovere l'attivazione di eventuali procedimenti disciplinari;
12. verificare e valutare, insieme alle funzioni preposte, l'idoneità del sistema disciplinare ai sensi e per gli effetti del d.lgs. 231/2001, vigilando sul rispetto del divieto di "atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione".
13. promuovere le iniziative per la diffusione della conoscenza e della comprensione del Modello, nonché per la formazione del personale e la sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello;
14. promuovere interventi di comunicazione e formazione sui contenuti del d.lgs. 231/2001, sugli impatti della normativa sull'attività della Società e sulle norme comportamentali.

Per perseguire i suoi fini l'Organismo di Vigilanza deve:

- esaminare eventuali segnalazioni ricevute ed effettuare gli accertamenti necessari ed opportuni;
- segnalare tempestivamente all'organo dirigente, per gli opportuni provvedimenti, le violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo alla Società;

- coordinarsi con la funzione Risorse Umane per i programmi di formazione del personale;
- aggiornare la lista delle informazioni che devono essergli trasmesse o tenute a sua disposizione;
- riferire periodicamente al Consiglio di Amministrazione e al Collegio Sindacale in merito all'attuazione del Modello;

Per svolgere i propri compiti, i membri dell'Organismo di Vigilanza hanno libero accesso presso tutte le funzioni della Società e alla documentazione aziendale, senza necessità di alcun consenso preventivo.

Il Consiglio di Amministrazione curerà l'adeguata comunicazione alle strutture dei compiti dell'Organismo di Vigilanza e dei suoi poteri.

All'OdV non competono poteri di gestione o poteri decisionali relativi allo svolgimento delle attività della Società, poteri organizzativi o di modifica della struttura della Società, né poteri sanzionatori. L'OdV, nonché i soggetti dei quali l'Organismo di Vigilanza, a qualsiasi titolo, si avvale, sono tenuti a rispettare l'obbligo di riservatezza su tutte le informazioni delle quali sono venuti a conoscenza nell'esercizio delle loro funzioni.

Nel contesto delle procedure di formazione del budget, il Consiglio di Amministrazione dovrà approvare una dotazione adeguata di risorse finanziarie della quale l'Organismo di Vigilanza potrà disporre per ogni esigenza necessaria al corretto svolgimento dei compiti (es. consulenze specialistiche, trasferte, gestione delle segnalazioni whistleblowing, ecc.).

## **4.2 Reporting dell'Organismo di Vigilanza verso gli organi societari**

L'Organismo di Vigilanza riferisce in merito all'attuazione del Modello, all'emersione di eventuali aspetti critici, alla necessità di interventi modificativi. Sono previste due distinte linee di reporting:

- la prima, su base continuativa, direttamente verso l'Amministratore Delegato e il Presidente;
- la seconda, su base periodica semestrale, nei confronti del Consiglio di Amministrazione e del Collegio Sindacale.

L'Organismo di Vigilanza:

i) riporta all'Amministratore Delegato e al Presidente rendendoli edotti, ogni qual volta lo ritenga opportuno, su circostanze e fatti significativi del proprio ufficio. L'OdV comunica immediatamente il verificarsi di situazioni straordinarie (ad esempio: significative violazioni dei principi contenuti nel Modello emerse a seguito dell'attività di vigilanza, innovazioni legislative in materia di responsabilità amministrativa degli enti, ecc.) e le segnalazioni ricevute che rivestono carattere d'urgenza;

ii) presenta una relazione scritta al Consiglio di Amministrazione e al Collegio Sindacale, su base periodica semestrale, che deve contenere quanto meno le seguenti informazioni:

- a) la sintesi delle attività svolte nel semestre e, in occasione della relazione

annuale, il piano delle attività previste per l'anno successivo;

b) eventuali problematiche o criticità che siano scaturite nel corso dell'attività di vigilanza; in particolare, qualora non oggetto di precedenti e apposite segnalazioni:

- le azioni correttive da apportare al fine di assicurare l'efficacia e/o l'effettività del Modello, ivi incluse quelle necessarie a rimediare alle carenze organizzative o procedurali accertate ed idonee ad esporre la Società al pericolo che siano commessi reati rilevanti ai fini del Decreto, inclusa una descrizione delle eventuali nuove attività "sensibili" individuate;

- sempre nel rispetto dei termini e delle modalità indicati nel sistema disciplinare adottato dalla Società ai sensi del Decreto, l'indicazione dei comportamenti accertati e risultati non in linea con il Modello;- il resoconto delle segnalazioni ricevute, ivi incluso quanto direttamente riscontrato, in ordine a presunte violazioni delle previsioni del presente Modello, del Codice Etico e di Condotta di Gruppo, dei protocolli di prevenzione e delle relative procedure di attuazione, delle policy ESG; nonché le violazioni del diritto dell'Unione Europea e gli illeciti amministrativi, contabili, civili o penali; e l'esito delle conseguenti verifiche effettuate;- informativa in merito all'eventuale commissione di reati rilevanti ai fini del Decreto;- i provvedimenti disciplinari e le sanzioni eventualmente applicate dalla Società, con riferimento alle violazioni delle previsioni del presente Modello, dei protocolli di prevenzione e delle relative procedure di attuazione;- una valutazione complessiva sul funzionamento e l'efficacia del Modello con eventuali proposte di integrazioni, correzioni o modifiche;- la segnalazione degli eventuali mutamenti del quadro normativo e/o significative modificazioni dell'assetto interno della Società che richiedono un aggiornamento del Modello;- il rendiconto delle spese sostenute.

Gli incontri con gli organi sociali, cui l'Organismo di Vigilanza riferisce, devono essere documentati.

### **4.3 Informativa verso l'Organismo di Vigilanza**

Per quanto concerne l'attività di reporting di carattere generale verso l'Organismo di Vigilanza essa deve avvenire in forma strutturata e deve avere ad oggetto:

1) i seguenti report, prodotti con periodicità trimestrale :

- report informativo di sintesi delle principali attività svolte ai fini della prevenzione e protezione dai rischi sui luoghi di lavoro (segnalazioni pervenute, rilievi a seguito di ispezioni, infortuni registrati e altri accadimenti, verbale della riunione periodica) e dell'efficacia e adeguatezza del sistema in materia di SSL e dei provvedimenti di gestione adottati;
- report degli ordini di acquisto inseriti nel sistema contabile e approvati

nel trimestre di riferimento con evidenza del valore dell'ordine, del nome del fornitore e del conto contabile di destinazione del costo, nonché di quelli conferiti tramite affidamento diretto; elenco degli incarichi di consulenza sottoscritti con evidenza di quelli conferiti tramite affidamento diretto;

- elenco delle liberalità, contributi, sponsorizzazioni e omaggi nonché delle spese di rappresentanza di entità superiore al “modico valore” qualificato nella documentazione aziendale (beneficiario, importo, data del versamento);
  - elenco delle assunzioni, e relativo processo di selezione, con la eventuale indicazione delle assunzioni effettuate extra budget;
  - lista delle nuove emissioni delle disposizioni aziendali (modelli, direttive, regolamenti, procedure, organigrammi, deleghe, poteri, etc.) relative alle attività sensibili indicate nel Modello;
  - elenco cause giudiziarie ed arbitrati in corso;
- 2) le seguenti informative, prodotte al verificarsi degli eventi di seguito elencati:
- report del DPO su eventuali violazioni della sicurezza informatica (“data breach”);
  - report del DPO sulle modalità di trattamento dei dati personali da parte del Titolare, anche con riguardo al profilo delle misure di sicurezza adottate e adeguate al livello di rischio;
  - esiti di ispezioni/verifiche da parte di soggetti pubblici (Ispettorato del lavoro, VV.F, INAIL, ASL, enti locali, Guardia di Finanza, etc.);
  - accordi transattivi a fronte di contenziosi o azioni legali attivati;
  - provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal D. Lgs. n. 231/2001 e che possano coinvolgere la società;
  - richieste di assistenza legale inoltrate dagli amministratori, dai dirigenti e/o dagli altri dipendenti in caso di avvio di procedimento giudiziario nei loro confronti ed in relazione ai reati di cui al D. Lgs. n. 231/2001, salvo espresso divieto dell'autorità giudiziaria;
  - rapporti preparati dai responsabili delle principali aree/funzioni interne (referente in materia di L. 262/05, etc.) , Internal Audit, Compliance, Controllo di Gestione o di altre funzioni aziendali di Gruppo nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili critici rispetto all'osservanza delle norme e previsioni del Modello;
  - notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate (ivi compresi i provvedimenti assunti verso i dipendenti) ovvero dei provvedimenti di archiviazione di tali

- procedimenti con le relative motivazioni;
- esiti delle delibere degli organi societari che possano comportare modifiche nella funzionalità e articolazione del Modello (es. variazioni della struttura organizzativa, modifiche della governance e modifiche delle linee di business);
  - qualsiasi altro atto o documenti con profili di criticità rispetto all'osservanza delle norme del Decreto o delle previsioni del Modello;
  - ogni altra informazione che, sebbene non ricompresa nell'elenco che precede, risulti rilevante ai fini di una corretta e completa attività di vigilanza ed aggiornamento del Modello.

In ambito aziendale dovrà essere portata a conoscenza dell'Organismo di Vigilanza, oltre alla documentazione prescritta nelle singole parti del Modello, ogni informazione, proveniente anche da terzi ed attinente all'attuazione del Modello stesso nelle aree di attività a rischio. In particolare, i membri degli organi societari, i dipendenti e le terze parti devono trasmettere all'Organismo di Vigilanza ogni informazione attinente a presumibili:

- violazioni del diritto dell'Unione Europea, in via meramente esemplificativa e non esaustiva, in materia di: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
- illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del Decreto Legislativo n. 231/2001 o violazioni (anche presunte) del Modello di Organizzazione, Gestione e Controllo della Società;
- violazioni del Codice Etico e di Condotta della Società;
- violazioni, presunte o accertate, delle procedure della Società o, comunque, del sistema normativo interno;
- violazioni in materia ESG.

A tal fine il segnalante deve presentare segnalazioni circostanziate<sup>2</sup> di presunte condotte illecite che siano fondate su elementi di fatto precisi e concordanti<sup>3</sup>.

La Società, in conformità a quanto previsto dalla normativa in materia di whistleblowing, ha attivato una piattaforma di segnalazione «Comunica

---

<sup>2</sup> Per segnalazione circostanziata si intende una segnalazione che contenga un grado di dettaglio sufficiente a consentire, almeno astrattamente, alle Funzioni/soggetti coinvolti nella gestione delle segnalazioni, di identificare elementi utili o decisivi ai fini della verifica della fondatezza della segnalazione stessa (ad esempio: tipologia di illecito commesso, periodo di riferimento, cause e finalità dell'illecito, persone/Funzioni aziendali coinvolte, anomalie riscontrate nel sistema di controllo interno, ecc.).

<sup>3</sup> Gli elementi (o indizi) si definiscono precisi quando non sono suscettibili di diverse interpretazioni e concordanti quando più elementi confluiscono necessariamente nella stessa direzione.

Whistleblowing» accessibile al sito:

<https://digitalplatform.unionefiduciaria.it/whistleblowingnew/it/accessoprincipale/identificazionegruppo?TOKEN=TINEXTAWB4>

Attraverso tale piattaforma di segnalazione la Società garantisce, attraverso sistemi crittografati, la riservatezza dell'identità del segnalante e delle informazioni contenute nella segnalazione.

La gestione delle segnalazioni da parte dell'Organismo di Vigilanza si suddivide in quattro fasi:

- Presa in carico;
- Istruttoria;
- Accertamento;
- Sanzioni/azioni di miglioramento;

Inoltre, in via residuale, sono mantenute:

- una casella e-mail aperta, a cura dell'Organismo di Vigilanza e pubblicata sul sito internet della Società, per effettuare segnalazioni di rilevanza 231 e per trasmettere i flussi informativi da e verso l'OdV;
- la posta prioritaria con l'indicazione di "RISERVATO" sulla busta indirizzata a: Organismo di Vigilanza, c/o YOROI S.r.l., Piazza Sallustio n.9 – 00187 - Roma.

Al fine di promuovere la diffusione e la conoscenza da parte delle società del Gruppo della metodologia e degli strumenti di attuazione del Modello, l'Organismo di Vigilanza di Tinexta S.p.A. incontra periodicamente gli Organismi di Vigilanza delle società controllate. Tali incontri sono dedicati ad esaminare e condividere le esperienze significative maturate.

Gli incontri hanno luogo almeno con cadenza annuale. Il calendario degli incontri è definito dall'Organismo di Vigilanza di TinextaS.p.A. in condivisione con gli Organismi di Vigilanza delle società controllate. La convocazione avviene a cura del presidente dell'Organismo di Vigilanza di S.p.A. ed è trasmessa agli interessati via e-mail almeno quindici giorni prima dell'incontro.

#### **4.4 Raccolta e conservazione delle informazioni**

Ogni informazione, segnalazione, report, relazione previsti nel Modello sono conservati dall'Organismo di Vigilanza in un apposito archivio (informatico o cartaceo) per un tempo non inferiore a 10 anni.

Per quanto concerne, invece, le segnalazioni, queste devono essere archiviate e conservate per un periodo non superiore a 5 anni.

---

<sup>4</sup> Le modalità di segnalazione sono riportate all'interno di un'apposita istruzione operativa pubblicata sul sito della Società.

## **5. SISTEMA DISCIPLINARE E SANZIONATORIO**

### **5.1 Principi generali**

L'efficace attuazione del Modello è assicurata anche dalla previsione e predisposizione, in YOROI S.r.l., di un adeguato sistema disciplinare e sanzionatorio per la violazione delle regole di condotta imposte dal citato Modello ai fini della prevenzione dei reati di cui al Decreto, e, in generale, delle procedure interne (cfr. art. 6, comma secondo, lett. e, art. 7, comma quarto, lett. b).

L'applicazione delle sanzioni disciplinari prescinde dall'effettiva commissione di un reato e, quindi, dalla instaurazione e dall'esito di un eventuale procedimento penale. Le regole di condotta imposte dal Modello sono, infatti, assunte dall'azienda in piena autonomia, al fine del miglior rispetto del precetto normativo che sull'azienda stessa incombe.

Le sanzioni disciplinari potranno quindi essere applicate dalla Società ad ogni violazione del presente Modello e del Codice Etico di Condotta di Gruppo, indipendentemente dalla commissione di un reato e dallo svolgimento e dall'esito di un processo penale avviato dall'Autorità Giudiziaria.

La violazione delle singole disposizioni del presente Modello e del Codice Etico e di Condotta di Gruppo costituiscono sempre illecito disciplinare.

In ogni caso, l'Organismo di Vigilanza deve essere informato del procedimento di irrogazione delle sanzioni disciplinari o dell'eventuale archiviazione.

La Società cura l'informazione di tutti i soggetti sopra previsti, sin dal sorgere del loro rapporto di lavoro, circa l'esistenza ed il contenuto del presente apparato sanzionatorio.

### **5.2 Condotte sanzionabili: categorie fondamentali**

Sono sanzionabili le azioni poste in essere in violazione del Codice Etico e di Condotta di Gruppo, del Modello e delle procedure operative interne e la mancata ottemperanza ed eventuali indicazioni e prescrizioni provenienti dall'Organismo di Vigilanza.

Le violazioni sanzionabili possono essere suddivise in quattro categorie fondamentali secondo un ordine di gravità crescente:

- violazioni non connesse alle Attività Sensibili;
- violazioni connesse alle Attività Sensibili;
- violazioni idonee ad integrare il solo fatto (elemento oggettivo) di uno dei reati per i quali è prevista la responsabilità amministrativa delle persone giuridiche;
- violazioni finalizzate alla commissione di reati previsti dal Decreto 231/2001 o che, comunque, comportino la possibilità di attribuzione di responsabilità amministrativa in capo alla Società.

A titolo esemplificativo, costituiscono condotte sanzionabili:

- la mancata osservanza di procedure prescritte nel Modello e/o ivi richiamate;

- l'inosservanza di obblighi informativi prescritti nel sistema di controllo;
- l'omessa o non veritiera documentazione delle operazioni in conformità al principio di trasparenza;
- l'omissione di controlli da parte di soggetti responsabili;
- il mancato rispetto non giustificato degli obblighi informativi;
- l'adozione di qualsiasi atto elusivo dei sistemi di controllo;
- l'adozione di comportamenti che espongono la Società alla comunicazione delle sanzioni previste dal D. Lgs.231/2001;
- le violazioni delle misure di tutela del segnalante nonché l'effettuazione, con dolo o colpa grave, di segnalazioni che si rivelino infondate.

### **5.3 Soggetti**

Sono soggetti al sistema sanzionatorio e disciplinare, di cui al presente Modello, tutti i lavoratori Dipendenti, i Dirigenti, gli Amministratori e i Collaboratori della Società, nonché tutti coloro che abbiano rapporti contrattuali con la società, in virtù di apposite clausole contrattuali.

Qualora presso la Società svolgano la propria attività lavorativa uno o più dipendenti distaccati di una società del Gruppo, tali soggetti sono tenuti al rispetto di quanto previsto dal Codice Etico e di Condotta di Gruppo e dal presente Modello.

### **5.4 Violazioni del modello e relative sanzioni**

La Società ha predisposto, in conformità alla normativa vigente ed al principio di tipicità delle violazioni e delle sanzioni, le regole comportamentali contenute nel Modello e nel Codice Etico e di Condotta di Gruppo, la cui violazione costituisce illecito disciplinare, nonché le sanzioni applicabili, proporzionate alla gravità delle infrazioni.

Si ritiene opportuno rinviare al Codice Etico e di Condotta di Gruppo, nel quale sono riportate le possibili violazioni poste in essere dal dipendente e le corrispondenti sanzioni comminabili.

È fatto salvo il diritto della Società di richiedere il risarcimento del danno derivante dalla violazione del Modello, che sarà commisurato:

1. al livello di autonomia del dipendente;
2. alla gravità delle conseguenze della violazione, ovvero le possibili implicazioni in materia di D. Lgs. n. 231/01;
3. al livello di intenzionalità del comportamento;
4. all'eventuale presenza di precedenti sanzioni disciplinari irrogate.

In conformità a quanto previsto dall'art. 6, comma 2-bis, D.Lgs. 231/01 e ss.mm.ii. nel caso di:

- (i) atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla

## Segnalazione

- (ii) violazione, da parte dell'organo deputato a ricevere e/o a gestire la Segnalazione, degli obblighi di riservatezza dell'identità del segnalante
- (iii) mancata attivazione, da parte dell'organo deputato a ricevere e/o a gestire la Segnalazione, delle necessarie verifiche volte a valutare la fondatezza dei fatti oggetto di Segnalazione
- (iv) effettuazione, con dolo o colpa grave, di Segnalazioni infondate si provvederà ad applicare nei confronti del soggetto che ha posto in essere anche solo una delle suddette fattispecie le misure disciplinari di cui ai paragrafi seguenti in funzione della relativa posizione aziendale ricoperta.

Il responsabile dell'avvio e dello svolgimento del procedimento disciplinare è la funzione Risorse Umane, la quale deve tenere costantemente informato l'Organismo sull'andamento del procedimento, le giustificazioni addotte, l'esito e qualsiasi altra informazione possa essere di interesse per il citato Organismo.

### **5.5 Misure nei confronti dei dipendenti**

I lavoratori subordinati devono rispettare gli obblighi stabiliti dall'art. 2104 c.c., obblighi dei quali il presente Modello ed il Codice Etico e di Condotta adottato dal Gruppo, rappresentano parte integrante.

È opportuno evidenziare che, tra i dipendenti, vi sono i soggetti di qualifica non dirigenziale che sono sottoposti al Contratto Collettivo Nazionale Metalmeccanico e del Commercio. Per i dipendenti di livello non dirigenziale, le sanzioni irrogabili, conformemente a quanto previsto dall'art. 7 delle Legge n. 300/1970 (c.d. Statuto dei Lavoratori) ed eventuali normative speciali applicabili, sono quelle previste dalla legge, nonché dall'apparato sanzionatorio dei contratti di lavoro. In particolare, il richiamato CCNL prevede, a seconda della gravità delle violazioni, i seguenti provvedimenti:

- richiamo verbale,
- richiamo scritto,
- sospensione dal servizio e dal trattamento economico,
- licenziamento per giustificato motivo,
- licenziamento per giusta causa.

### **5.6 Misure nei confronti dei dirigenti**

I soggetti di qualifica dirigenziale sono sottoposti al Contratto Nazionale normativo ed economico per i dirigenti Industria di Confindustria e al Contratto Dirigenti per i dirigenti di aziende del terziario, della distribuzione e dei servizi. In caso di violazione del Modello o del Codice Etico e di Condotta di Gruppo da

parte dei dirigenti, la Società provvederà ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto normativamente previsto.

Nel caso in cui la violazione interrompa il rapporto fiduciario tra la Società e il dirigente, la sanzione è quella del licenziamento per giusta causa.

### **5.7 Misure nei confronti di amministratori e sindaci**

In caso di violazione del Modello o del Codice Etico e di Condotta di Gruppo da parte di un membro del Consiglio di Amministrazione, l'Organismo di Vigilanza procede a darne immediata comunicazione all'intero Consiglio di Amministrazione ed al Collegio Sindacale, esprimendo parere in merito alla gravità dell'infrazione. Il Consiglio di Amministrazione, sentito il parere del Collegio Sindacale, è competente ad assumere gli opportuni provvedimenti, sino ad arrivare, nei casi di gravi infrazioni, alla convocazione dell'assemblea dei soci, al fine di esporre a tale organo i fatti accertati e adottare le deliberazioni ritenute necessarie.

Il membro o i membri del Consiglio di Amministrazione della cui infrazione si discute saranno tenuti ad astenersi dalle relative deliberazioni.

Qualora le violazioni siano commesse da un numero di membri del Consiglio di Amministrazione tale da impedire all'Organo in questione di deliberare, l'Organismo di Vigilanza dovrà darne immediata comunicazione al Collegio Sindacale perché si attivi ai sensi di legge, convocando in particolare l'Assemblea dei soci per l'adozione delle misure necessarie.

In caso di violazione del Modello o del Codice Etico e di Condotta di Gruppo da parte di un membro del Collegio Sindacale, l'Organismo di Vigilanza procede a darne immediata comunicazione all'intero Collegio Sindacale e al Consiglio di Amministrazione, esprimendo parere in merito alla gravità dell'infrazione.

Il Collegio, sentito il parere del Consiglio di Amministrazione, provvederà ad assumere gli opportuni provvedimenti, in conformità alla normativa vigente, e nei casi di gravi infrazioni, convocherà l'Assemblea dei soci al fine di esporre a tale organo i fatti accertati e per adottare le deliberazioni ritenute necessarie.

Qualora le violazioni siano commesse da più membri del Collegio Sindacale, l'Organismo di Vigilanza dovrà darne immediata e diretta comunicazione al Consiglio di Amministrazione perché si attivi ai sensi di legge, convocando in particolare l'Assemblea dei soci per l'adozione delle misure necessarie.

### **5.8 Misure nei confronti degli altri destinatari**

La violazione da parte di consulenti, collaboratori e partners commerciali delle disposizioni del Codice Etico e di Condotta di Gruppo ai medesimi applicabili è sanzionata secondo quanto stabilito nelle clausole contrattuali di riferimento.

Resta inteso che tutti i soggetti esterni aventi rapporti contrattuali con la Società devono impegnarsi per iscritto, all'atto di sottoscrizione del contratto, al rispetto del Codice Etico e di Condotta di Gruppo.

## **6. COMUNICAZIONE E FORMAZIONE DEL PERSONALE**

### **6.1 Formazione e diffusione del Modello**

La Società, al fine di dare efficace attuazione al Modello, assicura una corretta divulgazione dei contenuti e dei principi dello stesso all'interno e all'esterno della propria organizzazione.

Obiettivo della Società è quello di comunicare i contenuti e i principi del Modello anche ai soggetti che, pur non rivestendo la qualifica formale di dipendente, operano – anche occasionalmente – per il conseguimento degli obiettivi della Società in forza di rapporti contrattuali.

La Società, infatti, intende:

- determinare, in tutti coloro che operano in suo nome e per suo conto nelle attività “sensibili”, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni;
- informare tutti coloro che operano a qualsiasi titolo in suo nome, per suo conto o comunque nel suo interesse che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni ovvero la risoluzione del rapporto contrattuale;
- ribadire che la Società non tollera comportamenti illeciti, di qualsiasi tipo e indipendentemente da qualsiasi finalità, in quanto tali comportamenti (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono comunque contrari ai principi etici cui la Società intende attenersi.

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D. Lgs. n. 231/2001 è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno i destinatari funzioni di rappresentanza della Società.

La Società cura l'adozione e l'attuazione di un adeguato livello di formazione mediante il supporto della Funzione Education & Talent Management di Tinexta, avvalendosi di idonei strumenti di diffusione quali:

- meeting aziendali;
- e-mail ai dipendenti;
- intranet aziendale (continuamente aggiornata);
- predisposizione di questionari di verifica dell'efficacia formativa raggiunta.

La formazione deve vertere sulla completa conoscenza e comprensione delle seguenti aree:

- il D.Lgs. 231/2001: i principi generali, i reati previsti (anche quelli di cui alla

Legge n. 146/2006) e le sanzioni applicabili alla Società;

- i principi di comportamento contenuti nel Modello e nel Codice Etico e di Condotta di Gruppo;
- i poteri dell'Organismo di Vigilanza, nonché gli obblighi informativi nei suoi confronti;
- il sistema disciplinare;
- il sistema di segnalazione degli illeciti (c.d. whistleblowing).

## **6.2 Componenti degli organi sociali, dipendenti, dirigenti e quadri**

L'Organismo di Vigilanza promuove, mediante la predisposizione di appositi piani comunicati al Consiglio di Amministrazione ed implementati dalla Società, le attività di formazione ed informazione del Modello.

La diffusione del Modello e l'informazione del personale in merito al contenuto del D. Lgs. n. 231/2001 e ai suoi obblighi relativamente all'attuazione dello stesso sono costantemente realizzate attraverso i vari strumenti a disposizione della Società.

L'attività di formazione e di informazione riguarda tutto il personale, compreso il personale direttivo e prevede, oltre ad una specifica informativa all'atto dell'assunzione, lo svolgimento di ulteriori attività ritenute necessarie al fine di garantire la corretta applicazione delle disposizioni previste nel D. Lgs. n. 231/2001.

L'adozione del Modello e le sue successive integrazioni o modifiche di rilievo sostanziale sono comunicate a tutti i Dipendenti, i Fornitori, i Collaboratori e gli Organi Sociali.

Ai nuovi assunti è consegnato un set informativo, che contiene il Codice Etico e di Condotta di Gruppo ed il Modello di organizzazione, gestione e controllo in modo da assicurare agli stessi le conoscenze considerate di primaria rilevanza per la società.

## **6.3 Altri Destinatari**

L'attività di comunicazione dei contenuti e dei principi del Modello dovrà essere indirizzata anche ai soggetti terzi che intrattengano con la Società rapporti di collaborazione contrattualmente regolati con particolare riferimento a quelli che operano nell'ambito di attività ritenute sensibili ai sensi del d.lgs. 231/2001.