



TINEXTA CYBER S.P.A.

**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO**

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

Versione:	01	Data Versione:	07/2022
Descrizione modifiche:	Prima versione del Modello		
Motivazioni:	Implementazione		
Approvazione:	27 LUGLIO 2022		



	1
PARTE GENERALE		4
1. IL DECRETO LEGISLATIVO 231/2001		5
1.1 Principi generali della responsabilità amministrativa degli Enti.....		5
1.2 I presupposti della responsabilità amministrativa degli Enti		6
1.2.1 I soggetti attivi del reato-presupposto ed il loro “legame” con l’Ente.....		6
1.2.2 Interesse o vantaggio dell’Ente		7
1.2.3 I reati-presupposto della responsabilità amministrativa degli Enti		7
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		8
1.3.2 Responsabilità amministrativa dell’ente e reati-presupposto commessi da soggetti sottoposti all’altrui direzione		10
1.4 L’applicazione pratica del D. Lgs. n. 231/01		11
1.4.1 Gli “adempimenti ad efficacia esimente” della responsabilità amministrativa degli Enti		11
1.4.2. Le Linee Guida di Confindustria.....		11
1.5. Le sanzioni amministrative applicabili agli Enti		13
1.5.1 Le sanzioni pecuniarie		14
1.5.2 Le sanzioni interdittive		15
1.5.3 La pubblicazione della sentenza di condanna		16
1.5.4 La confisca del prezzo o del profitto del reato		16
2. IL MODELLO DI GOVERNANCE E L’ASSETTO ORGANIZZATIVO		17
2.1 La Società		17
2.2 L’assetto societario		17
2.3 Gli strumenti di governance della Società		22
2.4 Il sistema di controllo interno		25
2.5 Rapporti infragruppo		26
3. IL MODELLO DI ORGANIZZAZIONE E DI GESTIONE DELLA SOCIETA’		27
3.1 Obiettivi e funzione del Modello		27
3.2 Destinatari del Modello		28
3.3 Struttura del Modello: Parte Generale e Parte Speciale		29

3.4 Il progetto della Società per la definizione del proprio Modello	31
3.4.1 Individuazione delle aree, delle attività e dei processi sensibili	31
3.4.2 Identificazione dei Key Officer.....	32
3.4.3 Analisi dei processi e delle Attività Sensibili.....	32
3.4.4 Individuazione dei meccanismi correttivi: analisi di comparazione della situazione esistente rispetto al Modello a tendere.....	34
3.4.5 Adeguamento del Modello.....	34
3.4.6 Criteri di aggiornamento del Modello.....	35
3.5 Estensione dei principi del Modello di Tinexta S.p.A. alla Società	36
4. ORGANISMO DI VIGILANZA.....	37
4.2 Reporting dell’Organismo di Vigilanza verso gli organi societari	41
4.3 Informativa verso l’Organismo di Vigilanza	42
4.4 Raccolta e conservazione delle informazioni.....	45
5.1. Principi generali.....	46
5.2 Condotte sanzionabili: categorie fondamentali	46
5.3 Soggetti	47
5.4 Violazioni del modello e relative sanzioni	47
5.5 Misure nei confronti dei dipendenti	48
5.6 Misure nei confronti dei dirigenti.....	48
5.7 Misure nei confronti di amministratori	49
5.8 Misure nei confronti degli altri destinatari	49
6. COMUNICAZIONE E FORMAZIONE DEL PERSONALE.....	50
6.1 Formazione e diffusione del Modello	50
6.2 Componenti degli organi sociali, dipendenti, dirigenti e quadri	51
6.3 Altri Destinatari.....	52

PARTE GENERALE

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).
- Concussione e corruzione (art. 25).
- 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 (art. 25-quater).
- Pratiche di mutilazione degli organi genitali femminili (art. 25-quater 1).
- Delitti contro la personalità individuale (art. 25-quinquies).
- Abusi di mercato (art. 25-sexies).
- Reati commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies).
- 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)¹.

¹ ¹ Si segnala che l'art. 25-octies.1. "Delitti in materia di strumenti di pagamento diversi dai contanti", al comma 2 prevede sanzioni in capo all'ente anche: "... *Salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente, in relazione alla commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti...*". Si fa riferimento, quindi, ai reati previsti dai Titoli VII (Delitti contro la fede pubblica) e XIII (Delitti contro il patrimonio) del codice penale, laddove questi non siano già

- 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 tributari (art.25-quinquiesdecies).
- 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).
- Reati transnazionali (Legge 16 marzo 2006, n. 146, artt. 3 e 10).

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.

ricompresi nel catalogo dei reati presupposto per la responsabilità amministrativa degli enti dagli artt. 24 e seguenti del D.lgs. 231/2001 ed esclusivamente quando abbiano ad oggetto strumenti di pagamenti diversi dai contanti. In particolare:

- Art. 490 c.p. - Soppressione, distruzione e occultamento di atti veri;
- Art. 491 c.p. - Falsità in testamento olografo, cambiale o titoli di credito;
- Art. 624 c.p. - Furto;
- Art. 624 bis c.p. - Furto in abitazione e furto con strappo;
- Art. 628 c.p. - Rapina;
- Art. 629 c.p. - Estorsione;
- Art. 635 c.p. - Danneggiamento;
- Art. 640 c.p. - Truffa;
- Art. 642 c.p. - Fraudolento danneggiamento dei beni assicurati e mutilazione fraudolenta della propria persona;
- Art. 644 c.p. - Usura;
- Art. 645 c.p. - Frode in emigrazione;
- Art. 646 c.p. - Appropriazione indebita.

Inoltre, stante il richiamo della norma ai reati "che comunque offendono il patrimonio" qualora aventi ad oggetto strumenti di pagamento diversi dai contanti, i reati che non sono già ricompresi nel catalogo del D.lgs. 231/2001 e che ora possono assumere rilevanza sono:

- Art. 382 c.p. - Millantato credito del patrocinatore.

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: in tale evenienza, infatti, si tratterebbe di un vantaggio in un certo qual modo "fortuito", come tale non attribuibile alla volontà 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.

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).

Con la legge 30 novembre 2017, n. 179 è stato aggiunto il comma 2-bis all'art. 6 del D.Lgs. 231/2001 con lo scopo di disciplinare le segnalazioni di comportamenti illeciti.

In particolare, è stato previsto, ai fini dell'esimente, che i Modelli debbano prevedere:

- a) "uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere a) e b), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;

- b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
- c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

In base al d.lgs 231/01, la Società prende atto che l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al comma 2-bis possa essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo

Inoltre, la Società rispetta quanto prescritto dal d.lgs 231/01 in merito al licenziamento ritorsivo o discriminatorio del soggetto segnalante, che deve ritenersi nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. È onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

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.

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 per conto della società.

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.

Preme evidenziare, in ogni modo, che 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.

Nella prima ipotesi, la disciplina di cui al Decreto prevede la c.d. "l'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 ("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.

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

1.4.1 Gli "adempimenti ad efficacia esimente" della responsabilità amministrativa degli Enti

Il Decreto prevede, dunque, quale adempimento dell'Ente ad efficacia esimente, l'adozione di un Modello che risponda 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.

L'efficace attuazione del Modello, inoltre, richiede:

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

1.4.2. Le Linee Guida di Confindustria

Come già evidenziato, 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, la principale organizzazione rappresentativa delle imprese manifatturiere e di servizi in Italia, raggruppa, su base volontaria, circa 150.000 imprese di tutte le dimensioni per un totale di oltre 5 milioni di addetti.

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'ausilio 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.

Nel corso degli anni sono stati emanati, e successivamente approvati dal Ministero della Giustizia, tre aggiornamenti delle Linee Guida, il primo dei quali a marzo 2008, il secondo a marzo 2014 e l'ultimo a giugno 2021.

Le nuove Linee Guida di Confindustria per la costruzione dei modelli organizzativi adeguano i precedenti testi alle novità legislative, giurisprudenziali e della 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*;
- 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.

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.

A seguito dell'entrata in vigore della legge n. 179 recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato", Confindustria ha pubblicato una Nota illustrativa sulla disciplina in materia di whistleblowing che illustra i principali contenuti della normativa di riferimento e fornisce chiarimenti applicativi per gli Enti dotati del Modello 231.

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;
 - confisca (e sequestro preventivo in sede cautelare);
 - pubblicazione della sentenza (in caso di applicazione di una sanzione interdittiva).

La ratio della disciplina predisposta in ambito sanzionatorio è evidente: con la previsione delle sanzioni pecuniarie e interdittive 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, l'importo della quota è sempre pari a 103,29 Euro 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.

Sono previste, infine, due ipotesi di riduzione della pena pecuniaria:

- 1) la prima concernente i casi di particolare tenuità del fatto, nel cui ambito

la sanzione pecuniaria da irrogare non può essere superiore a Euro 103.291,00 né inferiore ad Euro 10.329,00;

2) la seconda è dipendente dalla riparazione o reintegrazione dell'offesa realizzata.

Comunque, l'art. 27 del Decreto fissa un limite invalicabile all'ammontare della sanzione, disponendo che l'Ente può essere chiamato a rispondere del pagamento della sanzione pecuniaria solo entro i limiti del fondo comune o del patrimonio.

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 (comporta la sospensione ovvero la revoca delle autorizzazioni, licenze o concessioni funzionali allo svolgimento dell'attività e si applica soltanto quando l'irrogazione di altre sanzioni interdittive risulta inadeguata);
- 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.

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.

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 affittiva 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.

Tinexta Cyber S.p.A. è una società di diritto italiano - controllata interamente da Tinexta S.p.A., entità quotata al MTA di Borsa di Milano, Segmento Star, controllante di un gruppo di aziende ("Gruppo Tinexta") - che offre servizi nei settori del digital trust, cyber security, marketing solutions e credit information & management, a beneficio di imprese, utilities, professionisti, privati, pubbliche amministrazioni.

All'interno del Gruppo TINEXTA è stato costituito un Polo Cyber, composto dalle società Corvallis S.r.l., Swascan S.r.l., Yoroi S.r.l., controllate e oggetto di coordinamento da parte di Tinexta Cyber in veste di sub-holding.

L'oggetto sociale principale e prevalente Tinexta Cyber è costituito dall'attività, non esercitata nei confronti del pubblico, di assunzione e gestione di partecipazioni in società operanti nello sviluppo dei servizi informatici e in generale nello sviluppo di servizi innovativi per le imprese e le amministrazioni pubbliche, nonché di finanziamento sotto qualsiasi forma e di coordinamento tecnico, finanziario e amministrativo delle società partecipate, anche indirettamente.

Rientra, in via subordinata, nell'oggetto sociale di Tinexta Cyber anche la produzione, la realizzazione e al relativa commercializzazione di prodotti e servizi nel settore dell'informatica; lo sviluppo, la produzione e al commercializzazione di sistemi hardware e software per l'elaborazione elettronica dei dati, nel campo dell'automazione per quanto attiene sia l'informatica tradizionale e d'ufficio che la telematica e la robotica; la produzione e la commercializzazione di ogni sorta di servizi per la soluzione di esigenze organizzative, informatiche e telematiche; la progettazione, realizzazione, installazione, trasformazione e manutenzione di sistemi integrati per il controllo e la gestione dei dati e delle procedure informatiche e telematiche, la concessione a terzi dell'utilizzo di software di sua proprietà gestendo le relative royalties.

2.2 L'assetto societario

Tinexta Cyber S.p.A., con sede legale a Roma (RM), Piazza Sallustio n. 9 (e unità locale a Milano, in via Meravigli n. 7), nasce nel 2021 come società facente parte del Gruppo Tinexta: è sottoposta ad attività di direzione e coordinamento da

parte della Capogruppo Tinexta S.p.A.

Il sistema di amministrazione adottato da Tinexta Cyber S.p.A. è il sistema tradizionale, pertanto presenta un'assemblea dei soci, un organo amministrativo che si esplicita in un Consiglio d'Amministrazione e un organo di controllo rappresentato da un Collegio Sindacale.

Assemblea

L'assemblea ordinaria regolarmente costituita rappresenta l'universalità degli azionisti e le sue deliberazioni, ove conformi alla legge e allo statuto, obbligano tutti i Soci anche quando non intervenuti o assenti.

Sono inderogabilmente riservate alla competenza dell'assemblea ordinaria:

- a) l'approvazione del bilancio;
- b) la definizione del numero di membri dell'organo amministrativo e relativo compenso;
- c) la nomina e la revoca degli amministratori; la nomina dei sindaci e, quando previsto, del soggetto incaricato di effettuare la revisione legale dei conti;
- d) la determinazione del compenso degli amministratori e dei sindaci, se non è stabilito dallo statuto;
- e) l'attribuzione di responsabilità degli amministratori e dei sindaci;
- f) la deliberazione in merito agli altri oggetti attribuiti dalla legge alla competenza dell'assemblea, nonché sulle autorizzazioni eventualmente richieste dallo statuto per il compimento di atti degli amministratori, ferma in ogni caso la responsabilità di questi per gli atti compiuti.

Sono di competenza dell'assemblea straordinaria:

- a) le modifiche dello statuto, oggetto sociale o capitale sociale;
- b) la nomina, la sostituzione e la determinazione dei poteri dei liquidatori;
- c) le altre materie ad essa attribuite dalla legge e dallo Statuto.

Organo Amministrativo

La Società è amministrata da un Consiglio di Amministrazione composto da 3 membri scelti anche fra i non soci, nominati per la prima volta nell'atto costitutivo e successivamente dall'Assemblea dei Soci, che ne stabilisce il compenso e il numero.

Il CdA è investito dei più ampi poteri per la gestione ordinaria e straordinaria della Società ed ha la facoltà di compiere tutti gli atti che ritenga opportuni per il raggiungimento e l'attuazione degli scopi sociali, esclusi quelli che la legge riserva indelegabilmente alle decisioni dei soci. Inoltre, il Consiglio di Amministrazione è competente per:

- l'assunzione delle deliberazioni di cui agli art. 2505 e 2505bis del Codice Civile,
- la riduzione del capitale sociale in caso di recesso di un socio
- gli adeguamenti dello statuto alle disposizioni normative.

Il CdA può delegare tutti o parte dei propri poteri a uno o più dei suoi componenti, anche disgiuntamente. Tuttavia, non possono essere delegate le attribuzioni indicate nell'art. 2381 quarto comma del Codice Civile e le decisioni inerenti alle materie espressamente elencate all'interno dei documenti societari. Tra i poteri rientrano anche la possibilità di impartire direttive agli organi delegati e nominare direttori generali e procuratori speciali, scegliendoli anche fra persone estranee alla Società determinandone poteri e compenso.

La firma sociale e la rappresentanza sociale generale di fronte ai terzi ed in giudizio spettano al Presidente del CdA e all'Amministratore Delegato. Il Presidente e l'Amministratore Delegato possono, nell'ambito delle rispettive deleghe, conferire procura ad altre persone per singoli affari.

Collegio Sindacale

Il Collegio Sindacale si compone di 3 (tre) membri effettivi e 2 (due) membri supplenti, nominati dall'Assemblea, che provvede alla nomina del Presidente tra i sindaci effettivi. I membri del Collegio Sindacale devono essere iscritti nel registro dei revisori legali. La nomina dei membri del Collegio Sindacale avviene sulla base di liste presentate dai Soci. Il Collegio Sindacale ha i doveri e i poteri ad esso attribuiti di cui agli artt. 2403, primo comma, e 2403 – bis del Codice Civile.

DPO e Privacy Officer

In conformità con quanto previsto dall'articolo 37(2) del GDPR, il Gruppo TINEXTA ha nominato un unico DPO al quale rivolgersi attraverso un indirizzo e-mail dedicato, il quale sarà supportato nella sua attività dal soggetto preposto al Privacy Officer della Società.

In adempimento a quanto previsto dal Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679 il DPO di Gruppo ha 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 le 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 Informativa,

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) sorvegliare sul rispetto della Normativa Privacy al fine di evitare eventuali violazioni e conseguenti rischi e responsabilità per la Società, anche favorendo la sensibilizzazione e la formazione del personale, in conformità con gli obblighi in materia di trattamento dei dati personali;

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) qualora venga a conoscenza o sospetti che il comportamento del Personale della Società autorizzato ai trattamenti non si conformi con gli obblighi a loro carico, raccogliere ulteriori informazioni e collaborare con il DPO al fine di procedere alla contestazione della violazione nei confronti degli stessi;

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.

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.

Comitato Guida

È composto dall'Amministratore delegato di Tinexta Cyber nonché dai Chief Executive Officers delle società del Polo Cyber. Al Comitato Guida è demandata la valutazione in ordine ad attività e iniziative del Polo Cyber finanziate dalla controllatata nell'ambito del progetto di gestione delle sinergie determinate dall'appartenenza al Gruppo, valorizzando le caratteristiche delle diverse società.

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 dell'Amministratore Delegato le seguenti funzioni:

- Segreteria di Direzione;
- Operation;
- Amministrazione e Finanza;
- Pianificazione e Controllo di Gestione;
- Marketing e Innovazione Strategica;
- Process e Modelling.

2.3 Gli strumenti di governance della Società

La Società è dotata di un insieme di strumenti di governo dell'organizzazione che garantiscono il funzionamento della Società. Tali strumenti garantiscono sia la trasparenza delle scelte gestionali della Società, sia l'efficienza e l'efficacia del sistema di controllo interno.

In particolare, tali strumenti possono essere così riassunti:

Statuto: costituisce l'atto normativo fondamentale che disciplina l'organizzazione e il funzionamento della Società.

Codice Etico di Gruppo: 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 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;
- 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;
- 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 e conflitto di interessi che prevede l'obbligo di evitare situazioni di conflitto d'interesse.

L'adozione del Codice Etico di Gruppo costituisce altresì uno dei presupposti per l'efficace funzionamento del Modello. Il Codice Etico 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.

Organigramma aziendale: riporta l'attuale struttura organizzativa ed è stato concepito e sviluppato al fine di considerare le specificità operative e dimensionali della Società.

Sistema di deleghe e procure: La Società ha adottato, anche alla luce della sua collocazione nell'ambito del Gruppo TINEXTA, di un sistema di deleghe e procure

ai fini della prevenzione dei reati (rintracciabilità ed evidenziabilità delle attività sensibili) che, nel contempo, consenta 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.

Modello di governance in ambito Privacy: Tinexta Cyber, 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 del Gruppo TINEXTA e relativi Allegati.

Il sistema di controllo sull'informativa finanziaria: Tinexta Cyber sta intraprendendo un percorso di adeguamento alle prescrizioni della Legge

262/05 finalizzate a documentare il modello di controllo contabile-amministrativo adottato, nonché ad eseguire specifiche verifiche sui controlli rilevati e a supportare il processo di attestazione del Dirigente Preposto della Capogruppo alla redazione dei documenti contabili societari.

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

Il Modello di Dialogo di Gruppo non descrive, né disciplina, tuttavia, i processi gestiti internamente alle singole società e le interazioni tra le funzioni della stessa società.

L'insieme degli strumenti di governance e regolamentari adottati, qui sopra richiamati in estrema sintesi, e delle previsioni del presente Modello consente, di individuare, rispetto a tutte le attività, come si siano formate e attuate le decisioni dell'ente (cfr. art. 6, comma 2 lett. b, d.lgs. n. 231/2001). La particolare valenza dei presidi sopra menzionati ai fini della prevenzione dei reati richiamati dal D.lgs. 231/2001 verrà specificamente evidenziata, con riferimento a ciascuna tipologia di reato a tal fine rilevante, nella Parte Speciale del presente documento. Il presente Modello si inserisce quindi nell'ambito del sistema aziendale di gestione dei rischi e garantisce una costante attenzione al raggiungimento dell'obiettivo di integrazione dei presidi di controllo al fine di ottimizzare l'efficacia della prevenzione dei rischi.

2.4 Il sistema di controllo interno

La Società è dotata di un sistema di controllo interno finalizzato a presidiare nel tempo i rischi tipici dell'attività sociale.

Il Sistema di Controllo Interno è un insieme di regole, procedure e strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi.

Il sistema di controllo interno e di gestione dei rischi risponde all'esigenza di

garantire:

- (i) l'efficacia e l'efficienza dei processi e delle operazioni;
- (ii) la qualità e l'affidabilità dell'informazione economica e finanziaria;
- (iii) il rispetto di leggi e regolamenti, nonché dello statuto, delle norme e delle procedure interne;
- (iv) la salvaguardia del valore delle attività e del patrimonio sociale;
- (v) l'individuazione, la prevenzione e la gestione dei rischi di natura finanziaria ed operativa e frodi a danno della Società e del Gruppo TINEXTA.

La Società adotta strumenti normativi improntati ai principi generali di:

- a) chiara descrizione delle linee di riporto;
- b) conoscibilità, trasparenza e pubblicità dei poteri attribuiti (all'interno della Società e nei confronti dei terzi interessati);
- c) chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione, dei relativi poteri e responsabilità.

Le procedure interne da adottare devono essere caratterizzate dai seguenti elementi:

- separatezza, all'interno di ciascun processo, tra il soggetto che assume la decisione (impulso decisionale), il soggetto che esegue tale decisione e il soggetto cui è affidato il controllo del processo (c.d. "segregazione delle funzioni");
- traccia scritta di ciascun passaggio rilevante del processo (c.d. "tracciabilità");
- adeguato livello di formalizzazione.

La struttura gerarchica e funzionale indicata nell'organigramma societario, unitamente alle procedure di Dialogo e Controllo di Gruppo per singola funzione o area di rischio, nonché alle procedure interne di adattamento e implementazione delle linee guida di Gruppo - finalizzate a garantire la segregazione dell'attività, l'esistenza di procedure scritte, l'esistenza di poteri autorizzativi, la tracciabilità - fondano il predetto sistema di controllo interno.

Le procedure in essere adottate e applicabili a Tinexta Cyber S.p.A. tenuto conto anche del presente Modello 231, sono allegate alla Parte Speciale (All.to 1).

2.5 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 le seguenti clausole:

- l'obbligo da parte della società beneficiaria del servizio di attestare la veridicità e completezza della documentazione o delle informazioni comunicate alla società che presta il servizio, ai fini dello svolgimento dei servizi richiesti;
- il potere dell'Organismo di Vigilanza della società che presta il servizio di richiedere informazioni all'Organismo di Vigilanza, o altra funzione di controllo, della società beneficiaria del servizio, al fine del corretto svolgimento delle proprie funzioni nell'ambito dei servizi richiesti alla Società;
- il potere dell'Organismo di Vigilanza, o altra funzione di controllo, della società beneficiaria del servizio di richiedere informazioni all'Organismo di Vigilanza della società che presta il servizio, ovvero – previo consenso di quest'ultimo – alle Direzioni/Funzioni della Società;
- 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 contenente presidi di controllo coerenti con quelli previsti nel Modello di organizzazione, gestione e controllo adottato dalla Società;
- clausola con cui le parti dichiarano di aver impartito e attuato disposizioni ai propri amministratori, dipendenti e/o collaboratori finalizzate a prevenire la commissione, anche tentata, dei comportamenti sanzionati dal d.lgs. 231/01 e si obbligano a mantenerle tutte efficacemente attuate per l'intera durata del contratto;
- clausole risolutive espresse che attribuiscono alle parti la facoltà di risolvere il contratto in questione nel caso di coinvolgimento, a qualsiasi titolo, di una delle Parti in un procedimento rilevante ai sensi e per gli effetti del d.lgs. 231/2001 e successive modifiche e integrazioni e/o in caso di emissione nei confronti di una delle Parti di provvedimenti interdettivi o di sospensione dell'attività lavorativa di qualsiasi natura e/o durata.

Nell'erogare i servizi la Società si attiene a quanto previsto dal presente Modello e dalle procedure stabilite per la sua attuazione.

Qualora i servizi erogati rientrino nell'ambito di Attività Sensibili non contemplate dal proprio Modello, la società che presta il servizio, su proposta dell'OdV, deve dotarsi di regole e procedure adeguate e idonee a prevenire la commissione dei Reati.

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

3.1 Obiettivi e funzione del Modello

La Società è particolarmente sensibile all'implementazione e continuo aggiornamento di un sistema di prevenzione e gestione dei rischi, in linea con quanto previsto nelle disposizioni del Decreto ed idoneo a prevenire e ridurre nella maggior misura possibile, in ambito aziendale, il rischio di commissione di reati, e conseguentemente ad evitare l'applicazione delle sanzioni previste dal medesimo Decreto. 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;
- allinearsi al sistema di controllo e prevenzione dei rischi di reato adottato dalla Capogruppo, che dispone di un Modello 231 nonché di procedure interne ivi richiamate applicabili anche alla controllata.

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 i 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 di Gruppo e al Modello.

In particolare con riferimento ad eventuali partner, 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 di Gruppo.

Pertanto, il Modello si applica, ove possibile, ai consulenti esterni, partner commerciali e finanziari, fornitori e – in generale – a tutti i terzi con i quali la Società intrattiene rapporti inerenti alle attività sociali. Il Modello è condiviso con i Dirigenti/ Responsabili interessati dalle “aree a rischio” individuate che si impegnano ad informare i propri collaboratori degli scopi ed obiettivi perseguiti dal medesimo.

La Società si impegna a facilitare e promuovere la conoscenza del Modello da parte dei suoi destinatari ed il loro contributo costruttivo sui suoi contenuti, ed a predisporre ogni strumento idoneo ad assicurare la piena ed effettiva applicazione dello stesso.

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.

Coerentemente con la struttura prevista dalle Linee Guida per la redazione del Modello di Organizzazione, Gestione e Controllo, la Parte Generale, dopo una introduzione sulla finalità e i principali contenuti del Decreto Legislativo 231/2001, ha fornito indicazioni sull'assetto organizzativo, gli strumenti di governance e il sistema di controllo interno della Società. Nel presente capitolo, a seguito della definizione della funzione e dei destinatari del Modello, sono indicate le modalità adottate dalla Società per l'adeguamento e l'aggiornamento dello stesso. Nel proseguo del documento saranno trattati:

- i ruoli, le responsabilità e i flussi informativi dell'Organismo di Vigilanza;
- le modalità di segnalazione di comportamenti illeciti;
- il sistema disciplinare e sanzionatorio;
- i criteri per la selezione e la formazione del personale, nonché le modalità di diffusione del Modello.

Nella “Parte Speciale” vengono affrontate le aree di attività della Società 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;
- 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-querterdecies), dei reati contro la personalità individuale (di cui all'art. 25-quinquies) ad eccezione del reato di intermediazione illecita e sfruttamento del lavoro, dei reati contro il patrimonio culturale e di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici. Infine, in alcun modo riferibile all'attività di Tinexta Cyber S.p.A. è il delitto di mutilazione organi genitali femminili (art. 25-querter.1).

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 nella mappatura contenuta nel presente Modello. Di conseguenza i presidi previsti in relazione all'ipotetica realizzazione mono-soggettiva 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 all'Organo Amministrativo 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:

- Acquisti di beni e servizi
- Consulenze e incarichi professionali a terzi
- Gestione di sponsorizzazioni, donazioni e omaggi
- Gestione del contenzioso
- Gestione delle risorse umane
- Gestione finanziaria e Tesoreria
- Gestione della contabilità e delle attività di predisposizione del Bilancio

- Affari Societari
- Gestione delle attività di Merger & Acquisition
- Gestione dei rapporti con la Pubblica Amministrazione e le Autorità di Vigilanza
- Gestione delle operazioni con Parti Correlate e dei Rapporti Infragruppo
- Gestione dei rapporti con la Società di Revisione
- Gestione dei sistemi informativi
- Gestione degli adempimenti fiscali
- Comunicazioni verso l'esterno
- Sistema di gestione ambientale
- Gestione adempimenti in materia di salute e sicurezza sui luoghi di lavoro

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.

L’approccio operativo e metodologico adottato dalla Società nell’attività di risk assessment è coerente con quanto definito all’interno delle “Linee Guida per la redazione del Modello di Organizzazione, Gestione e Controllo”.

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”).

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.

Nell'eventualità che esigenze operative impongano una maggiore articolazione dei controlli, si provvederà a individuare altri soggetti cui affidare la mansione di key officer senza che ciò comporti obbligo di modifica del presente Modello Organizzativo.

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.

Nel caso di specie, 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 a livello di Gruppo e un modello astratto di riferimento valutato sulla base delle esigenze manifestate dalla disciplina di cui al d.lgs. 231/2001.

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

Terminate le fasi precedenti, è stato redatto 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;
- 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.

La predisposizione 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 propone all'Organo Amministrativo l'opportunità di 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, l'Organo Amministrativo ha ritenuto di delegare alla Funzione Pianificazione e Controllo di Gestione della Società 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 dall'Organo Amministrativo (come, ad esempio la ridefinizione dell'organigramma) o da funzioni munite di specifica delega (es. nuove procedure).

La Funzione Pianificazione e Controllo di Gestione (nella figura del suo Responsabile) comunica tempestivamente all'OdV le eventuali modifiche apportate al Modello relative ad aspetti di carattere descrittivo e ne informa l'Organo Amministrativo, in occasione della prima riunione utile, al fine di farne oggetto di ratifica da parte dello stesso.

Rimane, in ogni caso, di esclusiva competenza dell'Organo Amministrativo 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 cura, sviluppo e promozione del costante aggiornamento del Modello. A tal fine, formula osservazioni e proposte, attinenti all'organizzazione e al sistema di controllo, alle strutture a ciò preposte o, in casi di particolare rilevanza, all'Organo Amministrativo.

3.5 Estensione dei principi del Modello di Tinexta S.p.A. alla Società

Si ribadisce che 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.

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 possono essere così identificati:

- l'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, ed, in particolare, del management aziendale;
- la professionalità: l'organismo deve avere un bagaglio di conoscenze, strumenti e tecniche necessari per svolgere efficacemente la propria attività;
- la 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 è un organismo monocratico

L'Organismo di Vigilanza è istituito con delibera del Consiglio di Amministrativo e resta in carica per la durata del mandato del Consiglio di Amministrazione che lo ha nominato.

Alla scadenza del termine, l'Organismo di Vigilanza rimane in carica fino a quando interviene una nuova nomina deliberata dal Consiglio di Amministrazione. Se nel corso della carica, l'Organismo di Vigilanza cessa per qualsiasi motivo dal suo incarico, il Consiglio di Amministrazione provvede senza indugio alla 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 Amministrativo 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 membro 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 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 del componente dell'OdV può essere esercitata in qualsiasi momento e deve essere comunicata al Consiglio di Amministrativo per iscritto, unitamente alle motivazioni che l'hanno determinata.

Il componente dell'Organismo di Vigilanza può essere revocato esclusivamente per giusta causa, sentito il parere non vincolante del Sindaco, mediante un'apposita delibera dell'Organo Amministrativo. A tale proposito, per giusta causa di revoca dovrà intendersi, a titolo esemplificativo:

- l'interdizione o l'inabilitazione, ovvero una grave infermità che renda l'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 all'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 ed incompatibilità;
- un grave inadempimento dei doveri propri dell'Organismo di Vigilanza.

In tali ipotesi, il Consiglio di Amministrativo provvede tempestivamente a nominare il nuovo Organismo di Vigilanza in sostituzione di quello revocato 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.

L'Organismo di Vigilanza di Tinexta Cyber S.p.A. è chiamato a svolgere i seguenti compiti:

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. promuovere l'attivazione di eventuali procedimenti disciplinari;
11. 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".
12. 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;
13. 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 Struttura preposta per i programmi di formazione del personale;
- aggiornare la lista delle informazioni che devono essergli trasmesse o tenute a sua disposizione;
- riferire periodicamente all'Organo Amministrativo e al Sindaco Unico in merito all'attuazione del Modello.

Per svolgere i propri compiti, l'Organismo di Vigilanza ha libero accesso presso

tutte le funzioni della Società e alla documentazione aziendale, senza necessità di alcun consenso preventivo.

L'Organo Amministrativo 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, l'Organo Amministrativo 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, 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 il vertice aziendale (Amministratore Delegato e Presidente) rendendolo edotto, ogni qual volta lo ritenga opportuno, su circostanze e fatti significativi del proprio ufficio. L'Organismo di Vigilanza 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;
- la seconda, su base periodica semestrale, nei confronti dell'organo amministrativo e dell'organo di controllo.

L'Organismo di Vigilanza presenta una relazione scritta all'Organo Amministrativo, 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 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;
- c) il resoconto delle segnalazioni ricevute, ivi incluso quanto direttamente riscontrato, in ordine a presunte violazioni delle previsioni del presente Modello, dei protocolli di prevenzione e delle relative procedure di attuazione e l'esito delle conseguenti verifiche effettuate;
 - d) informativa in merito all'eventuale commissione di reati rilevanti ai fini del Decreto;
 - e) 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;
 - f) una valutazione complessiva sul funzionamento e l'efficacia del Modello con eventuali proposte di integrazioni, correzioni o modifiche;
 - g) la segnalazione degli eventuali mutamenti del quadro normativo e/o significative modificazioni dell'assetto interno della Società che richiedono un aggiornamento del Modello;
 - h) 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 avere ad oggetto

i) in forma strutturata i seguenti report, che devono essere prodotti con periodicità semestrale:

- 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 semestre di riferimento con evidenza del valore dell'ordine, del nome del fornitore e del conto contabile di destinazione del costo;
- elenco degli incarichi di consulenza sottoscritti con evidenza di quelli conferiti tramite affidamento diretto;
- elenco delle liberalità, contributi 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;

ii) in forma strutturata al verificarsi dei seguenti eventi:

- report del DPO/Privacy Officer su eventuali violazioni della sicurezza informatica (“data breach”);
- report del DPO/Privacy Officer 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, INAIL, ASL, enti locali, Guardia di Finanza, etc.);
- elenco degli 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 o dai responsabili di Internal Audit, Compliance, Controllo di Gestione o di altre funzioni aziendali di Gruppo nell’ambito della loro attività di controllo avente ad oggetto anche Tinexta Cyber 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;
- rapporti predisposti dall’Area Amministrazione e finanza e dai soggetti preposti al controllo interno dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all’osservanza delle norme del Decreto, delle previsioni del Modello 231 e delle procedure;
- 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 di procedure che potrebbero agevolare la commissione dei reati in relazione o a comportamenti non in linea con le regole di condotta adottate dalla società.

La Società, in conformità a quanto previsto dalla normativa in materia di whistleblowing istituisce i seguenti canali di segnalazione al fine di garantire la riservatezza dell'identità del segnalante.

1) con riferimento alle segnalazioni effettuate anche da parte di "terzi", la Società ha predisposto:

- la casella e-mail: odv@tinextacyber.com, a cura dell'Organismo di Vigilanza e pubblicata sul sito internet della Società;
- la posta prioritaria con l'indicazione di "RISERVATO" sulla busta indirizzata a: Organismo di Vigilanza, c/o Piazza Sallustio n. 9, 00187, Roma (RM);

2) con riferimento, invece, al canale dedicato al whistleblowing, la Società adotta la piattaforma «Comunica Whistleblowing» accessibile dal sito:

https://digitalplatform.unionefiduciaria.it/whistleblowing/default_new4.asp

Attraverso tale sistema di segnalazioni la Società garantisce, con modalità informatiche, la riservatezza dell'identità del segnalante.

L'OdV valuta le segnalazioni ricevute e determina le eventuali iniziative, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e/o ogni altro soggetto che riterrà utile, motivando per iscritto ogni conclusione raggiunta. In particolare, le segnalazioni ricevute attraverso i canali sopra citati vengono gestite dall'OdV che effettua una prima valutazione della segnalazione al fine di:

- accertare che rientri nell'ambito di competenza dell'OdV;
- verificare che sia sufficientemente circostanziata per poter procedere ad un approfondimento della stessa.

Nel caso in cui la segnalazione presenti le caratteristiche sopra riportate, l'OdV avvia le attività di istruttoria, in caso contrario, provvede all'archiviazione della segnalazione, con una breve nota esplicativa. In particolare:

- Attività istruttoria: l'OdV valuta discrezionalmente e sotto la propria responsabilità la segnalazione al fine di valutare la necessità di effettuare specifici approfondimenti per accertare i fatti ivi denunciati. Tale necessità

viene determinata sulla base dei seguenti elementi: (i) informazioni fornite a corredo della segnalazione; (ii) attuali procedure in vigore attinenti i fatti segnalati; (iii) segnalazioni/verifiche precedenti aventi lo stesso oggetto e già esaminate.

- Attività di accertamento: l'OdV avvia delle verifiche ad hoc (attività di indagine), eventualmente con modalità riservate, in funzione dell'oggetto della segnalazione. L'eventuale attività di indagine viene condotta mediante il supporto delle funzioni competenti o di soggetti esterni e nel rispetto di tutte le norme applicabili a tutela tanto del soggetto segnalante quanto di eventuali soggetti coinvolti nelle verifiche. Qualora l'OdV ritenga di non dover procedere all'effettuazione di ulteriori verifiche, redige una breve nota esplicativa delle analisi svolte e archivia la segnalazione.
- Misure correttive: qualora l'indagine rilevi la necessità di un intervento correttivo, l'OdV ne chiede l'attuazione alle funzioni competenti.

L'OdV istituisce un registro delle segnalazioni, contenente l'indicazione delle segnalazioni pervenute, dei relativi responsabili, nonché delle eventuali sanzioni irrogate nei loro confronti.

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 l'Organismo di Vigilanza di Tinexta Cyber S.p.A. 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 Tinexta S.p.A. in condivisione con l'Organismo di Vigilanza della società controllata. La convocazione avviene a cura del presidente dell'Organismo di Vigilanza di Tinexta S.p.A. ed è trasmessa all'interessato 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).

5. SISTEMA DISCIPLINARE E SANZIONATORIO

5.1. Principi generali

L'efficace attuazione del Modello è assicurata anche dalla previsione e predisposizione 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 sanzioni disciplinari potranno quindi essere applicate dalla Società ad ogni violazione del presente Modello e del Codice Etico 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 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 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'omesso controllo sulla diffusione del Codice Etico di Gruppo da parte dei soggetti responsabili;
 - 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 di cui al precedente paragrafo 4.2. 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 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 di Gruppo, la cui violazione costituisce illecito disciplinare, nonché le sanzioni applicabili, proporzionate alla gravità delle infrazioni.

Si ritiene opportuno rinviare al Codice Etico 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.

Il responsabile dell'avvio e dello svolgimento del procedimento disciplinare è la Funzione preposta alla gestione delle 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.

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 adottato dal Gruppo, rappresentano parte integrante.

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.

La previsione e l'applicazione delle sanzioni deve essere graduata in ragione della violazione connessa. La gradualità della sanzione può estendersi nell'ambito della tipologia di sanzioni previste dal CCNL applicato, ovvero:

- 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

In caso di violazione del Modello o del Codice Etico 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

In caso di violazione del Modello o del Codice Etico di Gruppo da parte di un membro dell'Organo Amministrativo, l'Organismo di Vigilanza procede a darne immediata comunicazione all'intero Organo Amministrativo e al Sindaco Unico, esprimendo parere in merito alla gravità dell'infrazione. L'Organo Amministrativo, sentito il parere del Sindaco, 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 dell'Organo Amministrativo della cui infrazione si discute saranno tenuti ad astenersi dalle relative deliberazioni.

Qualora le violazioni siano commesse da un numero di membri dell'Organo Amministrativo 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 di Gruppo da parte di un membro del Collegio Sindacale, l'Organismo di Vigilanza procede a darne immediata comunicazione all'intero Collegio Sindacale e all'Organo Amministrativo, esprimendo parere in merito alla gravità dell'infrazione.

Il Collegio, sentito il parere dell'Organo Amministrativo, 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 partner commerciali delle disposizioni del Codice Etico 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 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 Talent Acquisition & Education di Tinexta e anche attraverso idonei strumenti di diffusione quali:

a. Comunicazione e formazione verso i dipendenti:

- Comunicazione tramite e-mail, al momento dell'adozione del Modello stesso, in particolare si esplica mediante l'invio a tutti i dipendenti in organico di un'informativa, da parte della Funzione preposta, per comunicare che Tinexta Cyber ha provveduto all'aggiornamento di quanto riportato all'interno del Modello di Organizzazione Gestione e Controllo, allegando una copia dello stesso,

- Consegna ai nuovi dipendenti del Modello di Organizzazione, Gestione e Controllo, inserendo nel corpo della lettera di assunzione una nota informativa dedicata al D. Lgs 231/2001 ed alle caratteristiche del Modello adottato.
 - predisposizione di questionari di verifica dell'efficacia formativa raggiunta.
- b. Comunicazione e formazione verso fornitori e consulenti:
- Inserimento di una specifica clausola contrattuale, in qualunque contratto di fornitura, servizio e consulenza di: conoscenza delle disposizioni del D. Lgs 231/2001 e delle prescrizioni del Codice Etico, impegno nel rispetto delle stesse e condizione risolutiva in caso di inosservanza.

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 Codice Etico 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).

In alcuni casi, potranno inoltre essere tenuti corsi di formazione e informazione rivolti ai responsabili di direzione/funzione, ciascuno dei quali sarà responsabile della successiva diffusione del presente Modello nell'ambito della struttura organizzativa di riferimento, nonché dell'attuazione, per gli aspetti di sua competenza, delle regole alla base degli stessi.

Sulla base di quanto statuito nel presente Modello, l'Organismo di Vigilanza monitora l'esecuzione del piano di formazione ed informazione.

La partecipazione alle attività di formazione costituisce un obbligo e viene formalizzata mediante sottoscrizione del modulo di registrazione delle presenze (o registrazione dell'accesso ai moduli formativi di tipo e-learning). I nominativi del personale formato sono inseriti in un *repository* a cura della Funzione Risorse Umane.

6.2 Componenti degli organi sociali, dipendenti, dirigenti e quadri

L'Organismo di Vigilanza promuove, mediante la predisposizione di appositi piani comunicati all'Organo Amministrativo 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 del 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 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.