INFOCERT

TINEXTA GROUP

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

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

	VERSIONE E DATA	APPROVATO	NOTE
ADOZIONE E REVISIONE	n. 03 - febbraio 2024	Consiglio di Amministrazione	Revisione completa in base alle Linee Guida Gruppo Tinexta e revisione del Risk Assessment
	n. 02 - dicembre 2020	Consiglio di Amministrazione	Aggiornamento in base alle Linee Guida Gruppo Tinexta
	n. 01 - aprile 2020	Consiglio di Amministrazione	Revisione completa del modello in base alle Linee Guida Gruppo Tinexta

Indice

Parte generale

Definizioni

- "**Codice Etico e di Condotta di Gruppo**": Documento adottato dal Gruppo Tinexta S.p.A. volto ad indicare i valori cui le Società si ispirano nello svolgimento delle proprie attività;
- "**Decreto**": Decreto Legislativo 8 giugno 2001, n. 231 e successive integrazioni e modifiche;
- "**Organismo di Vigilanza**" o "**OdV**": organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo al quale, ai sensi del Decreto Legislativo n. 231/2001, è affidato compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento;
- "**Consulenti**": coloro che agiscono in nome e/o per conto di Infocert S.p.A. sulla base di apposito mandato o di altro vincolo di consulenza o collaborazione;
- "**Dirigenti**": i dirigenti di Infocert S.p.A.;
- "**Dipendenti**": tutti i lavoratori subordinati di Infocert S.p.A. (impiegati, quadri, operai, ecc.);
- "**Modello**": il modello di organizzazione, di gestione e controllo previsto dal D. Lgs. n. 231/2001, adottato ed efficacemente attuato sulla base dei principi di riferimento di cui al presente documento (di seguito denominato "Modello");
- "**P.A.**" o "**Pubblica Amministrazione**": la Pubblica Amministrazione, inclusi i relativi funzionari nella loro veste di pubblici Ufficiali o incaricati di pubblico servizio (con la stessa definizione ci si riferisce a qualsiasi soggetto che rivesta le funzioni di pubblico ufficiale o incaricato di pubblico servizio anche se non alle dipendenze di una Pubblica Amministrazione);
- "**Partner**": soggetti che intrattengono rapporti contrattuali con Infocert S.p.A., quali ad es. fornitori, sia persone fisiche sia persone giuridiche, ovvero soggetti con cui la società addivenga ad una qualunque forma di collaborazione contrattualmente regolata (consulenti, agenti, procacciatori, consorzi, ecc.), ove destinati a cooperare con l'azienda nell'ambito dei processi sensibili;
- "**Reati**": i reati per i quali è applicabile la disciplina prevista dal D. Lgs. n. 231/2001;
- "**Processi Sensibili**": attività di Infocert S.p.A. nel cui ambito ricorre il rischio di commissione dei reati per i quali è applicabile la disciplina prevista dal D. Lgs. n. 231/2001;
- "**Area di rischio**": area/settore aziendale a rischio di commissione dei reati per i quali è applicabile la disciplina prevista dal D. Lgs. n. 231/2001;
- "**Sistemi di controllo**": sistema di controllo predisposto dalla società al fine di prevenire, attraverso l'adozione di appositi protocolli, i rischi di commissione dei reati per i quali è applicabile la disciplina prevista dal D. Lgs. n. 231/2001;
- "**Linee Guida Confindustria**": le Linee Guida emanate da Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. n. 231/2001, approvate dal Ministero della Giustizia in data 24 maggio 2004 e, da ultimo aggiornate, nel 2021.

1. IL DECRETO LEGISLATIVO 231/2001

1.1 Principi generali della responsabilità amministrativa degli Enti

Il Decreto Legislativo 8 giugno 2001, n. 231, emanato in esecuzione della delega contenuta nell'art. 11 della Legge 29 settembre 2000, n. 300, ha introdotto nell'ordinamento giuridico italiano la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato.
In particolare, il Decreto ha previsto che gli enti forniti di personalità giuridica, le società e le associazioni, anche prive di personalità giuridica, sono responsabili nel caso in cui i propri apicali, i propri dirigenti o coloro che operano sotto la direzione o la vigilanza di questi, commettano alcune fattispecie di reato, tassativamente individuate nel Decreto, nell'interesse o a vantaggio dell'ente stesso.
Il fine della norma è quello di sensibilizzare gli enti sulla necessità di dotarsi di una organizzazione interna idonea a prevenire la commissione di reati da parte dei propri apicali o delle persone che sono sottoposto al loro controllo.
Si noti che la responsabilità amministrativa dell'Ente non è sostitutiva di quella penale della persona fisica che ha realizzato materialmente il c.d. reato presupposto, ma si aggiunge ad essa.
Le fattispecie di reato cui si applica la disciplina in esame possono essere comprese, per comodità espositiva, nelle seguenti categorie:

- Reati commessi nei rapporti con la P.A e di corruzione. (artt. 24 e 25).
- Delitti informatici e trattamento illecito di dati (art. 24-bis).
- Delitti di criminalità organizzata (art. 24-ter).
- Reati di falsità in monete, carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis).
- Delitti contro l'industria e il commercio (art. 25-bis.1).
- Reati societari (art. 25-ter).
- Reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater).
- Pratiche di mutilazione degli organi genitali femminili (art. 25-quater.1).
- Delitti contro la personalità individuale (art. 25-quinquies).
- Reati di abuso di mercato (art. 25-sexies; art. 187-quinquies TUF).
- Reati di omicidio colposo commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies).
- Reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25-octies).
- Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-octies.1).
- Delitti in materia di violazione del diritto d'autore (art. 25-novies).

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

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

1.2 I presupposti della responsabilità amministrativa degli Enti

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

L'art. 5, comma 1, del Decreto, indica le persone fisiche il cui comportamento delittuoso fa derivare la responsabilità amministrativa degli Enti, in virtù della teoria della c.d. immedesimazione organica.
Ai sensi di tale articolo, difatti, l'Ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone 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, alternativamente, nell'interesse o a vantaggio dell'Ente.

L'interesse dell'Ente presuppone sempre una verifica ex ante del comportamento delittuoso tenuto dalla persona fisica, mentre il "vantaggio" richiede sempre una verifica ex post e può essere tratto dall'Ente anche quando la persona fisica non abbia agito nel suo interesse. I termini "interesse" e "vantaggio" hanno riguardo a concetti giuridicamente diversi e hanno ciascuno una specifica ed autonoma rilevanza, in quanto può ben accadere, ad esempio, che una condotta che inizialmente poteva sembrare di interesse per l'ente, poi, di fatto, a posteriori non porti il vantaggio sperato.
L'Ente non risponde, di converso, se le persone indicate sub 1.2.1 hanno agito nell'interesse esclusivo proprio o dei terzi, poiché, in tale evenienza, viene meno il requisito della commissione del reato nell'interesse o a vantaggio dell'Ente.
Nell'ipotesi in cui la persona fisica abbia commesso il c.d. reato presupposto nel "prevalente" interesse proprio o di terzi e l'Ente non abbia ricavato vantaggio alcuno o ne abbia ricavato un vantaggio minimo, vi sarà comunque responsabilità e l'applicazione ai sensi e per gli effetti dell'art. 12, comma 1, lett. a) del Decreto della sanzione pecuniaria ridotta della metà e comunque non superiore a € 103.291,38.

1.2.3 I reati-presupposto della responsabilità amministrativa degli Enti

La responsabilità amministrativa dell'Ente può configurarsi solo in relazione a quei reati 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, in relazione a quel reato e le relative sanzioni non sono espressamente previste da una legge che sia entrata in vigore prima della commissione del fatto (c.d. principio di legalità).

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

Gli articoli 6 e 7 del Decreto disciplinano le condizioni per l'esonero della responsabilità amministrativa dell'Ente.
Il Modello è un complesso di regole e strumenti finalizzato a dotare l'Ente di un efficace sistema organizzativo e di gestione, che sia anche idoneo ad individuare e prevenire le condotte penalmente rilevanti poste in essere da coloro che operano, a qualsiasi titolo, per conto della società.

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

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

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

In base alle previsioni dell'art. 6 del D.Lgs. n. 231/2001 l'Ente può essere esonerato dalla responsabilità conseguente alla commissione di reati da parte dei soggetti qualificati ex art. 5, comma 1, lett. a) del D. Lgs. n. 231/2001, se prova che:

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

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

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

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

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

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

organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.
Il Modello deve prevedere, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.
L'efficace attuazione del Modello, inoltre, richiede:

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

1.3.3. Le segnalazioni whistleblowing

Il D. Lgs. n. 24/2023, attuando la Direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, ha modificato quanto previsto dall'art. 6, comma 2 bis[1] del D. Lgs. n. 231/2001 in materia di segnalazioni *Whistleblowing.*
In particolare, il D. Lgs. n. 24/2023 ha previsto una specifica tutela rivolta alle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato.
I Modelli di Organizzazione, Gestione e Controllo devono conformarsi a quanto disposto dal D. Lgs. n. 24/2023 prevedendo canali di segnalazione interna che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.
Ai sensi dell'art. 6 del D. Lgs. n. 24/2023 il segnalante può effettuare una segnalazione esterna attraverso il canale messo a disposizione da ANAC se, al momento della sua presentazione, ricorrano una delle seguenti condizioni:

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

Qualora la segnalazione esterna dovesse essere presentata ad un soggetto diverso dall'ANAC questa deve essere trasmessa all'Autorità entro sette giorni dalla data del suo

[1] Comma introdotto dalla Legge 30 novembre 2017, n. 179 in materia di *Whistleblowing,* G.U. n. 291 del 14 dicembre 2017.

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

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

I segnalanti non possono subire alcun tipo di ritorsione a seguito della segnalazione e, ove ciò invece dovesse accadere, è garantita loro la possibilità di denunciare eventuali comportamenti commessi nel contesto lavorativo direttamente all'Autorità Nazionale Anticorruzione la quale procederà a informare immediatamente il Dipartimento della funzione pubblica presso la Presidenza del Consiglio dei ministri e gli eventuali organismi di garanzia o di disciplina, qualora il lavoratore rientrasse nel settore pubblico, ovvero l'Ispettorato Nazionale del Lavoro qualora la ritorsione si sia consumata nel contesto lavorativo di un soggetto privato.
L'obbligo di informare il datore di lavoro di eventuali comportamenti sospetti rientra già nel più ampio dovere di diligenza ed obbligo di fedeltà del prestatore di lavoro e, conseguentemente, il corretto adempimento dell'obbligo di informazione non può dare luogo all'applicazione di sanzioni disciplinari, ad eccezione dei casi in cui l'informazione sia connotata da intenti calunniosi o sorretta da cattiva fede, dolo o colpa grave. Al fine di garantire l'efficacia del sistema di whistleblowing, è quindi necessaria una puntuale informazione da parte dell'Ente di tutto il personale e dei soggetti che con lo stesso collaborano non soltanto in relazione alle procedure e ai regolamenti adottati dalla Società e alle attività a rischio, ma anche con riferimento alla conoscenza, comprensione e diffusione degli obbiettivi e dello spirito con cui la segnalazione deve essere effettuata.
Con l'obiettivo di dare attuazione alle disposizioni in materia di obbligo di fedeltà del prestatore di lavoro e della legge sul Whistleblowing, si rende dunque necessaria l'introduzione nel Modello di Organizzazione, Gestione e Controllo di un sistema di gestione delle segnalazioni di illeciti che consenta di tutelare l'identità del segnalante e il

connesso diritto alla riservatezza di quest'ultimo, nonché l'introduzione di specifiche previsioni all'interno del sistema disciplinare volte a sanzionare eventuali atti di ritorsione e atteggiamenti discriminatori in danno del segnalante.

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

1.4.1. Le Linee Guida di Confindustria

Ai sensi dell'art. 6 del Decreto, i Modelli possono essere adottati, garantendo le suindicate esigenze, anche sulla base di codici di comportamento redatti dalle associazioni rappresentative degli Enti, comunicati al Ministero della Giustizia ai sensi dell'art. 6, comma 3, del Decreto.
Confindustria si propone, per Statuto, di contribuire, insieme alle istituzioni politiche e alle organizzazioni economiche, sociali e culturali, nazionali ed internazionali, alla crescita economica e al progresso sociale del paese.
Anche in tale ottica, e per essere d'ausilio alle imprese associate, Confindustria ha emanato le "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. n. 231/2001".
La prima versione delle Linee Guida, elaborata nel 2002 dal Gruppo di lavoro sulla "*Responsabilità amministrativa delle persone giuridiche*", costituito nell'ambito del Nucleo Affari Legali, Finanza e Diritto d'Impresa di Confindustria, è stata approvata dal Ministero della Giustizia nel giugno 2004.
A seguito dei numerosi interventi legislativi che, nel frattempo, hanno modificato la disciplina sulla responsabilità amministrativa degli Enti, estendendone l'ambito applicativo a ulteriori fattispecie di reato, il Gruppo di lavoro di Confindustria ha provveduto ad aggiornare le Linee Guida per la costruzione dei modelli organizzativi.
L'ultimo aggiornamento delle Linee Guida, del giugno 2021, è stato approvato dal Ministero della Giustizia in data 8 giugno 2021.
Le 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 al Decreto a giugno 2021.
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. n. 231/2001;
- individuazione delle modalità di commissione degli illeciti;
- esecuzione del *risk assessment*, in un'ottica integrata;
- individuazione dei punti di controllo tesi a mitigare il rischio reato;

- *gap analysis.*

Le componenti più rilevanti del sistema di controllo ideato da Confindustria sono:
- Codice Etico e di Condotta;
- sistema organizzativo;
- procedure manuali ed informatiche;
- poteri autorizzativi e di firma;
- sistemi di controllo e gestione;
- comunicazione al personale e sua formazione.
- disciplina delle modalità per effettuare segnalazioni whistleblowing e modalità di gestione delle stesse.

Le componenti del sistema di controllo devono essere orientate ai seguenti principi:
- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- applicazione del principio di separazione delle funzioni (nessuno può gestire in autonomia un intero processo);
- documentazione dei controlli;
- previsione di un adeguato sistema sanzionatorio per la violazione delle procedure previste dal modello;
- individuazione dei requisiti dell'Organismo di Vigilanza, riassumibili come segue:
  - autonomia e indipendenza;
  - professionalità;
  - continuità di azione.
- obblighi di informazione dell'Organismo di Vigilanza ed individuazione dei criteri per la scelta di tale Organismo.

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

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

1.5. Le sanzioni amministrative applicabili agli Enti

Il Decreto disciplina quattro tipi di sanzioni amministrative applicabili agli Enti per gli illeciti amministrativi dipendenti da reato:
1) le sanzioni pecuniarie (e sequestro conservativo in sede cautelare), applicabili a tutti gli illeciti;

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

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

1.5.1 Le sanzioni pecuniarie

La sanzione pecuniaria è la sanzione fondamentale, applicabile sempre e a tutti gli illeciti amministrativi dipendenti da reato.
La sanzione pecuniaria viene applicata per quote in un numero non inferiore a cento né superiore a mille.
Il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'ente, nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.
L'importo di una quota va da un minimo di Euro 258,23 ad un massimo di Euro 1.549,37 ed è fissato sulla base delle condizioni economiche e patrimoniali dell'ente allo scopo di assicurare l'efficacia della sanzione.
In ogni modo, la pena è ridotta della metà e non può superare, comunque, Euro 103.291,38 se:

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

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

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

della specie di quello verificatosi.
Nel caso in cui concorrono entrambe le condizioni, la sanzione è ridotta dalla metà ai due terzi. In ogni caso, la sanzione pecuniaria non può essere inferiore a Euro 10.329,14.

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

1.5.2 Le sanzioni interdittive

Le sanzioni interdittive si applicano unitamente alla sanzione pecuniaria, ma solamente in relazione ai reati-presupposto per i quali sono espressamente previste.
La loro durata non può essere inferiore a tre mesi e non può essere superiore a due anni.

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

Se necessario, le sanzioni interdittive possono essere applicate congiuntamente.

La loro applicazione, pertanto, può, da un lato, paralizzare lo svolgimento dell'attività dell'Ente, dall'altro, condizionarla sensibilmente attraverso la limitazione della sua capacità giuridica o la sottrazione di risorse finanziarie.

Trattandosi di sanzioni particolarmente gravose, nel Decreto è stabilito che possano essere applicate solo se ricorre almeno una delle seguenti condizioni:
a) l'ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
b) in caso di reiterazione degli illeciti.

Le sanzioni interdittive, salvo quanto disposto dall'art. 25, comma 5 del Decreto, hanno una durata non inferiore a tre mesi e non superiore a due anni; tuttavia, può essere disposta:
a) l'interdizione definitiva dall'esercizio dell'attività se l'Ente ha tratto dal reato un profitto

di rilevante entità ed è già stato condannato, almeno tre volte negli ultimi sette anni, alla interdizione temporanea dall'esercizio dell'attività;

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

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

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

Non si applicano, inoltre, quando, prima della dichiarazione di apertura del dibattimento di primo grado, "concorrono" le seguenti condizioni (c.d. riparazione delle conseguenze del reato):

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

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

1.5.3 La pubblicazione della sentenza di condanna

La pubblicazione della sentenza di condanna può essere disposta quando nei confronti dell'ente viene applicata una sanzione interdittiva.
La sentenza è pubblicata una sola volta, per estratto o per intero, in uno o più giornali indicati dal giudice, i quali, si può ipotizzare, saranno giornali "specializzati" o di "settore", ovvero potrà essere pubblicata mediante affissione nel comune ove l'ente ha la sede

principale. Il tutto a complete spese dell'ente.
Tale sanzione ha una natura meramente afflittiva ed è volta ad incidere negativamente sull'immagine dell'Ente.

1.5.4 La confisca del prezzo o del profitto del reato

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

InfoCert è una Società partecipata da Tinexta S.p.A. e ha come oggetto sociale la produzione, sperimentazione, vendita o commercializzazione di sistemi complessi, prodotti software, tecnologie, strumenti e servizi informatici di interesse del mercato pubblico e privato, ivi incluse le attività di ricerca di base e applicata.
Per il conseguimento dello scopo sociale, la Società può anche, in Italia e all'Estero:

- produrre, sviluppare, gestire e commercializzare prodotti, sistemi e servizi di certificazione e firme elettroniche, compresa quella digitale, nonché, più in generale, prodotti, sistemi e servizi attinenti alla sicurezza informatica;
- predisporre e fornire sistemi informatici e servizi di gestione amministrativa, contabile e del personale di soggetti privati o pubblici o di enti ad essi direttamente o indirettamente collegati, ivi compresa la raccolta, codificazione, elaborazione e presentazione di atti per conto terzi con particolare riferimento a quelli di natura contabile e fiscale;
- fornire servizi telematici, produrre e commercializzare software per elaborazioni di natura finanziaria/ bancaria, distribuire e commercializzare banche dati di natura pubblica o privata, anche nella qualità di agente con o senza esclusiva;
- produrre, sviluppare, gestire e commercializzare prodotti, sistemi e servizi inerenti alla gestione documentale, ivi compresi i processi di conservazione sostitutiva, digitalizzazione e custodia dei documenti;
- produrre, sviluppare, gestire e commercializzare prodotti, sistemi e servizi di posta elettronica, anche certificata, nonché servizi, prodotti o sistemi di comunicazione elettronica o servizi della società dell'informazione, prestare servizi di assistenza tecnica e funzionale, di addestramento e formazione del personale sui servizi e sistemi tecnologici, di consulenza organizzativa, gestionale e di processo, nonché ogni altra attività o servizio comunque finalizzato all'efficiente impiego delle tecnologie dell'informazione da parte di privati, imprese, amministrazioni pubbliche ed enti.

Essa, inoltre, può compiere, in via non prevalente, tutte le operazioni commerciali, industriali, mobiliari, immobiliari e finanziarie, queste ultime purché non nei confronti del pubblico, ritenute dall'organo amministrativo necessarie o utili per il conseguimento dell'oggetto sociale. La Società può, inoltre, non in via prevalente e non nei confronti del pubblico, prestare avalli, fideiussioni ed ogni altra garanzia anche reale ed a favori di terzi. Sempre in via non prevalente e non nei confronti del pubblico potrà procedere all'assunzione, sia diretta che indiretta, di interessenze e partecipazioni in altre società o imprese, qualora tale assunzione non sia finalizzata alla mera compravendita, ma concretizzi un'operazione per il raggiungimento dello scopo sociale.

InfoCert è leader del mercato italiano nei servizi di digitalizzazione e dematerializzazione nonché una delle principali Certification Authority a livello europeo per i servizi di Posta Elettronica Certificata, Firma Digitale e Conservazione digitale dei documenti (Conservatore Accreditato AgID).
Da dicembre 2015 InfoCert è anche gestore accreditato AgID dell'identità digitale di cittadini e imprese, in conformità ai requisiti regolamentari e tecnici dello SPID (Sistema Pubblico per la gestione dell'Identità Digitale).
InfoCert si pone sul mercato come un partner altamente specializzato nei servizi di dematerializzazione, capace di garantire ai propri clienti la piena innovazione nei processi di gestione del patrimonio documentale e informativo.
Con sedi a Roma, Milano e Padova, InfoCert rivolge la propria offerta sia alle imprese, pubbliche e private, operanti nel settore Bancario, Assicurativo, Farmaceutico, Manifatturiero, Energy, Utilities, Distribuzione Commerciale, Ambiente, Qualità, Sicurezza, Sanità, Pubblica Amministrazione; sia ad Associazioni di Categoria, Ordini Professionali e Professionisti.
La società progetta e sviluppa soluzioni informatiche ad alto valore tecnologico di dematerializzazione dei processi documentali, attraverso componenti di gestione documentale, conservazione digitale, firma digitale e posta elettronica certificata. I clienti – siano essi imprese o professionisti - vengono accompagnati nella scelta di servizi e soluzioni pienamente rispondenti alle esigenze organizzative, così come ai vincoli normativi generali e specifici di settore.
InfoCert è un Provider di servizi di Digital Trust pienamente conforme alla normativa introdotta dal Regolamento eIDAS (electronic IDentification Authentication and Signature).

Il maturato bagaglio di conoscenze compliance ha consentito nel tempo alla Società di espandere le proprie attività anche all'estero e di approdare quindi in differenti Paesi rispondendo, di volta in volta, alle specifiche normative ivi vigenti.

Tale inclinazione è confermata anche dall'espansione della Società a livello nazionale e internazionale attraverso le proprie Controllate.

2.2 La “filosofia” di Infocert S.p.A.

Infocert S.p.A. ha sviluppato standard etici elevati, una cultura di trasparenza ed integrità e un forte senso di missione e di consapevolezza del valore del lavoro nell’attività aziendale quotidiana.

La Società è consapevole del fatto che garantire condizioni di integrità nella gestione delle attività aziendali è uno strumento di tutela della immagine aziendale, nonché degli affari e delle aspettative degli azionisti. Sulla scia del proprio credo aziendale è sensibile alla necessità di divulgare e rafforzare la cultura della trasparenza e della correttezza.

L’impegno della Società verso i temi della legalità, integrità e trasparenza è testimoniato anche del perseguimento della certificazione ISO 37001:2016 “Sistemi di gestione per la prevenzione della corruzione”.
Allo stesso modo l'obiettivo di promuovere il cambiamento culturale per la creazione di ambienti di lavoro inclusivi e paritari ha portato alla scelta di certificare l’Azienda secondo la PDR 125 per la parità di genere. Il sistema di attuazione della prassi è basato su un monitoraggio approfondito e una valutazione di sei ambiti specifici: cultura e strategia, governance, processi HR, opportunità di crescita e inclusione delle donne in azienda, equità retributiva per genere, tutela della genitorialità e conciliazione vita-lavoro.

2.3 L’assetto istituzionale di Infocert S.p.A.: organi e soggetti

InfoCert S.p.A. ha adottato il sistema di amministrazione tradizionale, pertanto presenta un’assemblea dei soci, un organo amministrativo che si esplicita nel Consiglio d’Amministrazione e un organo di controllo costituito dal Collegio Sindacale.

Assemblea

L’assemblea è l’organo avente funzioni deliberative, le cui competenze sono per legge circoscritte alle decisioni di maggior rilievo della vita sociale, con l’esclusione delle competenze gestorie. Tale organo regolarmente costituito 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 dissenzienti.
La funzione dell’assemblea è quella di formare la volontà della Società nelle materie riservate alla sua competenza dalla legge e dallo Statuto.

L’assemblea ordinaria è competente di deliberare in merito:

a) all’approvazione del bilancio;
b) alla nomina e alla revoca degli amministratori, dei sindaci, del presidente del collegio sindacale e, quando previsto, del soggetto al quale è demandato il controllo contabile;
c) alla determinazione dei compensi di amministratori e sindaci;
d) alle decisioni in materia di responsabilità di amministratori e sindaci;

e) alle altre materie attribuite dalla legge alla competenza assembleare, nonché alle autorizzazioni eventualmente richieste per il compimento di atti di amministrazione (ferma restando la responsabilità degli amministratori per il compimento di tali atti);
f) all'approvazione del regolamento assembleare.

Sono di competenza dell'assemblea straordinaria:
a) la nomina, sostituzione e determinazione dei poteri dei liquidatori;
b) ogni altra materia attribuita dalla legge.

Consiglio di Amministrazione

La Società è amministrata da un Consiglio di Amministrazione composto da un minimo di 5 (cinque) membri ad un massimo di 9 (nove) membri scelti anche fra i non soci, nominati per la prima volta nell'atto costitutivo e successivamente dall'Assemblea ordinaria dei Soci che ne stabilisce il compenso e il numero.
Il CdA è investito di tutti i poteri di ordinaria e straordinaria amministrazione, con funzione di supervisione strategica. Il CdA può attribuire alcuni dei propri poteri al Presidente e agli Amministratori Delegati, determinando il contenuto, i limiti e le modalità di esercizio della delega nonché, sentito il parere del Collegio Sindacale, definirne la remunerazione.
A tale organo è affidata la gestione dell'impresa sociale e agli amministratori spetta il compimento di tutte le operazioni/ atti per il conseguimento dell'oggetto sociale, ad esclusione di quelli che ex lege sono di competenza dell'Assemblea. Gli amministratori:
- deliberano su tutti gli argomenti attinenti alla gestione della Società,
- hanno la rappresentanza generale della Società,
- danno input alle attività dell'assemblea,
- curano la tenuta dei libri e delle scritture contabili,
- redigono il bilancio d'esercizio e curano gli adempimenti pubblicitari previsti per legge,
- operano al fine di prevenire il compimento di atti pregiudizievoli per la Società o, quanto meno, eliminarne o limitarne gli impatti.

Al CdA è poi attribuita, ai sensi dell'art. 2365 comma 2 del Codice Civile, la competenza, fatti salvi i limiti di legge, sulle seguenti deliberazioni:
- la fusione nei casi di cui agli artt. 2505 e 2505 bis del Codice Civile,
- l'istituzione e la soppressione di sedi secondarie; l'apertura, la chiusura ed il trasferimento di dipendenze ed uffici della Società, meri Uffici Amministrativi, stabilimenti industriali, depositi e rappresentanze,
- l'eventuale riduzione del capitale sociale in caso di recesso dei soci,
- gli adeguamenti dello Statuto e del Regolamento Assembleare a disposizioni normative,
- il trasferimento della sede sociale nel territorio nazionale,
- determinare gli indirizzi generali di gestione e di sviluppo organizzativo,
- stabilire i criteri relativi alla formazione ed alla modifica dei regolamenti interni,
- nominare il Direttore Generale, nonché i Vicedirettori Generali, i Direttori Centrali e i Dirigenti,
- assumere o cedere partecipazioni in Italia ed all'estero,

- deliberare - salvo quanto previsto dallo statuto – sulla designazione e nomina di Amministratori e Sindaci di istituti, società, consorzi in genere cui la Società partecipi, nonché di altri enti alla nomina dei cui Amministratori e/o Sindaci essa sia chiamata a provvedere,
- deliberare in materia di acquisto e di vendita di immobili di proprietà,
- deliberare sulla formazione dei contratti che regolano il rapporto di lavoro e il trattamento di quiescenza del personale della Società.

È fatta salva la facoltà del Consiglio di rimettere all'Assemblea la competenza su deliberazioni concernenti le suddette materie. Il Consiglio di Amministrazione, nei limiti previsti dall'art. 2381 c.c., può delegare tutte o parte delle proprie attribuzioni ad un comitato esecutivo composto da alcuni dei suoi membri, determinando il contenuto, i limiti e le eventuali modalità di esercizio della delega.
La firma sociale e la rappresentanza sociale generale di fronte ai terzi ed in giudizio spettano al Presidente del CdA e agli amministratori delegati nell'ambito delle deleghe. Il Presidente, il Vicepresidente 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) 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. Tale organo vigila sull'osservanza delle norme di legge, regolamentari e statutarie, sulla corretta amministrazione, e sull'adeguatezza degli assetti organizzativi della Società. Esso ha la responsabilità di vigilare sulla funzionalità del complessivo sistema dei controlli interni. Considerata la pluralità di funzioni e strutture aziendali aventi compiti e responsabilità di controllo, tale organo è tenuto ad accertare l'efficacia di tutte le strutture e funzioni coinvolte nel sistema dei controlli e l'adeguato coordinamento delle medesime, promuovendo gli interventi correttivi delle carenze e delle irregolarità rilevate.

DPO

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 Privacy Officer della Società.
In adempimento a quanto previsto dal Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679 è stato nominato il DPO con il compito di:

a) sorvegliare l'osservanza del GDPR, valutando i rischi di ogni Trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
b) condurre una valutazione di impatto sulla protezione dei dati (DPIA);
c) informare e sensibilizzare la Società riguardo agli obblighi derivanti dal Regolamento e da altre disposizioni in materia di protezione dei dati;
d) cooperare con l'Autorità di Controllo e fungere da punto di contatto per la medesima su ogni questione connessa al trattamento;
e) fungere da punto di contatto con l'Interessato per l'esercizio dei diritti di cui agli

art. 15-22 del GDPR;
f) supportare il Titolare o il Responsabile in ogni attività connessa al trattamento di Dati Personali, anche con riguardo all'eventuale tenuta di un registro delle attività di trattamento (art. 30 GDPR);
g) coordinare e supervisionare l'attività dei Privacy Officer che, in ossequio a quanto stabilito dalla Data Protection Policy di Gruppo, presidiano il tema della protezione dei dati personali nelle società controllate.
Nell'ambito delle funzioni di supporto al DPO, il Privacy Officer di InfoCert 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.

Group Head of Information Security

Il Group Head of Information Security coordina a livello di Gruppo tutti i programmi di cybersecurity, che prevedono l'utilizzo da parte di tutte le Società Controllate di un pacchetto di servizi erogati da altre Società del Gruppo, previa valutazione del grado di maturità dell'azienda in ambito sicurezza e successiva formulazione di un action plan finalizzato a raggiungere i target di Gruppo prefissati.
Inoltre, identifica la Security Strategy allineata con gli obiettivi di business, pianifica e sviluppa un Security Program per la messa in opera di tutte le iniziative previste nella Security Strategy; definisce le metodologie e le strumentazioni a supporto delle attività di Risk Management in ambito Cyber e a supporto delle attività di Incident Management e presidio del processo.

Chief Information Security Officer

Il Chief Information Security Officer (CISO) di InfoCert cura e garantisce la sicurezza, riservatezza, integrità e disponibilità delle informazioni gestite all'interno dell'organizzazione e delle risorse ICT aziendali.

Compliance Manager

L'attuazione della compliance nello svolgimento delle attività è affidata a diverse funzioni aziendali che svolgono il proprio ruolo in ottemperanza alle policy di Capogruppo.

Risk Manager

Il Risk Manager di InfoCert S.p.A. supporta il Consiglio di Amministrazione e l'Amministratore Delegato nell'implementazione delle linee guida di gruppo in materia di sistema di controllo interno e gestione dei rischi, coordinandosi con il Risk Manager di Gruppo.

Dirigente Preposto

Ai sensi dell'articolo 19 dello Statuto, il Consiglio di Amministrazione di Tinexta S.p.A., previo parere obbligatorio ma non vincolante del Collegio Sindacale e con l'ordinaria maggioranza prevista nel presente statuto, nomina il Dirigente Preposto di cui all'art. 154-bis del TUF, eventualmente stabilendo un determinato periodo di durata nell'incarico, tra

i dirigenti in possesso di un'esperienza di almeno un triennio maturata ricoprendo posizioni di dirigenza in aree di attività amministrativo/contabile e/o finanziaria e/o di controllo presso la società e/o sue società controllate e/o presso altre società per azioni.

Il Consiglio di Amministrazione può, sempre previo parere obbligatorio ma non vincolante del Collegio Sindacale e con l'ordinaria maggioranza prevista nel presente statuto, revocare l'incarico di Dirigente Preposto, provvedendo contestualmente ad un nuovo conferimento dell'incarico medesimo.

Il Consiglio di amministrazione, previo parere favorevole del Collegio Sindacale, ha individuato, quale Dirigente Preposto, il Group Chief Financial Officer di Tinexta.
All'atto della nomina, il Consiglio ha attribuito al Dirigente Preposto tutti i poteri ed i mezzi per l'esercizio dei compiti ad esso attribuiti dalla vigente normativa e dallo Statuto, ivi incluso l'accesso diretto a tutte le funzioni, uffici e informazioni necessarie per la produzione e la verifica dei dati contabili, finanziari ed economici, senza necessità di autorizzazione alcuna.

Ai sensi dell'art 154-bis del TUF, il Dirigente Preposto è responsabile della predisposizione di adeguate procedure amministrative e contabili per la formazione del bilancio di esercizio, del bilancio consolidato, nonché di ogni altra comunicazione di carattere finanziario. I documenti della Società e del Gruppo diffusi al mercato, relativi all'informativa contabile anche infrannuale, sono accompagnati da una dichiarazione scritta del Dirigente Preposto che ne attesti la conformità alle disposizioni normative previste dalla L.262/2005.
Il Dirigente Preposto si coordina con le funzioni aziendali della Società, delle controllate incluse nel perimetro di consolidamento, ivi inclusa InfoCert nell'ambito della quale è stato identificato il Referente Legge 262/2005, e gli organismi di corporate governance, al fine di fornire e ricevere informazioni in merito allo svolgimento di attività che hanno impatto sulla situazione economica, patrimoniale o finanziaria del Gruppo Tinexta. Tutte le funzioni aziendali appartenenti alle società del Gruppo Tinexta (incluse nel perimetro di consolidamento) e gli organismi di governance della capogruppo quali il Consiglio di Amministrazione, il Collegio Sindacale, il Comitato Controllo e Rischi e Sostenibilità, l'Organismo di Vigilanza, la società di revisione, gli organismi istituzionali che comunicano con l'esterno e l'Internal Audit, sono responsabili di interagire con il Dirigente Preposto al fine di informare ed eventualmente segnalare eventi che possano determinare modifiche significative nei processi, qualora esse abbiano impatto sull'adeguatezza o sul concreto funzionamento delle procedure amministrativo-contabili esistenti. I Responsabili Amministrativi (Referenti Legge 262/2005) di ciascuna di tali società sono stati individuati come responsabili di garantire l'adeguata implementazione e il mantenimento del sistema di controllo interno nelle rispettive organizzazioni per conto del Dirigente Preposto. A tale riguardo, il modello di governance amministrativo-finanziaria del Gruppo Tinexta prevede un sistema di attestazioni interne, che pone in capo agli Amministratori Delegati/Direttori Generali e ai Responsabili Amministrativi delle singole società del Gruppo Tinexta l'obbligo di rilasciare una specifica attestazione circa

l'affidabilità e l'accuratezza dei sistemi e processi per la reportistica finanziaria destinata alla predisposizione del bilancio consolidato di Gruppo Tinexta a supporto delle attestazioni semestrali e annuali effettuate dal Dirigente Preposto e dall'Amministratore Delegato (ai sensi del comma 5 dell'art.154-bis del TUF).

Per l'esercizio delle sue attività, il Dirigente Preposto si avvale della struttura di Internal Control Over Financial Reporting, a suo riporto e con il compito di supportarlo nelle attività e nei controlli previsti dalla Legge, dal Manuale Metodologico e dalle *best practices* di riferimento.

Internal Audit di Gruppo

Tinexta dispone di una funzione di Internal Audit la cui missione è quella di proteggere ed accrescere il valore della Società e del Gruppo, fornendo *assurance* obiettiva e *risk – based* e consulenza interna, finalizzate a valutare e migliorare i processi di controllo, di gestione dei rischi e di corporate governance.
La funzione risponde gerarchicamente al Consiglio di Amministrazione della Società, riportando le risultanze dei lavori svolti anche agli organi amministrativi, di controllo e vigilanza delle controllate interessate.
Tinexta, in forza di apposito contratto di service con Infocert, fornisce attività di controllo di terzo livello, pertanto, può essere chiamata a svolgere le suddette attività di *assurance* e consulenza su specifiche aree aziendali.

Società di revisione

La Società ha affidato la revisione legale ad una società esterna incaricata dall'Assemblea dei soci su proposta motivata del Collegio Sindacale in conformità con le prescrizioni di legge al tempo vigenti contenute nel D. Lgs. n. 39/2010, applicabili agli enti di interesse pubblico.

Funzione di Conformità per la Prevenzione della Corruzione / Responsabile Anticorruzione

La Società, in ottemperanza alla norma ISO 37001:2016 "Sistemi di gestione per la prevenzione della corruzione" ha provveduto alla identificazione della Funzione di Conformità per la Prevenzione della Corruzione e alla nomina del Responsabile Anticorruzione. A tale funzione sono conferite le responsabilità di cui ai punti 5.3.2 "Funzione di Conformità per la Prevenzione della Corruzione" e 9.4 "Riesame da parte della Funzione di Conformità per la Prevenzione della Corruzione" della menzionata norma.

Le altre funzioni aziendali

Nell'organigramma vengono individuate le funzioni e i relativi responsabili.
Più specificamente, nell'organigramma è precisato che operano a diretto riporto dell'Amministratore Delegato i responsabili delle seguenti direzioni:

- Business Operations & International Integration;
- Sales;

- Product Factory;
- Legal, Regulatory & Privacy;
- Human Resources;
- Administration, Finance, Control, Procurement, BU Digital Trust.

2.4 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 ed è incentrato sulla trasparenza delle scelte gestionali sia all'interno della Società sia nei confronti del mercato; sull'efficienza e sull'efficacia del sistema di controllo interno; sulla rigorosa disciplina dei potenziali conflitti di interesse e su saldi principi di comportamento per l'effettuazione di operazioni con parti correlate.

I suddetti strumenti possono essere così riassunti:

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

Regolamento assembleare: disciplina lo svolgimento dell'Assemblea ordinaria e straordinaria di InfoCert S.p.A. al fine di garantire l'ordinato svolgimento delle adunanze, nel rispetto del fondamentale diritto del socio di chiedere chiarimenti sugli argomenti in discussione, di esprimere la propria opinione e di formulare le proposte.

Codice Etico e di Condotta 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 e di Condotta di Gruppo fissa i principi etici nei quali le Società del Gruppo TINEXTA si rispecchiano e ai quali, coerentemente, si devono ispirare tutti i soggetti con i quali esse operano.
In particolare, la Società si ispira ai seguenti principi:

- osservanza delle leggi vigenti nazionali, comunitarie e in generale la normativa internazionale dei Paesi in cui opera, i regolamenti o codici interni e, ove applicabili, le norme di deontologia professionale;
- onestà, correttezza e trasparenza delle azioni, poste in essere nel perseguimento dei propri obiettivi;
- rispetto dei Diritti Umani nello svolgimento delle nostre operazioni e lungo la catena del valore è un fattore imprescindibile nella gestione aziendale;
- diversità e inclusione all'interno delle politiche societarie;
- valorizzazione delle capacità e delle competenze delle persone, in modo che ognuno possa esprimere al meglio il proprio potenziale;
- fedeltà nei rapporti con le controparti di qualsiasi natura;
- tutela della privacy e delle informazioni sensibili in rispetto di quanto previsto dalla normativa in materia di privacy;

- prevenzione della corruzione, anche internazionale, sia dal lato attivo che passivo. A tal fine, a titolo esemplificativo: sono vietati favori, comportamenti collusivi, sollecitazioni dirette e/o attraverso terzi, al fine di ottenere vantaggi per la Società, per sé o per altri; il personale non deve cercare di influenzare impropriamente le decisioni della controparte (funzionari pubblici/esponenti degli Enti Privati che trattano o prendono decisioni per conto rispettivamente delle Pubbliche Amministrazioni e degli Enti Privati); non è mai consentito corrispondere né offrire, direttamente o indirettamente, denaro, omaggi o qualsiasi utilità alla Pubblica Amministrazione e agli Enti Privati o a loro familiari, per compensare un atto del proprio ufficio;
- mantenimento di un rapporto corretto e trasparente con l'amministrazione finanziaria, di una gestione etica del tema fiscale, nonché rispettare la normativa in materia fiscale;
- trasparenza verso il mercato, le Autorità di Vigilanza, gli Enti e le Istituzioni assicurando la veridicità, completezza e tempestività nelle comunicazioni sociali di qualsiasi natura
- contrasto a qualsiasi restrizione del confronto competitivo e astensione da pratiche commerciali collusive che favoriscano la conclusione di affari a vantaggio della Società e che comportino una violazione della normativa vigente in materia di concorrenza leale;
- imparzialità che prevede l'obbligo di evitare situazioni di conflitto d'interesse;
- ripudio del terrorismo che trova attuazione anche attraverso l'esecuzione di verifiche circa la non appartenenza dei potenziali partner alle Liste di Riferimento, pubblicate dall'Unità di Informazione Finanziaria (UIF), istituita presso la Banca d'Italia ex art. 6 c. 1 del D. Lgs. n. 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.

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

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

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

Per “delega” si intende il trasferimento, non occasionale, all’interno della Società, di responsabilità e poteri da un soggetto all’altro in posizione a questo subordinata. Per “procura” si intende il negozio giuridico con il quale una parte conferisce all’altra il potere di rappresentarla (ossia ad agire in nome e per conto della stessa). La procura, a differenza della delega, assicura alle controparti di negoziare e contrarre con le persone preposte ufficialmente a rappresentare la Società.
Al fine di un‘efficace prevenzione dei reati, il sistema di deleghe e procure deve rispettare i seguenti requisiti essenziali:

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

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

Regolamento di Gruppo:
in qualità di Società Capogruppo, TINEXTA esercita nei confronti delle Società da essa controllate un’attività di direzione e coordinamento, condotta in ogni momento nel rispetto dell’interesse sociale di tali Società e in ossequio ai principi di corretta e prudente gestione societaria e imprenditoriale.
Nell’esercizio di tale attività, TINEXTA definisce ed implementa modelli organizzativi e di funzionamento di Gruppo finalizzati a:

- garantire livelli di integrazione coerenti con la realizzazione del comune progetto strategico, nell’ottica di massimizzare il valore del Gruppo, sempre nel rispetto dell’autonomia giuridica delle Società Controllate e dei principi di corretta gestione societaria e imprenditoriale delle medesime;
- ottimizzare le sinergie determinate dall’appartenenza al Gruppo, valorizzando le caratteristiche delle diverse Società;
- assicurare omogeneità e coerenza organizzativa all’interno del Gruppo, al fine di semplificare i processi trasversali, diffondere best practices e rafforzare le competenze interne.

In tale contesto, TINEXTA definisce il Regolamento di Gruppo che ha lo scopo di delineare le modalità di esercizio dell'attività di direzione e coordinamento da parte della capogruppo e disciplinare i rapporti fra questa e le società Controllate, destinatarie del Regolamento stesso.
Il Regolamento di Gruppo non descrive, né disciplinai processi gestiti internamente alle singole società e le interazioni tra le funzioni della Capogruppo.
In attuazione del suddetto Regolamento, sono emanate le Procedure/Policy/Linee Guida di Gruppo per le quali si rinvia all'Allegato 1 del presente documento.

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

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

Modello di governance in ambito Compliance: nell'ambito dei documenti di Dialogo e Controllo emessi dalla Capogruppo, InfoCert ha adottato gli specifici documenti normativi interni per identificare, valutare, monitorare e controllare il rischio di non conformità alle norme ("rischio di compliance") a cui può essere esposta. Rientrano tra tali documenti:

- Procedura Compliance di Gruppo;
- Linee Guida Anticorruzione.

Inoltre, InfoCert, certificata ISO 37001:2016 si è dotata anche dei seguenti documenti normativi (redatti in coerenza con quelli di Dialogo e Controllo):

- Politica Anticorruzione.
- Procedura di Due Diligence Anticorruzione

Modello di governance in ambito Risk Management: nell'ambito dei documenti di Dialogo e Controllo emessi dalla Capogruppo, InfoCert ha adottato le Linee Guida di Enterprise Risk Management per la gestione del processo ERM finalizzato a identificare, valutare e gestire tutti i rischi che possono avere impatto sull'attività d'impresa della Società e così influire sul raggiungimento degli obiettivi strategici e di business in linea con la propensione al rischio definita nel Risk Appetite Statement dal Consiglio di Amministrazione.
In aggiunta, InfoCert si è dotata anche di un proprio documento metodologico di Risk Management "Metodologia Risk Management" redatto in coerenza con le Linee Guida sopra richiamate.

Modello di governance in ambito Privacy: la Società a seguito dell'entrata in vigore del Regolamento Generale sulla Protezione dei Dati – Regolamento UE 2016/679 ha adottato una serie di misure e di azioni che permettono il monitoraggio ed il mantenimento delle stesse, nell'ottica di Sistema di gestione della Privacy richiesto dal GDPR. Gli adempimenti in tema privacy confluiscono all'interno del Sistema di Gestione integrato di InfoCert, già certificato per le norme ISO 9001, 27001, 20000 e 14001.

InfoCert è inoltre un Qualified Trust Service Provider (ETSI EN 319 401) per i servizi di certificazione qualificata di: firme elettroniche, sigilli elettronici, validazione temporale e autenticazione siti web.
In ambito Privacy vengono poi adottati i documenti di Dialogo e Controllo emessi da parte della Capogruppo.

Modello di governance in ambito Cyber Security: come indicato anche per il Modello Privacy, la documentazione inerente il modello di Governance in ambito Cyber Security confluisce all'interno del Sistema di Gestione integrato di InfoCert, già certificato per le norme ISO 9001, 27001, 20000 e 14001. Inoltre, si evidenzia nuovamente che InfoCert è un Qualified Trust Service Provider (ETSI EN 319 401) per i servizi di certificazione qualificata di: firme elettroniche, sigilli elettronici, validazione temporale e autenticazione siti web.
Tra i documenti normativi adottati vi sono:

- Policy Generale di sicurezza;
- Policy Password, credenziali e strumenti di autenticazione;
- Policy Utilizzo workstation posta elettronica e internet;
- Policy di back up;
- Procedura di Incident Management;
- Istruzione Gestione Accessi Fisici DC/CA;
- Policy Amministratori di Sistema;
- Policy Operativa di back up.

Vengono poi adottati i documenti di Dialogo e Controllo emessi da parte della Capogruppo.

Modello di governance in ambito ESG: la Società si è dotata di specifiche policy (emesse dalla Capogruppo Tinexta) in cui definisce il proprio impegno nella gestione della sostenibilità e delle tematiche ESG rilevanti, in modo sempre più integrato alla strategia e alle attività operative aziendali. Si riporta di seguito l'elenco di tali policy:

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

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

di monitoraggio per accertare l'implementazione dei correttivi definiti. Tale attività di monitoraggio e di test del sistema di controllo sull'informativa finanziaria è coordinata dall'Unità Organizzativa Internal Control over Financial Reporting e condotta con il supporto della funzione Internal Audit del Gruppo Tinexta secondo uno schema di tipo "*agreed upon procedures*". Gli esiti delle attività di monitoraggio sono oggetto di un flusso informativo periodico (semestrale) sullo stato del sistema di controllo sull'informativa finanziaria relativamente al disegno, struttura e funzionamento del sistema, da parte del Responsabile Internal Control over Financial Reporting, direttamente nei confronti del Dirigente Preposto, oltre che al top management, al Comitato Controllo e Rischi e Sostenibilità e al Collegio Sindacale per le valutazioni di competenza.

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 il monitoraggio della corretta esecuzione delle attività affidate in service;
- definire una clausola con cui le parti si impegnano al rispetto dei principi di organizzazione, gestione e controllo idonei a prevenire la commissione di atti illeciti di cui al d.lgs. 231/01, definiti nel Modello di Organizzazione, Gestione e Controllo adottato o altro modello di compliance, ove non sia vigente la disciplina 231, contenente presidi di controllo coerenti con quelli previsti nel Modello di organizzazione, gestione e controllo adottato dalla Società.

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 DI INFOCERT S.P.A.

3.1 Obiettivi e funzione del Modello

InfoCert è particolarmente sensibile all'esigenza di diffondere e consolidare la cultura della trasparenza e dell'integrità, poiché, anche prescindendo dall'aspetto strettamente giuridico-sanzionatorio sin qui illustrato, tali valori costituiscono il fulcro del credo societario della Società e delle controllate.
Il raggiungimento delle predette finalità si concretizza in un sistema coerente di principi, procedure organizzative, gestionali e di controllo e disposizioni che danno vita al Modello che la Società ha predisposto e adottato.

Tale Modello ha quali obiettivi quelli di:

- sensibilizzare i Destinatari richiedendo loro, nei limiti delle attività svolte nell'interesse della Società, di adottare comportamenti corretti e trasparenti, in linea con i valori etici a cui la stessa si ispira nel perseguimento del proprio oggetto sociale e tali da prevenire il rischio di commissione degli illeciti contemplati nel Decreto;
- determinare nei predetti soggetti la consapevolezza di potere incorrere, in caso di violazione delle disposizioni impartite dalla Società, in conseguenze disciplinari e/o contrattuali, oltre che in sanzioni penali e amministrative comminabili nei loro confronti;
- istituire e/o rafforzare controlli che consentano alla Società di prevenire o di reagire tempestivamente per impedire la commissione di illeciti da parte dei soggetti apicali e delle persone sottoposte alla direzione o alla vigilanza dei primi che comportino la responsabilità amministrativa della Società;
- consentire alla Società, grazie a una azione di monitoraggio sulle aree di attività a rischio, di intervenire tempestivamente, al fine di prevenire o contrastare la commissione dei reati stessi e sanzionare i comportamenti contrari al proprio Modello;
- migliorare l'efficacia e la trasparenza nella gestione delle attività;
- determinare una piena consapevolezza nel potenziale autore dell'illecito che la commissione di un eventuale illecito è fortemente condannata e contraria – oltre che alle disposizioni di legge – sia ai principi etici ai quali la Società intende attenersi, sia agli stessi interessi della Società anche quando apparentemente potrebbe trarne un vantaggio.

3.2 Destinatari del Modello

Le regole contenute nel Modello si applicano in primo luogo a coloro che svolgono funzioni di rappresentanza, amministrazione o direzione della Società nonché a chi esercita, anche di fatto, la gestione e il controllo della Società.
Il Modello si applica, inoltre, a tutti i dipendenti della Società, ivi compresi 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 rispetto del Codice Etico e di Condotta di Gruppo e del Modello 231/01.
In particolare, con riferimento ad eventuali partners, in Italia e all'estero, con cui la Società può operare, pur nel rispetto dell'autonomia delle singole entità giuridiche, la Società si fa promotrice dell'adozione di un sistema di controllo interno atto a prevenire anche i reati presupposto del D. Lgs. n. 231/01 adoperandosi, attraverso la previsione di specifiche clausole contrattuali, per garantire che gli stessi uniformino la propria condotta ai principi posti dal Decreto e sanciti nel Codice Etico e di Condotta di Gruppo.

3.3 Struttura del Modello: Parte Generale e Parte Speciale

Il Modello è articolato nella presente "Parte Generale", che ne contiene i principi fondamentali e in una "Parte Speciale", suddivisa in capitoli, il cui contenuto fa riferimento alle tipologie di reato previste dal Decreto e ritenute potenzialmente verificabili all'interno di InfoCert S.p.A.
La Parte Generale, dopo aver fornito le "definizioni" dei principali istituti e concetti presi in considerazione nel Modello, illustra dapprima i principi generali, i criteri ed i presupposti per l'attribuzione della responsabilità amministrativa degli Enti (individuazione dei soggetti attivi del reato- presupposto; loro "legame" con l'Ente; concetti di "interesse" o "vantaggio" dell'Ente; catalogo dei reati-presupposto della responsabilità amministrativa degli Enti; etc.), per poi chiarire quali sono le condizioni per l'esonero della responsabilità amministrativa degli Enti e, in assenza di quest'ultime, le gravi sanzioni amministrative applicabili all'Ente. Nella redazione del Modello si è cercato di renderne il contenuto fruibile a tutti i livelli aziendali, al fine di determinare una piena consapevolezza in tutti coloro che operano in nome e per conto della Società, sia in relazione alla materia della responsabilità da reato degli Enti, sia con riferimento alle gravi conseguenze sanzionatorie in cui incorrerebbe la Società qualora venga commesso uno dei reati contemplati dal Decreto e dalla Legge 146/06.
Calandosi nel contesto aziendale, sono stati poi analizzati gli strumenti di governance, il sistema di controllo interno e l'assetto societario.
Inoltre, vengono descritti gli obiettivi, la funzione e i destinatari del Modello, nonché la metodologia adottata per l'attività di redazione/aggiornamento del Modello di organizzazione, gestione e controllo.

La Parte Generale, infine, tratta dell'Organismo di Vigilanza e dei flussi informativi nei confronti di quest'ultimo, del sistema disciplinare e sanzionatorio dei principi di riferimento per la comunicazione e la formazione.
Nella "Parte Speciale" vengono affrontate le aree di attività della Società considerate a rischio in relazione alle diverse tipologie di reato previste dal Decreto e dalla Legge n. 146/2006 ritenute potenzialmente verificabili all'interno della Società.

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

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

In relazione alla descrizione normativa delle fattispecie e alla tipologia di attività svolta dalla Società, l'analisi delle aree potenzialmente a rischio consente ragionevolmente di escludere in astratto la rilevanza dei delitti in materia di falsità in monete, in carte di pubblico credito in valori in bollo e in strumento o segni di riconoscimento (ex art. 25-*bis*), dei reati di razzismo e xenofobia (*art.25-terdecies*), dei reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (ex art. 25-*quaterdecies*), dei reati di contrabbando (art. 25-sexiesdecies), nonché quelli contro il patrimonio culturale (art. 25-*septiesdecies*) e quelli di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-*duodevicies*).
Infine, in alcun modo riferibili all'attività di InfoCert S.p.A. è il delitto di mutilazione organi genitali femminili (art. 25-*quater.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 monosoggettiva degli stessi possono servire alla prevenzione della loro commissione in forma plurisoggettiva, stabile e organizzata.

Nell'eventualità in cui si rendesse necessario procedere all'emanazione di ulteriori specifici capitoli della Parte Speciale, relativamente a nuove fattispecie di reato che in futuro venissero ricomprese nell'ambito di applicazione del Decreto è demandato 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.

3.4 Il progetto della Società per la definizione e l'aggiornamento del proprio Modello

La Società ha proceduto all'adozione del Modello in quanto consapevole che tale sistema, seppur costituendo una "facoltà" e non un obbligo, in quanto 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.
Tale Modello è stato successivamente aggiornato[2] in conseguenza delle modifiche normative che hanno interessato il catalogo dei reati-presupposto e delle modifiche organizzative intervenute all'interno della stessa.
In particolare, nel corso del 2023, la Società ha proseguito il percorso di adeguamento al D.Lgs. n. 231/01, al fine di recepire all'interno del Modello e del relativo Risk Assessment le variazioni normative intercorse a partire dalla data di approvazione della precedente versione del Modello stesso. Quanto di seguito riportato si riferisce pertanto alla versione aggiornata del Modello.
La metodologia scelta per eseguire il progetto, in termini di organizzazione, definizione delle modalità operative, strutturazione in fasi, assegnazione delle responsabilità tra le varie funzioni, è stata elaborata al fine di garantire la qualità e l'autorevolezza dei risultati.
Il progetto è articolato nelle fasi sinteticamente di seguito riassunte, che esclusivamente per una spiegazione metodologica, sono evidenziate autonomamente.

3.4.1 Individuazione delle aree, delle attività e dei processi sensibili

L'art. 6, comma 2, lett. a) del D. Lgs. n. 231/2001 indica, tra i requisiti del Modello, l'individuazione dei processi e delle attività nel cui ambito possono essere commessi i reati espressamente richiamati dal Decreto. Si tratta, in altri termini, di quelle attività e processi che comunemente vengono definiti "sensibili" (di seguito, "Attività Sensibili", identificate nell'ambito delle cosiddette "Aree a Rischio").
Scopo della prima fase è stato identificare gli ambiti oggetto dell'intervento e individuare preliminarmente le Attività Sensibili.
Propedeutica all'individuazione delle Attività Sensibili è l'analisi della struttura organizzativa della Società, svolta al fine di meglio comprendere l'attività della Società e di identificare gli ambiti oggetto dell'intervento.
L'analisi della struttura organizzativa della Società ha consentito l'individuazione dei processi/Attività Sensibili e la preliminare identificazione delle funzioni responsabili di tali processi/attività.
Qui di seguito sono elencate le attività svolte nella prima fase:

[2] Per l'elenco degli aggiornamenti, si veda la tabella "Adozione e Revisione" a pagina 2 della Parte Generale.

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

3.4.2 Identificazione dei key Officer

Scopo della seconda fase è stato identificare i responsabili dei processi / Attività Sensibili, ovvero le risorse con una conoscenza approfondita dei processi / Attività Sensibili e dei meccanismi di controllo attualmente in essere (di seguito, "key Officer"), completando e approfondendo l'inventario preliminare dei processi / Attività Sensibili nonché delle funzioni e dei soggetti coinvolti.
Le attività operative per l'esecuzione della fase in oggetto presupponevano la raccolta delle informazioni necessarie per i) comprendere ruoli e responsabilità dei soggetti partecipanti alle Attività Sensibili e ii) identificare i key Officer in grado di fornire il supporto operativo necessario a dettagliare le Attività Sensibili ed i relativi meccanismi di controllo.
In particolare, i key Officer sono stati identificati nelle persone di più alto livello organizzativo in grado di fornire le informazioni di dettaglio sui singoli processi e sulle attività delle singole funzioni.

3.4.3 Analisi dei processi e delle Attività Sensibili

Obiettivo della terza fase è stato analizzare e formalizzare, per ogni processo / Attività Sensibile individuato nelle fasi prima e seconda, le attività principali, le funzioni e i ruoli/responsabilità dei soggetti interni ed esterni coinvolti, gli elementi di controllo esistenti, al fine di verificare in quali aree/settori di attività e secondo quali modalità si potessero astrattamente realizzare le fattispecie di reato di cui al d.lgs. 231/2001.
L'attività che ha caratterizzato la terza fase ha riguardato l'esecuzione di interviste strutturate con i key Officer al fine di raccogliere, per i processi / Attività Sensibili individuati nelle fasi precedenti, le informazioni necessarie a comprendere:

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

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

- acquisire una visione sistematica di tutte le aree/settori di attività della società e del loro effettivo funzionamento;
- verificare l'effettività dei protocolli e delle procedure esistenti, ossia la rispondenza

tra i comportamenti concreti e quelli previsti nei protocolli;

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

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

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

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

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

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

In particolare, il confronto è stato condotto in termini di compatibilità al sistema delle deleghe e dei poteri, al sistema delle procedure, al Codice Etico e di Condotta di Gruppo. Attraverso il confronto operato, è stato possibile desumere le aree di miglioramento del sistema di controllo interno esistente e i relativi meccanismi correttivi. Sulla scorta di quanto emerso, è stato predisposto un piano di attuazione, teso a individuare i requisiti organizzativi caratterizzanti un modello di organizzazione, gestione e controllo conforme a quanto disposto dal D. Lgs. n. 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 aggiornato 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 le 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;
- il ruolo e i compiti dell'Organismo di Vigilanza;
- flussi informativi da e verso l'Organismo di Vigilanza e specifici obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- sistema disciplinare atto a sanzionare la violazione delle disposizioni contenute nel Modello;
- principi generali per l'adozione del piano di formazione e comunicazione ai destinatari;
- criteri di aggiornamento del Modello.

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

3.4.6 Criteri di aggiornamento del Modello

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

In particolare, il Modello potrà essere aggiornato qualora:

- si riscontrino violazioni delle prescrizioni del Modello;
- intervengano modifiche dell'assetto interno o evoluzioni del modello di business della Società;

- siano intervenute modifiche alla normativa di riferimento.

In particolare, al fine di garantire che le variazioni del Modello siano operate con la necessaria tempestività ed efficacia, senza al contempo incorrere in difetti di coordinamento tra i processi operativi, le prescrizioni contenute nel Modello e la diffusione delle stesse, il Consiglio di Amministrazione ha ritenuto di delegare alla Funzione Management Systems il compito di apportare con cadenza periodica, ove risulti necessario, le modifiche al Modello che attengano ad aspetti di carattere descrittivo.
Si precisa che con l'espressione "aspetti descrittivi" si fa riferimento a elementi e informazioni che derivano da atti deliberati dal Consiglio di Amministrazione (come, ad esempio la ridefinizione dell'organigramma) o da funzioni munite di specifica delega (es. nuove procedure).

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

Rimane, in ogni caso, di esclusiva competenza del Consiglio di Amministrazione la delibera di aggiornamenti e/o di adeguamenti del Modello dovuti ai seguenti fattori:
- intervento di modifiche normative in tema di responsabilità amministrativa degli enti;
- identificazione di nuove Attività Sensibili, o variazione di quelle precedentemente identificate, anche eventualmente connesse all'avvio di nuove attività;
- commissione dei reati richiamati dal D. Lgs. n. 231/2001 da parte dei destinatari delle previsioni del Modello o, più in generale, di significative violazioni del Modello;
- riscontro di carenze e/o lacune nelle previsioni del Modello a seguito di verifiche sull'efficacia del medesimo.

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

3.5 Estensione dei principi del Modello di TINEXTA alla Società

La Società, al fine di evitare discrasie negli indirizzi e nei criteri adottati, nel predisporre e/o adeguare il proprio Modello, pur nel rispetto delle esigenze operative e con gli opportuni adattamenti resi necessari dalle proprie dimensioni e dalla realtà in cui opera, si attiene alle Linee Guida e si ispira ai principi del Modello adottato dalla controllante.

4. ORGANISMO DI VIGILANZA

4.1 I requisiti dell'Organismo di Vigilanza

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

L'affidamento dei suddetti compiti ad un organismo dotato di autonomi poteri di iniziativa e controllo, unitamente al corretto ed efficace svolgimento degli stessi, rappresenta, quindi, presupposto indispensabile per l'esonero dalla responsabilità prevista dal Decreto.
I requisiti principali dell'Organismo di Vigilanza (quali richiamati anche dalle Linee Guida di Confindustria) 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, e, 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 collegiale pluripersonale composto da un minimo di 3 (tre) membri ad un massimo di 5 (cinque), tra i quali uno con le funzioni di Presidente, di cui:

- due (o tre se composto da 4 o 5 membri) esterni alla Società, e di cui almeno uno esperto in materie economico-giuridiche e consulenziali,
- uno (o due se composto da 4 o 5 membri) interno alla Società, ma privo di mansioni operative e di interessi che possano confliggere con l'incarico condizionandone l'autonomia di giudizio. Nel caso in cui il membro interno non sia privo di mansioni operative, lo stesso non potrà partecipare alle attività riguardanti il proprio settore

e dovrà astenersi da qualsiasi attività/ decisione in merito.

Il Presidente viene scelto dallo stesso OdV tra i membri esterni, tenendo conto dei requisiti di autonomia, indipendenza e professionalità. Tale soggetto deve coordinare le attività dell'OdV e provvede all'espletamento delle formalità relative alla convocazione, alla fissazione degli argomenti da trattare e allo svolgimento delle riunioni collegiali.
Il CdA di InfoCert nomina i componenti dell'Organismo di Vigilanza, determinandone compensi e durata. Allo scopo di garantire l'efficace e costante attuazione del Modello, nonché la continuità dell'azione di verifica, la durata è equiparata a quella del CdA. In ogni caso ciascun componente rimane in carica fino alla nomina del suo successore. La nomina avviene mediante conferimento di incarico, formalizzato anche contrattualmente, e mediante il quale il soggetto nominato attesta il possesso dei requisiti previsti dalle norme di riferimento. È rimessa al CdA la responsabilità di valutare periodicamente l'adeguatezza dell'OdV, provvedendo con apposite delibere ad apportare tutte le modifiche e le integrazioni ritenute necessarie al fine di assicurarne l'autonomia, l'indipendenza, l'efficacia e la continuità d'azione.

Le cause di ineleggibilità sono direttamente correlate ai requisiti di indipendenza ed autonomia dell'OdV e dei componenti. A tal fine, tenuto conto di quanto stabilito dagli artt. 2399 e 2382 c.c., inerenti rispettivamente le cause di ineleggibilità e decadenza dei sindaci e degli amministratori, nel caso di specie richiamati analogicamente, nonché dal D.lgs. n. 231/2001, dalle Linee guida di Confindustria e dalla giurisprudenza di merito e di legittimità, non possono essere nominati membri dell'OdV:

- il coniuge, i parenti e gli affini entro il quarto grado degli amministratori della Società, gli amministratori, il coniuge, i parenti e gli affini entro il quarto grado degli amministratori delle società da questa controllate, delle società che la controllano e di quelle sottoposte a comune controllo,
- coloro che sono legati alla Società o alle Società da questa controllate o alle società che la controllano o a quelle sottoposte a comune controllo da interessi e altri rapporti di natura personale/ patrimoniale che ne compromettano l'indipendenza,
- coloro che rivestono incarichi esecutivi o delegati nel CdA,
- coloro che intrattengono rapporti d'affari con la società, con le sue controllate o con le controllanti (distributori, fornitori, ecc.),
- coloro che, per qualsiasi ragione, si trovino in situazioni tali da poter generare un conflitto d'interessi, anche potenziale, in grado di comprometterne l'autonomia e l'indipendenza,
- coloro che sono stati condannati ad una pena che ne ha comportato l'interdizione, anche temporanea dai pubblici uffici o l'incapacità ad esercitare ruoli direttivi,
- coloro che sono stati condannati con sentenza, seppur non definitiva, anche se patteggiata ai sensi dell'art. 444 c.p.p., e ancorché con pena sospesa, fatti salvi gli effetti della riabilitazione di cui agli artt. 178 e 179 c.p.

A tal fine, all'atto di nomina, i componenti dell'OdV dovranno autocertificare con dichiarazione sostitutiva di notorietà, di non trovarsi in nessuna delle condizioni di

ineleggibilità suindicate, impegnandosi altresì a comunicare eventuali rilevanti mutazioni rispetto alle dichiarazioni stesse.

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

L'OdV cessa il proprio incarico per naturale scadenza del mandato, decadenza o revoca per giusta causa da parte del CdA, oltre che per rinuncia di tutti i suoi componenti o, per quanto riguarda i componenti nominati in ragione della funzione di cui siano titolari in ambito aziendale, dal venir meno della titolarità di questa.

I componenti dell'OdV decadono automaticamente qualora venga meno anche solo uno dei requisiti di autonomia, indipendenza, professionalità e onorabilità, ed in particolare quando:

- si trovino, per carenza originaria o sopravvenuta, in una delle condizioni di ineleggibilità o incompatibilità di cui al precedente punto,
- sia intervenuta interdizione o inabilitazione, ovvero una grave infermità psico-fisica che renda il componente dell'Organismo inidoneo a svolgere le proprie funzioni di controllo e vigilanza,
- vi sia stata condanna ad una pena che comporti l'interdizione, anche temporanea, dai pubblici uffici o dagli uffici direttivi delle società e delle imprese,
- vengano meno, o se ne scopra successivamente la mancanza ab origine, i requisiti di onorabilità di cui all'art. 109 T.U.B.,
- vengano meno, o se ne scopra successivamente la mancanza ab origine, i requisiti di professionalità,
- dopo la nomina, si accerti che abbiano fatto parte dell'OdV di una società nei cui confronti siano state irrogate, con sentenza definitiva, le sanzioni di cui all'art. 9 del decreto 231,
- venga accertata dagli amministratori una grave negligenza, imperizia o colpa nello svolgimento dei compiti assegnati, nonché, nei casi più gravi, la commissione di reati,
- sia stata emessa una sentenza di condanna, anche non definitiva, a carico dei componenti dell'OdV per aver personalmente commesso uno dei reati previsti dal decreto 231.

Costituiscono ipotesi di giusta causa di revoca dei componenti dell'OdV:

- il grave, e reiterato, inadempimento degli obblighi inerenti all'incarico affidato;
- la mancanza reiterata di buona fede e di diligenza nell'esercizio del proprio incarico;
- la mancata e reiterata collaborazione con gli altri membri dell'OdV;
- l'assenza ingiustificata a più di due adunanze dell'OdV;
- documentata e perdurante inattività del membro dell'OdV sulla base del piano

presentato annualmente al CdA della Società;
- la violazione degli obblighi di riservatezza, così come descritti nel Codice Etico.

Ciascun membro dell'OdV può rinunciare in ogni momento all'incarico affidatogli, dando un preavviso di almeno tre mesi, salvo i casi di comprovata necessità ed urgenza. Al fine di garantire la "continuità d'azione" dell'OdV, la rinuncia all'incarico deve essere comunicata al CdA con qualsiasi mezzo che consenta la certezza della ricezione, in maniera tale che l'organo amministrativo possa al più presto attivarsi per la sostituzione del componente venuto meno evitando danni o ritardi all'attività di vigilanza e controllo.

Le funzioni di un componente dell'OdV possono venire meno anche solo temporaneamente. In particolare, costituiscono cause di sospensione dalla funzione:
- l'applicazione di una misura cautelare personale;
- l'applicazione di una misura di prevenzione previste dall'art. 10, c. 3, della L. n. 575/65, come sostituito dall'art. 3 della L n. 55/90 e successive modificazioni;
- la condanna per un reato diverso da quelli per i quali è prevista la decadenza.

La sospensione viene disposta dal CdA, sentito il Collegio Sindacale e gli altri membri dell'OdV.
In caso di decadenza, revoca, sospensione o rinuncia di uno dei componenti dell'OdV, sarà compito del CdA, sentito il Collegio Sindacale e gli altri membri dell'OdV, provvedere tempestivamente alla sua sostituzione. Nel caso di sospensione, il CdA potrà nominare in via provvisoria dei sostituti, fino all'interruzione della sospensione a carico dei membri permanenti.

All'Organismo di Vigilanza di InfoCert S.p.A. è affidato il compito di:
a) 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;
b) 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;
c) 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;
d) verificare il mantenimento nel tempo dei requisiti di efficienza ed efficacia del Modello;
e) 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;
f) 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;

g) monitorare il periodico aggiornamento del sistema di identificazione, mappatura e classificazione delle Attività Sensibili;
h) 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;
i) 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;
j) promuovere l'attivazione di eventuali procedimenti disciplinari;
k) 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".
l) 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;
m) 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 al Consiglio di Amministrazione e al Collegio Sindacale in merito all'attuazione del Modello;

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

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

All'OdV non competono poteri di gestione o poteri decisionali relativi allo svolgimento delle attività della Società, poteri organizzativi o di modifica della struttura della Società, né poteri sanzionatori. L'OdV, nonché i soggetti dei quali l'Organismo di Vigilanza, a

qualsiasi titolo, si avvale, sono tenuti a rispettare l'obbligo di riservatezza su tutte le informazioni delle quali sono venuti a conoscenza nell'esercizio delle loro funzioni.

Nel contesto delle procedure di formazione del budget, 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, gestione delle segnalazioni whistleblowing ecc.).

4.2 Reporting dell'Organismo di Vigilanza verso gli organi societari

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

- la prima, su base continuativa, direttamente verso il vertice aziendale (Amministratore Delegato) 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.

Per quanto concerne l'attività di reporting semestrale, compiuta dall'Organismo di Vigilanza verso gli organi societari, essa deve avere ad oggetto quanto meno le seguenti informazioni:

a) la sintesi delle attività svolte nel semestre e, in occasione della relazione annuale, il piano delle attività previste per l'anno successivo;
b) eventuali problematiche o criticità che siano scaturite nel corso dell'attività di vigilanza; in particolare, qualora non oggetto di precedenti e apposite segnalazioni:

- le azioni correttive da apportare al fine di assicurare l'efficacia e/o l'effettività del Modello, ivi incluse quelle necessarie a rimediare alle carenze organizzative o procedurali accertate ed idonee ad esporre la Società al pericolo che siano commessi reati rilevanti ai fini del Decreto, inclusa una descrizione delle eventuali nuove attività "sensibili" individuate;
- sempre nel rispetto dei termini e delle modalità indicati nel sistema disciplinare adottato dalla Società ai sensi del Decreto, l'indicazione dei comportamenti accertati e risultati non in linea con il Modello;
- il resoconto delle segnalazioni ricevute, ivi incluso quanto direttamente riscontrato, in ordine a presunte violazioni delle previsioni del presente Modello, del Codice Etico e di Condotta, dei protocolli di prevenzione e delle relative procedure di attuazione, delle policy ESG; nonché le violazioni del diritto dell'Unione Europea

e gli illeciti amministrativi, contabili, civili o penali; e l'esito delle conseguenti verifiche effettuate;
- informativa in merito all'eventuale commissione di reati rilevanti ai fini del Decreto;
- i provvedimenti disciplinari e le sanzioni eventualmente applicate dalla Società, con riferimento alle violazioni delle previsioni del presente Modello, del Codice Etico e di Condotta, dei protocolli di prevenzione e delle relative procedure di attuazione, delle policy ESG; nonché le violazioni del diritto dell'Unione Europea e gli illeciti amministrativi, contabili, civili o penali;
- una valutazione complessiva sul funzionamento e l'efficacia del Modello con eventuali proposte di integrazioni, correzioni o modifiche;
- la segnalazione degli eventuali mutamenti del quadro normativo e/o significative modificazioni dell'assetto interno della Società che richiedono un aggiornamento del Modello;
- il rendiconto delle spese sostenute.

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

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 della Società. 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 gli Organismi di Vigilanza delle società controllate. La convocazione avviene a cura del Presidente dell'Organismo di Vigilanza di Tinexta S.p.A. ed è trasmessa agli interessati via e-mail almeno quindici giorni prima dell'incontro.

4.3 Informativa verso l'Organismo di Vigilanza

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

1) i seguenti *report*, prodotti con periodicità 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, nonché di quelli conferiti tramite affidamento diretto;

- elenco degli incarichi di consulenza sottoscritti con evidenza di quelli conferiti tramite affidamento diretto;
- elenco delle liberalità, contributi, sponsorizzazioni e omaggi nonché delle spese di rappresentanza di entità superiore al "modico valore" qualificato nella documentazione aziendale (beneficiario, importo, data del versamento);
- elenco delle assunzioni, e relativo processo di selezione, con la eventuale indicazione delle assunzioni effettuate extra budget;
- lista delle nuove emissioni delle disposizioni aziendali (modelli, direttive, regolamenti, procedure, organigrammi, deleghe, poteri, etc.) relative alle attività sensibili indicate nel Modello;
- elenco delle cause giudiziarie ed arbitrati in corso.

2) le seguenti informative, prodotte al verificarsi degli eventi di seguito elencati:
- *report* del DPO su eventuali violazioni della sicurezza informatica ("data breach");
- *report* del DPO sulle modalità di trattamento dei dati personali da parte del Titolare, anche con riguardo al profilo delle misure di sicurezza adottate e adeguate al livello di rischio;
- esiti di ispezioni/verifiche da parte di soggetti pubblici (Ispettorato del lavoro, VV.FF., 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 Internal Audit, Management System, Planning & Control o di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili critici rispetto all'osservanza delle norme e previsioni del Modello;
- notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate (ivi compresi i provvedimenti assunti verso i dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- rapporti predisposti dal Dirigente Preposto alla redazione dei documenti contabili societari *ex* L. n. 262/05 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 (anche qualora il rapporto lavorativo non sia stato avviato o si sia concluso) e qualsiasi terza parte devono trasmettere all'Organismo di Vigilanza ogni informazione attinente a presumibili:

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

A tal fine il segnalante deve presentare segnalazioni circostanziate[3] di presunte condotte illecite che siano fondate su elementi di fatto precisi e concordanti[4].

La Società, in conformità a quanto previsto dalla normativa in materia di whistleblowing ha attivato una piattaforma di segnalazione «Comunica Whistleblowing» accessibile dal sito.
Attraverso tale sistema di segnalazioni la Società garantisce, attraverso sistemi crittografati, la riservatezza dell'identità del segnalante e delle informazioni contenute nella segnalazione.
La gestione delle segnalazioni da parte dell'Organismo di Vigilanza si suddivide in quattro fasi:

- Presa in carico;
- Istruttoria;
- Accertamento;

[3] Per segnalazione circostanziata si intende una segnalazione che contenga un grado di dettaglio sufficiente a consentire, almeno astrattamente, alle Funzioni/soggetti coinvolti nella gestione delle segnalazioni, di identificare elementi utili o decisivi ai fini della verifica della fondatezza della segnalazione stessa (ad esempio: tipologia di illecito commesso, periodo di riferimento, cause e finalità dell'illecito, persone/Funzioni aziendali coinvolte, anomalie riscontrate nel sistema di controllo interno, ecc.).
[4] Gli elementi (o indizi) si definiscono precisi quando non sono suscettibili di diverse interpretazioni e concordanti quando più elementi confluiscono necessariamente nella stessa direzione.

- Sanzioni/azioni di miglioramento.

Inoltre, in via residuale, sono mantenute:

- una casella e-mail aperta, a cura dell'Organismo di Vigilanza e pubblicata sul sito internet della Società, per effettuare segnalazioni di rilevanza 231 e per trasmettere i flussi informativi da e verso l'OdV, all'indirizzo OdV231@legalmail.it;
- la posta prioritaria con l'indicazione di "RISERVATO" sulla busta indirizzata a: Organismo di Vigilanza, c/o InfoCert S.p.A. – Via Marco e Marcelliano, 45, 00147 – Roma.

4.4 Raccolta e conservazione delle informazioni

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

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

5. SISTEMA DISCIPLINARE E SANZIONATORIO

5.1 Principi generali

L'efficace attuazione del Modello è assicurata anche dalla previsione e predisposizione, in InfoCert, di un adeguato sistema disciplinare e sanzionatorio per la violazione delle regole di condotta imposte dal citato Modello ai fini della prevenzione dei reati di cui al Decreto, e, in generale, delle procedure interne (cfr. art. 6, comma secondo, lett. e, art. 7, comma quarto, lett. b).
L'applicazione delle sanzioni disciplinari prescinde dall'effettiva commissione di un reato e, quindi, dalla instaurazione e dall'esito di un eventuale procedimento penale.
Le regole di condotta imposte dal Modello sono, infatti, assunte dall'azienda in piena autonomia, al fine del miglior rispetto del precetto normativo che sull'azienda stessa incombe.
Le sanzioni disciplinari potranno quindi essere applicate dalla Società ad ogni violazione del presente Modello e del Codice Etico e di Condotta di Gruppo, indipendentemente dalla commissione di un reato e dallo svolgimento e dall'esito di un processo penale avviato dall'Autorità Giudiziaria.
La violazione delle singole disposizioni del presente Modello e del Codice Etico e di Condotta di Gruppo costituiscono sempre illecito disciplinare.
In ogni caso, l'Organismo di Vigilanza deve essere informato del procedimento di irrogazione delle sanzioni disciplinari o dell'eventuale archiviazione.
La Società cura l'informazione di tutti i soggetti sopra previsti, sin dal sorgere del loro rapporto di lavoro, circa l'esistenza ed il contenuto del presente apparato sanzionatorio.

5.2 Condotte sanzionabili: categorie fondamentali

Sono sanzionabili le azioni poste in essere in violazione del Codice Etico e di Condotta di Gruppo, del Modello e delle procedure operative interne e la mancata ottemperanza ed eventuali indicazioni e prescrizioni provenienti dall'Organismo di Vigilanza.
Le violazioni sanzionabili possono essere suddivise in quattro categorie fondamentali secondo un ordine di gravità crescente:

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

comunque, comportino la possibilità di attribuzione di responsabilità amministrativa in capo alla Società.

A titolo esemplificativo, costituiscono condotte sanzionabili:

- la mancata osservanza di procedure prescritte nel Modello e/o ivi richiamate;
- l'inosservanza di obblighi informativi prescritti nel sistema di controllo;
- l'omessa o non veritiera documentazione delle operazioni in conformità al principio di trasparenza;
- l'omissione di controlli da parte di soggetti responsabili;
- il mancato rispetto non giustificato degli obblighi informativi;
- l'omesso controllo sulla diffusione del Codice Etico e di Condotta 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 alle 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 di una società del Gruppo che siano – a seguito della stipulazione di un accordo contrattuale – distaccati presso una società del Gruppo, tali soggetti sono tenuti al rispetto di quanto previsto dal Codice Etico e di Condotta di Gruppo e dal presente Modello.

5.4 Violazioni del modello e relative sanzioni

La Società ha predisposto, in conformità alla normativa vigente ed al principio di tipicità delle violazioni e delle sanzioni, le regole comportamentali contenute nel Modello e nel Codice Etico e di Condotta di Gruppo, la cui violazione costituisce illecito disciplinare, nonché le sanzioni applicabili, proporzionate alla gravità delle infrazioni.
Si ritiene opportuno rinviare al Codice Etico e di Condotta di Gruppo, nel quale sono riportate le possibili violazioni poste in essere dal dipendente e le corrispondenti sanzioni comminabili.
È fatto salvo il diritto della Società di richiedere il risarcimento del danno derivante dalla violazione del Modello, che sarà commisurato:

1. al livello di autonomia del dipendente;
2. alla gravità delle conseguenze della violazione, ovvero le possibili implicazioni in

materia di D. Lgs. n. 231/01;
3. al livello di intenzionalità del comportamento;
4. all'eventuale presenza di precedenti sanzioni disciplinari irrogate.

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

(i) atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla Segnalazione;
(ii) violazione, da parte dell'organo deputato a ricevere e/o a gestire la Segnalazione, degli obblighi di riservatezza dell'identità del segnalante;
(iii) mancata attivazione, da parte dell'organo deputato a ricevere e/o a gestire la Segnalazione, delle necessarie verifiche volte a valutare la fondatezza dei fatti oggetto di Segnalazione;
(iv) effettuazione, con dolo o colpa grave, di Segnalazioni infondate.

Si provvederà ad applicare nei confronti del soggetto che ha posto in essere anche solo una delle suddette fattispecie le misure disciplinari di cui ai paragrafi seguenti in funzione della relativa posizione aziendale ricoperta.
Il responsabile dell'avvio e dello svolgimento del procedimento disciplinare è la Struttura aziendale competente, la quale deve tenere costantemente informato l'Organismo sull'andamento del procedimento, le giustificazioni addotte, l'esito e qualsiasi altra informazione possa essere di interesse per il citato Organismo.

5.5 Misure nei confronti dei dipendenti

I lavoratori subordinati devono rispettare gli obblighi stabiliti dall'art. 2104 c.c., obblighi dei quali il presente Modello ed il Codice Etico e di Condotta adottato dal Gruppo, rappresentano parte integrante.
Per i dipendenti di livello non dirigenziale, le sanzioni irrogabili, conformemente a quanto previsto dall'art. 7 delle Legge n. 300/1970 (c.d. Statuto dei Lavoratori) ed eventuali normative speciali applicabili, sono quelle previste dalla legge, nonché dall'apparato sanzionatorio dei contratti di lavoro.

In particolare, il richiamato CCNL prevede, a seconda della gravità delle violazioni, i seguenti provvedimenti:

1) richiamo verbale;
2) ammonizione scritta;
3) multa non superiore a tre ore di paga base e contingenza o minimo stipendio e contingenza;
4) sospensione del lavoro e della retribuzione fino a un massimo di tre giorni;
5) sospensione cautelare;
6) licenziamento.

5.6 Misure nei confronti dei dirigenti

In caso di violazione del Modello o del Codice Etico e di Condotta di Gruppo da parte dei dirigenti, la Società provvederà ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto normativamente previsto.
Nel caso in cui la violazione interrompa il rapporto fiduciario tra la Società e il dirigente, la sanzione è quella del licenziamento per giusta causa.

5.7 Misure nei confronti di amministratori e sindaci

In caso di violazione del Modello o del Codice Etico e di Condotta di Gruppo da parte di un membro del Consiglio di Amministrazione, l'Organismo di Vigilanza procede a darne immediata comunicazione all'intero Consiglio di Amministrazione ed al Collegio Sindacale, esprimendo parere in merito alla gravità dell'infrazione. Il Consiglio di Amministrazione, sentito il parere del Collegio Sindacale, è competente ad assumere gli opportuni provvedimenti, sino ad arrivare, nei casi di gravi infrazioni, alla convocazione dell'assemblea dei soci, al fine di esporre a tale organo i fatti accertati e adottare le deliberazioni ritenute necessarie.
Il membro o i membri del Consiglio di Amministrazione della cui infrazione si discute saranno tenuti ad astenersi dalle relative deliberazioni.
Qualora le violazioni siano commesse da un numero di membri del Consiglio di Amministrazione tale da impedire all'Organo in questione di deliberare, l'Organismo di Vigilanza dovrà darne immediata comunicazione al Collegio Sindacale perché si attivi ai sensi di legge, convocando in particolare l'Assemblea dei soci per l'adozione delle misure necessarie.

In caso di violazione del Modello o del Codice Etico e di Condotta di Gruppo da parte di un membro del Collegio Sindacale, l'Organismo di Vigilanza procede a darne immediata comunicazione all'intero Collegio Sindacale e al Consiglio di Amministrazione, esprimendo parere in merito alla gravità dell'infrazione.
Il Collegio, sentito il parere del Consiglio di Amministrazione, provvederà ad assumere gli opportuni provvedimenti, in conformità alla normativa vigente, e nei casi di gravi infrazioni, convocherà l'Assemblea dei soci al fine di esporre a tale organo i fatti accertati e per adottare le deliberazioni ritenute necessarie.
Qualora le violazioni siano commesse da più membri del Collegio Sindacale, l'Organismo di Vigilanza dovrà darne immediata e diretta comunicazione al Consiglio di Amministrazione perché si attivi ai sensi di legge, convocando in particolare l'Assemblea dei soci per l'adozione delle misure necessarie.

5.8 Misure nei confronti degli altri destinatari

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

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

6. COMUNICAZIONE E FORMAZIONE DEL PERSONALE

6.1 Formazione e diffusione del Modello

La Società, al fine di dare efficace attuazione al Modello, assicura una corretta divulgazione dei contenuti e dei principi dello stesso all'interno e all'esterno della propria organizzazione.
Obiettivo della Società è quello di comunicare i contenuti e i principi del Modello anche ai soggetti che, pur non rivestendo la qualifica formale di dipendente, operano – anche occasionalmente – per il conseguimento degli obiettivi della Società in forza di rapporti contrattuali.

La Società, infatti, intende:

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

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

La Società cura l'adozione e l'attuazione di un adeguato livello di formazione mediante idonei strumenti, tra i quali:

- inserimento del Modello (comprensivo di allegati e parti speciali) e del Codice Etico nell'intranet aziendale, nella sezione "Corporate" del sito internet della Società;
- disponibilità del Modello e del Codice Etico per tutto il personale, e distribuzione ovvero invio telematico ai neoassunti di tali documenti al momento del loro inserimento in azienda con firma (di proprio pugno o digitale) attestante l'avvenuta ricezione e l'impegno alla conoscenza e rispetto delle relative prescrizioni;
- corso on-line permanente presso la intranet aziendale sui contenuti del Decreto,

del Modello e del Codice Etico;
- aggiornamento sulle modifiche apportate al Modello o al Codice Etico conseguenti ad intervenute modifiche normative e/o organizzative rilevanti ai fini del Decreto, anche attraverso la revisione del corso on-line disponibile sull'intranet aziendale;
- per il Personale direttivo e con funzioni di rappresentanza dell'Ente incontri con i Responsabili delle U.O. e workshop in aula, con test o questionari finali volti a verificare l'apprendimento e le eventuali criticità delle tematiche trattate;
- per gli altri dipendenti informativa al momento dell'assunzione, corso di formazione realizzato con modalità di corsi in aula con test o questionari finali volti a verificare l'apprendimento e le eventuali criticità delle tematiche trattate ovvero con modalità e-learning attraverso supporto informatico presso l'intranet aziendale ed aggiornato attraverso la collaborazione con l'OdV.

La formazione deve vertere sulla completa conoscenza e comprensione delle seguenti aree:
- il D.Lgs. 231/2001: i principi generali, i reati previsti (anche quelli di cui alla Legge n. 146/2006) e le sanzioni applicabili alla Società;
- i principi di comportamento contenuti nel Modello e nel Codice Etico e di Condotta di Gruppo;
- i poteri dell'Organismo di Vigilanza, nonché gli obblighi informativi nei suoi confronti;
- il sistema disciplinare;
- il sistema di segnalazione degli illeciti (c.d. whistleblowing).

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 una banca dati a cura della Struttura Human Resources.

6.2 Componenti degli organi sociali, dipendenti, dirigenti e quadri

L'Organismo di Vigilanza promuove mediante la predisposizione di appositi piani comunicati al Consiglio di Amministrazione ed implementati dalla Società, le attività di formazione ed informazione del Modello.
La diffusione del Modello e l'informazione del personale in merito al contenuto del D.Lgs. n. 231/2001 e ai suoi obblighi relativamente all'attuazione dello stesso sono costantemente realizzate attraverso i vari strumenti a disposizione della Società.

L’attività di formazione e di informazione riguarda tutto il personale, compreso il personale direttivo e prevede, oltre ad una specifica informativa all’atto dell’assunzione, lo svolgimento di ulteriori attività ritenute necessarie al fine di garantire la corretta applicazione delle disposizioni previste nel D. Lgs. n. 231/2001.
L’adozione del Modello e le sue successive integrazioni o modifiche di rilievo sostanziale sono comunicate a tutti i Dipendenti, i Fornitori, i Collaboratori e gli Organi Sociali.
Ai nuovi assunti è consegnato un set informativo, che contiene il Codice Etico e di Condotta di Gruppo ed il Modello di organizzazione, gestione e controllo in modo da assicurare agli stessi le conoscenze considerate di primaria rilevanza per la società.

6.3 Altri Destinatari

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