

MODELLO
DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
7LAYERS S.R.L.

(ai sensi del Decreto Legislativo 231/2001)

Documento approvato dal Consiglio di Amministrazione di 7Layers S.r.l.
in data 17 dicembre 2021

PARTE GENERALE	5
DEFINIZIONI	5
PREMESSA	7
1. IL DECRETO LEGISLATIVO 231/2001 - SOGGETTI, FATTISPECIE CRIMINOSE E SANZIONI	9
2. ESONERO DA RESPONSABILITÀ.....	10
3. LE LINEE GUIDA PER LA COSTRUZIONE DEI MODELLI	10
4. IL MODELLO DI 7LAYERS	12
5. IL MODELLO DI GOVERNANCE E L'ASSETTO ORGANIZZATIVO DI LAYERS S.R.L.	12
5.1 7Layers S.r.l.	12
5.2 7Layers S.r.l. e il Gruppo di appartenenza	13
6. LA COSTRUZIONE DEL MODELLO.....	14
6.1. Struttura del Modello.....	14
6.2. La funzione del Modello e i principi ispiratori	15
7. I PROCESSI SENSIBILI IN 7LAYERS.....	16
7.1 La mappatura delle aree potenzialmente a rischio-reato	16
7.2 L'analisi del sistema di controllo interno	17
7.3 Il sistema di controllo interno e le modalità di gestione dei rischi	18
8. L'ORGANISMO DI VIGILANZA.....	19
8.1. Identificazione dell'Organismo di Vigilanza	19
8.2. Durata in carica e sostituzione dei membri dell'Organismo di Vigilanza.....	20
8.3. Compiti dell'Organismo di Vigilanza	20
8.4. Attività e <i>reporting</i> dell'Organismo di Vigilanza	21
8.5. <i>Reporting</i> nei confronti dell'Organismo di Vigilanza	22
8.6. Verifiche periodiche	22
8.7. Raccolta e conservazione delle informazioni.....	23
9. INFORMAZIONE E FORMAZIONE DEI DIPENDENTI	23
9.1. Comunicazione	23
9.2. Formazione	23
10. DESTINATARI E CAMPO DI APPLICAZIONE.....	24
11. PROCEDURA DI ADOZIONE DEL MODELLO	25
12. SISTEMA DISCIPLINARE	25
12.1. Principi generali.....	25
12.2. Sanzioni per i lavoratori subordinati cui si applicano i Contratti Collettivi Nazionali di Lavoro relativi alle imprese esercenti commercio, terziario, distribuzione e servizi.....	26
12.4. Misure nei confronti degli Amministratori.....	27
12.5. Misure nei confronti del Sindaco.....	27
12.6. Misure nei confronti dell'Organismo di Vigilanza	28

12.7. Misure nei confronti di Partner	28
13. NORME E STANDARD DI COMPORTAMENTO NELLE RELAZIONI CON DIPENDENTI E CON <i>STAKEHOLDER</i> ESTERNI.....	28

PARTE GENERALE

PARTE GENERALE

DEFINIZIONI

- **"Destinatari"**: i componenti degli organi sociali, coloro che svolgono funzioni di gestione, amministrazione, direzione o controllo della Società, i dirigenti, i dipendenti della Società ed in generale quanti si trovino ad operare sotto la direzione e/o vigilanza delle persone suindicate;
- **"CCNL"**: Contratti Collettivi Nazionali di Lavoro attualmente in vigore ed applicati da 7Layers S.r.l.;
- **"Consulenti"**: coloro che agiscono in nome e/o per conto di 7Layers sulla base di incarichi di consulenza;
- **"D.Lgs. 231/2001"** o **"Decreto"**: il Decreto Legislativo n. 231/2001 e successive modifiche;
- **"7Layers", "7L" o "Società"**: 7Layers S.r.l.;
- **"Gruppo Fastweb"**: l'insieme di società comprendente Fastweb S.p.A., Fastweb Air S.r.l. e 7Layers S.r.l.;
- **"Direttiva Anti-corruzione"**: documento che descrive le misure anticorruzione implementate e adottate da Fastweb S.p.A., applicabili a tutto il Gruppo;
- **"Linee Guida Confindustria"**: le Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001 approvate da Confindustria in data 7 marzo 2002 e successive modifiche ed integrazioni;
- **"Modello"**: il modello di organizzazione, gestione e controllo adottato da 7Layers sulla base delle disposizioni del D.Lgs. 231/2001;
- **"Codice Etico"** il documento adottato da 7Layers S.r.l. in data 30 settembre 2019 e successivamente aggiornato;
- **"Organismo di Vigilanza" o "OdV"**: organismo preposto alla vigilanza sul funzionamento e sull'osservanza del Modello e al relativo aggiornamento;
- **"Data Protection Officer" o "DPO"** : Responsabile della gestione del trattamento di dati personali e della loro protezione all'interno dell'azienda, figura introdotta dal GDPR (General Data Protection Regulation);
- **"P.A."**: la Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio;
- **"Partner" o "Partner Commerciali"**: controparti contrattuali di 7Layers S.r.l., quali ad es. fornitori, subfornitori, appaltatori, subappaltatori, agenti, agenzie, intermediari, rivenditori, consulenti o collaboratori, sia persone

fisiche sia persone giuridiche, con cui la Società addivenga ad una qualunque forma di collaborazione contrattualmente regolata, ove destinati a cooperare con il personale aziendale nell'ambito dei Processi Sensibili;

- **“Processi Sensibili”**: attività di 7Layers nel cui ambito ricorre il rischio di commissione dei Reati;
- **“Reati”**: i reati ai quali si applica la disciplina prevista dal D.Lgs. 231/2001 (il cui elenco può anche essere eventualmente integrato in futuro).

PREMESSA

7Layers S.r.l. ha inteso procedere all'adozione di un proprio Modello di Organizzazione, Gestione e Controllo, in conformità a quanto previsto dalla normativa di cui al D.Lgs. 231/2001, relativa alla disciplina della responsabilità amministrativa delle società per taluni reati.

Il presente Modello è stato approvato dal Consiglio di Amministrazione di 7Layers S.r.l. in data 17 dicembre 2021.

Nella predisposizione del presente Modello, la Società si è ispirata alle Linee Guida adottate da Confindustria in data 7 marzo 2002 e aggiornate da ultimo nel mese di giugno 2021, approvate dal Ministero della Giustizia. Eventuali difformità che si dovessero riscontrare rispetto al contenuto delle Linee Guida non inficerebbero di per sé la validità del Modello in quanto quest'ultimo deve essere adattato alla specifica realtà di 7Layers e quindi ben può discostarsi dalle Linee Guida - che per loro natura hanno carattere generale - per specifiche esigenze di tutela e prevenzione.

Le regole di comportamento contenute nel presente Modello sono coerenti con quelle del Codice Etico adottato da 7Layers S.r.l. in data 30 settembre 2019 e successivamente aggiornato, pur avendo il presente Modello finalità specifiche di ottemperanza al D.Lgs. 231/2001.

Il Modello di 7Layers è composto da:

- a) Parte Generale;
- b) le regole di comportamento e le procedure organizzative già in vigore all'interno di 7Layers e che siano attinenti ai fini del controllo di comportamenti, fatti o atti rilevanti a norma del Decreto, tra i quali:
 - Statuto sociale;
 - Sistema di deleghe interne (poteri delegati dal Consiglio di Amministrazione e poteri delegati in materia di uso della firma);
 - Codice Etico;
 - Procedure aziendali e la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale ed organizzativa di 7Layers;
 - Regolamento aziendale;
 - Contratto Collettivo Nazionale Lavoro per Commercio, Terziario, Distribuzione e Servizi.
- c) le Parti Speciali, concernenti le specifiche categorie di reato rilevanti per 7Layers e la relativa disciplina applicabile.

I documenti menzionati al punto *b)*, pur non essendo stati emanati esplicitamente ai sensi del D.Lgs. 231/2001, mirano a regolamentare lo svolgimento delle attività aziendali da parte dei Destinatari e, pertanto, contribuiscono ad assicurare la prevenzione dei Reati. I principi, le regole e le procedure di cui agli strumenti sopra elencati non vengono riportati dettagliatamente nel presente documento, ma fanno

parte del più ampio sistema di organizzazione e controllo che lo stesso intende integrare.

Inoltre viene estesa a 7Layers la “Direttiva Anti-corrruzione” adottata da Fastweb S.p.A., applicabile a tutto il Gruppo.

1. IL DECRETO LEGISLATIVO 231/2001 - SOGGETTI, FATTISPECIE CRIMINOSE E SANZIONI

1.1 Il regime della responsabilità amministrativa previsto a carico delle persone giuridiche

La responsabilità amministrativa da reato delle società, e degli enti in genere, è stata introdotta dal D.Lgs. 231/2001, che tratta della “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica”, e discende da alcuni reati commessi, nell’interesse o a vantaggio degli enti citati, da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell’ente o di una unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso e, infine, da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

La responsabilità della società è diretta ed autonoma da quella propria della persona fisica che ha commesso il reato.

1.2 I reati

I reati da cui può conseguire la responsabilità amministrativa per l’ente sono espressamente indicati nel Decreto ed in successivi provvedimenti normativi che ne hanno esteso il campo di applicazione e sono ad oggi:

- Reati contro la Pubblica Amministrazione (artt. 24 e 25);
- Delitti informatici e trattamento illecito di dati (art. 24 *bis*);
- Delitti di criminalità organizzata (art. 24 *ter*);
- Falsità in monete, in carte di pubblico credito, in valori di bollo ed in strumenti o segni di riconoscimento (art. 25 *bis*);
- Delitti contro l’industria e il commercio (art. 25 *bis*.1);
- Reati societari e corruzione tra privati (art. 25 *ter*);
- Delitti con finalità di terrorismo o di eversione dell’ordine democratico (art. 25 *quater*);
- Pratiche di mutilazione degli organi genitali femminili (art. 25 *quater*-1);
- Delitti contro la personalità individuale (art. 25 *quinquies*);
- Abusi di mercato (art. 25 *sexies*);
- Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 *septies*);
- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25 *octies*);
- Delitti in materia di violazione del diritto d’autore (art. 25 *novies*);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria (art. 25 *decies*);
- Reati ambientali (art. 25 *undecies*);

- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 *duodecies*);
- Razzismo e xenofobia (art. 25 *terdecies*);
- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25 *quaterdecies*);
- Reati tributari (art. 25 *quinqüesdecies*);
- Reati di contrabbando (art. 25 *sexiesdecies*);
- Reati transnazionali (L. 146/2006).

Lo stesso Decreto, infine, ha introdotto una specifica fattispecie penale, rubricata "Inosservanza delle sanzioni interdittive" (art. 23), anch'essa presupposto della responsabilità amministrativa degli enti.

Per una spiegazione sintetica delle singole fattispecie si rimanda all'Allegato n. 1.

2. ESONERO DA RESPONSABILITÀ

Il Decreto (artt. 6 e 7 D.Lgs. 231/2001) prevede che la società sia esonerata da responsabilità ove dimostri di aver adottato ed efficacemente attuato modelli di organizzazione, gestione e controllo idonei a prevenire la commissione dei reati considerati, ferma restando la responsabilità personale di chi ha commesso il reato.

L'adozione dei modelli non è obbligatoria, ma costituisce presupposto necessario perché possa sussistere l'esonero della società da responsabilità.

Adottando il Modello, la società istituisce un Organismo di Vigilanza con il compito di vigilare sul funzionamento, l'efficacia e osservanza del Modello stesso nonché di curarne l'aggiornamento.

3. LE LINEE GUIDA PER LA COSTRUZIONE DEI MODELLI

La prima Associazione di categoria che ha redatto un documento di indirizzo per la costruzione dei modelli è stata Confindustria che nel marzo del 2002 ha emanato delle Linee Guida, poi parzialmente modificate e da ultimo aggiornate al giugno 2021 (di seguito, anche "Linee Guida")¹.

¹Tutte le versioni delle Linee Guida di Confindustria sono state poi giudicate adeguate dal Ministero di Giustizia (con riferimento alle Linee Guida del 2002, cfr. la "Nota del Ministero della Giustizia" del 4 dicembre 2003; con riferimento agli aggiornamenti del 2004 e del 2008, cfr. la "Nota del Ministero della Giustizia" del 28 giugno 2004 e la "Nota del Ministero della Giustizia" del 2 aprile 2008; con riferimento alle Linee Guida del 23 luglio 2014 cfr. la "Nota del Ministero della Giustizia" del 21 luglio 2014; da ultimo in data 8 giugno 2021 il Ministero della Giustizia ha approvato le Linee Guida aggiornate al giugno 2021).

Le Linee Guida di Confindustria costituiscono, quindi, un punto di partenza per la corretta costruzione di un Modello. Secondo dette Linee Guida, i passi operativi per la realizzazione di un sistema di gestione del rischio possono essere schematizzati secondo i seguenti punti fondamentali:

- **inventariazione degli ambiti aziendali di attività**, attraverso l'individuazione delle aree potenzialmente interessate al rischio, ossia delle aree/settori aziendali nei quali sia astrattamente possibile la realizzazione degli eventi pregiudizievoli previsti dal D.Lgs. 231/2001 (c.d. "mappa delle aree aziendali a rischio");
- **analisi dei rischi potenziali** e delle possibili modalità attuative dei reati, attraverso la c.d. "mappa documentata delle potenziali modalità attuative degli illeciti";
- **valutazione/costruzione/adequamento del sistema di controllo interno**, al fine di prevenire la commissione dei reati *ex* D.Lgs. 231/2001, attraverso la descrizione documentata dei controlli preventivi attivati, con dettaglio delle singole componenti del sistema, nonché degli adeguamenti eventualmente necessari.

Le componenti (cd. "*protocolli*") più rilevanti di un sistema di controllo preventivo individuate da Confindustria con riferimento ai reati dolosi sono:

- Codice Etico (o di comportamento) con riferimento ai reati considerati;
- sistema organizzativo;
- procedure manuali ed informatiche;
- poteri autorizzativi e di firma;
- comunicazione al personale e sua formazione;
- sistemi di controllo integrato.

Con riferimento ai reati colposi (reati in materia di salute e sicurezza sul lavoro ed alcune fattispecie di reati ambientali), le componenti più rilevanti di un sistema di controllo preventivo individuate da Confindustria sono:

- Codice Etico (o di comportamento) con riferimento ai reati considerati;
- struttura organizzativa;
- formazione e addestramento;
- comunicazione e coinvolgimento;
- gestione operativa;
- sistema di monitoraggio della sicurezza.

Le componenti del sistema di controllo devono integrarsi organicamente in un'architettura che rispetti alcuni principi fondamentali:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione/transazione/azione;
- applicazione del principio di separazione delle funzioni, in ragione del quale nessuno può gestire in autonomia un intero processo e può essere

destinatario di poteri illimitati, attraverso la chiara definizione e diffusione dei poteri autorizzativi e di firma in coerenza con le responsabilità organizzative assegnate;

- documentazione dei controlli, anche di supervisione.

Il sistema di controllo deve altresì prevedere l'adozione di principi etici rilevanti relativamente alle fattispecie di reato contemplate dal Decreto, che possono essere documentati in un Codice Etico o comportamentale.

Un adeguato sistema sanzionatorio deve essere definito in relazione alla violazione dei principi etico-comportamentali e più in generale dei protocolli definiti dall'azienda.

Le suddette Linee Guida sono state oggetto di successivi aggiornamenti, la cui esigenza è stata determinata dalla necessità di adeguamento alle modifiche legislative che hanno nel tempo introdotto nel *corpus* del Decreto nuovi reati presupposto.

4. IL MODELLO DI 7LAYERS

7Layers S.r.l., ha ritenuto opportuno adottare il presente Modello con la delibera del Consiglio di Amministrazione sopra menzionata al paragrafo "Premessa" (in conformità al disposto dell'art. 6 comma I, lettera a) del D.Lgs 231 del 2001) ed ha istituito l'Organismo di Vigilanza (di seguito anche solo "l'OdV").

Il Modello sarà sottoposto a periodiche attività di aggiornamento, laddove intervengano cambiamenti organizzativi interni, modifiche alla normativa in tema di responsabilità degli enti, ovvero ciò si renda necessario facendo seguito all'attività di monitoraggio e controllo svolta dall'OdV.

Il Modello è suscettibile di modifiche, aggiornamenti ed integrazioni secondo le medesime formalità con cui è stato approvato.

5. IL MODELLO DI GOVERNANCE E L'ASSETTO ORGANIZZATIVO DI LAYERS S.R.L.

5.1 7Layers S.r.l.

La società 7Layers S.r.l. è stata fondata nel 2012 e rappresenta una tra le aziende in maggiore crescita in ambito di cyber-sicurezza nel panorama europeo. La Società è dislocata in due sedi operative, situate in Montelupo Fiorentino (FI) e Torino ed è specializzata nella progettazione e consulenza tecnologica in materia di

innovazione e sicurezza IT (Cyber Security) a supporto dell'attività di *business* dei propri clienti.

7Layers fornisce soluzioni di sicurezza informatica per le imprese in tutti i settori; l'oggetto sociale della Società prevede:

- la prestazione di servizi di consulenza nel campo IT, del networking e di tutto ciò che riguarda il mondo dell'informatica e di internet;
- il commercio di hardware, l'assistenza tecnica su software e hardware, la commercializzazione e la distribuzione di prodotti informatici;
- l'ideazione, la progettazione, la creazione, la commercializzazione, l'installazione, l'assistenza tecnica e la gestione di basi dati, di sistemi informativi e di comunicazioni di ogni tipo, nonché di sistemi elettronici, effettuate con l'impiego di computer, di software e altri mezzi tecnologici di qualsiasi natura o funzione, nonché l'assunzione e la cessione di licenze, brevetti, know-how e rappresentanze a ciò relative;
- l'esecuzione di corsi di formazione e l'allestimento e coordinamento di conferenze o di programmi di lezioni.

I servizi offerti da 7Layers sul mercato comprendono:

- Sicurezza difensiva: Security Infrastructure, Data Assessment / Gap Analysis, Security Advisor, Network Operations Center (NOC), Security Operations Center (SOC), Incident Response, Threat Intelligence;
- Sicurezza offensiva: Penetration Test Vulnerability Assessment, Dark web intelligence, Cyber Security Education.

I servizi di sicurezza offensiva sono svolti con il supporto di *partner* strategici, con i quali la Società stipula accordi *ad hoc* per integrare l'offerta da proporre ai propri clienti.

7Layers, in fase di post-delivery, può gestire la struttura informatica del cliente tramite strumenti di *monitoring* e gestione "on-premise" e "in-the-cloud". Inoltre, possono essere forniti *assessment* programmati che verifichino in modo continuativo lo stato di sicurezza del cliente.

La struttura di *governance* delle società è caratterizzata dalla presenza del Consiglio di Amministrazione, all'interno del quale sono stati individuati due Amministratori Delegati (CEO) ed un Amministratore con delega alla finanza (CFO), e di un sindaco unico.

5.2 7Layers S.r.l. e il Gruppo di appartenenza

A partire dal settembre 2020 la Società fa parte del Gruppo Fastweb, in seguito all'acquisizione da parte di quest'ultima del 70% del capitale sociale della controllante 7Layers Group S.r.l. e della successiva fusione tra 7Layers S.r.l. e 7Layers Group S.r.l. avvenuta nel 2021.

Non sono stati stipulati accordi tra 7Layers e Fastweb S.p.A. per l'erogazione di servizi tecnici e di *staff*, nell'ottica di promuovere le autonomie gestionali di ciascuna società; mentre sono state definite specifiche *policies* per la vendita di beni/servizi per la sicurezza informatica dei sistemi Fastweb, che prevedono prezzi e marginalità per le prestazioni erogate dalla Società verso Fastweb S.p.A.

6. LA COSTRUZIONE DEL MODELLO

6.1. Struttura del Modello

Il Modello intende uniformare il sistema aziendale di prevenzione e gestione dei rischi alle disposizioni ed alle finalità del D.Lgs. 231/2001.

La redazione del Modello è stata condotta sulla base della versione vigente del D.Lgs. 231/2001, dei principali casi giudiziari accertati, delle opinioni dottrinali, delle *best practices* adottate dalle principali società nonché sulle principali normative anche volontarie che indicano principi guida e *standard* di controllo per un sistema di organizzazione interno.

Il Modello è costituito da una "Parte generale" e da tre "Parti speciali" che descrivono i controlli interni applicati per la riduzione del rischio di commissione dei seguenti reati:

- Reati commessi nei rapporti con la Pubblica Amministrazione (articoli 24 e 25 del D.Lgs. 231/2001);
- Reati informatici e trattamento illecito dei dati (articolo 24 *bis* del D.Lgs. 231/2001);
- Reati di criminalità organizzata (articolo 24 *ter* del D.Lgs. 231/2001);
- Reati contro l'industria ed il commercio (articolo 25 *bis.1* del D.Lgs. 231/2001);
- Reati societari (articolo 25 *ter* del D.Lgs. 231/2001);
- Reati aventi finalità di terrorismo e di eversione dell'ordine democratico (articolo 25 *quater* del D.Lgs. 231/2001);
- Reati contro la personalità individuale (articolo 25 *quinqies* del D.Lgs. 231/2001);
- Reati in tema di tutela della salute e sicurezza sul luogo di lavoro (articolo 25 *septies* del D.Lgs. 231/2001);
- Reati di riciclaggio (articolo 25 *octies* del D.Lgs. 231/2001);
- Reati in materia di violazione del diritto di autore (articolo 25 *novies* del D.Lgs. 231/2001);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 *decies*);

- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (articolo 25 *duodecies* del D.Lgs. 231/2001);
- Reati tributari (articolo 25 *quinquiesdecies* del D.Lgs. 231/2001);
- Reati transnazionali (articoli 3 e 10 della L. 16 marzo 2006, n. 146).

Non è stato considerato applicabile il rischio di commissione dei reati di falsità in monete, in carte di pubblico credito, e in valori di bollo ed in strumenti o segni di riconoscimento (articolo 25 *bis* del Decreto), di mutilazione degli organi genitali femminili (art. 25 *quater*.1 del Decreto), di associazione per delinquere finalizzata al traffico di organi prelevati da persona vivente (artt. 416, comma 4, c.p. e 601 *bis* c.p.), dei reati ambientali (art. 25 *undecies* del Decreto), dei reati di razzismo e xenofobia (art. 25 *terdecies* del Decreto), dei reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25 *quaterdecies* del Decreto 231/2001) e di contrabbando (art. 25 *sexiesdecies* del Decreto), trattandosi di condotte che non potrebbero essere compiute nell'ambito delle attività aziendali nell'interesse e/o a vantaggio della Società.

Non è stato ritenuto applicabile il rischio di commissione del reato di frode in agricoltura previsto dall'art. 24 del Decreto, in quanto l'oggetto sociale e le attività aziendali non possono presentare occasioni di realizzazione delle condotte punite da tale fattispecie.

Per la completa associazione dei rischi-reato rispetto ai processi/attività aziendali si veda l'All. n. 2 al Modello.

6.2. La funzione del Modello e i principi ispiratori

Lo scopo del Modello è la predisposizione di un sistema strutturato ed organico di procedure ed attività di controllo (preventive ed *ex post*) che abbia come obiettivo la minimizzazione del rischio di commissione dei reati.

I principi e le regole contenuti nel Modello intendono far acquisire ai "soggetti apicali", quali a titolo esemplificativo i componenti degli organi sociali, i direttori ed i responsabili di funzione ed ai "soggetti sottoposti o subordinati", quali a titolo esemplificativo i dipendenti, i *partner* a vario titolo che operano in nome e/o per conto e/o nell'interesse di 7layers, e la cui attività potrebbe degenerare nella commissione di reati, la piena consapevolezza che determinati comportamenti costituiscono reato, la cui commissione è totalmente inaccettabile, fermamente condannata da 7Layers e contraria agli interessi di quest'ultima anche qualora, apparentemente, la stessa potesse trarne vantaggio. A questo va aggiunta l'ulteriore consapevolezza che la commissione del reato comporterà, oltre alle sanzioni previste dalla legge, anche sanzioni disciplinari interne.

Sotto un altro profilo, 7Layers, grazie ad un costante monitoraggio dell'attività aziendale ed alla possibilità di attivarsi tempestivamente, si pone in condizione di

prevenire la commissione dei Reati e comunque, se del caso, di irrogare agli autori degli stessi le sanzioni che si renderanno opportune. A tal fine sono fondamentali i compiti affidati all'Organismo di Vigilanza, descritti nel presente Modello.

7. I PROCESSI SENSIBILI IN 7LAYERS

La mappatura aggiornata delle attività e dei rischi, volta a valutare l'aderenza del Modello alla realtà organizzativa ed operativa della Società, ha portato alla individuazione dei Processi Sensibili; tale attività è stata effettuata attraverso lo svolgimento di un processo articolato nelle seguenti fasi:

1. **l'identificazione delle fattispecie di reato** contemplate dal Decreto astrattamente applicabili e rilevanti per 7Layers;
2. **la mappatura delle aree aziendali a rischio**, con indicazione delle relative attività sensibili;
3. **la definizione delle potenziali modalità di realizzazione dei reati** astrattamente applicabili e rilevanti per 7Layers;
4. **l'identificazione**, per ciascuna area a rischio, **dell'adeguatezza dei controlli aziendali esistenti**, comprendente anche l'analisi delle procedure in essere,
5. **l'identificazione dei punti di miglioramento** nel sistema di controllo interno e delle relative azioni correttive da sviluppare (*gap analysis*), nonché la definizione di un piano per la loro risoluzione;
6. **l'adeguamento del sistema di controllo interno** al fine di ridurre ad un livello accettabile i rischi identificati.

7.1 La mappatura delle aree potenzialmente a rischio-reato

L'individuazione delle aree a rischio ha rappresentato un'attività fondamentale per la costruzione del Modello della Società.

Tale attività è stata effettuata tenendo in considerazione ed analizzando il contesto della Società, sia sotto il profilo della struttura organizzativa sia dell'operatività, per evidenziare in quali aree/settori di attività e secondo quali modalità potrebbero verificarsi eventi pregiudizievoli per i reati contemplati dal Decreto.

In particolare, dall'analisi della struttura organizzativa e dell'operatività della Società è stato possibile:

- a) identificare le **fattispecie di reato** astrattamente applicabili e rilevanti per la Società stessa;

- b) effettuare **una ricognizione delle aree aziendali a rischio** nell'ambito delle quali potrebbero essere astrattamente commessi (o tentati), autonomamente o in concorso con terzi, i reati previsti dal Decreto.

Come risultato di tale lavoro, è stato inoltre redatto un elenco completo dei processi "sensibili" e, nell'ambito di questi, le aree/attività rispetto cui è connesso - direttamente o indirettamente - il rischio potenziale di commissione dei reati, nonché i relativi ruoli aziendali interessati.

Appare opportuno rilevare che nello svolgimento delle attività di mappatura delle aree a rischio, in conformità a quanto stabilito dalle Linee Guida di Confindustria e seguendo gli orientamenti giurisprudenziali, l'analisi è stata condotta anche chiedendo informazioni circa eventuali episodi o situazioni a rischio-reato che hanno interessato la vita della società (c.d. "analisi storica").

Con riferimento ai processi ipoteticamente a rischio di commissione dei reati contemplati dal Decreto si rinvia alle singole Parti Speciali del Modello.

7.2 L'analisi del sistema di controllo interno

A seguito della mappatura dei processi aziendali a rischio e dell'identificazione delle potenziali modalità di attuazione dei reati, sono state condotte interviste finalizzate all'identificazione dei principali fattori di rischio che potrebbero favorire la commissione dei reati potenzialmente rilevanti per la Società. In seguito è stato analizzato il sistema di controllo interno presente al fine di verificarne l'adeguatezza preventiva.

Si è quindi provveduto alla rilevazione e all'analisi dei controlli aziendali esistenti - c.d. "*As-is analysis*" - e alla successiva identificazione dei punti di miglioramento, con la formulazione di suggerimenti e dei relativi piani di azione - c.d. "*Gap analysis*".

L'analisi del sistema di controllo interno è stata effettuata per verificare in particolare:

- l'esistenza di regole comportamentali di carattere generale a presidio delle attività svolte;
- l'esistenza e l'adeguatezza delle regole e delle procedure esistenti per la regolamentazione delle attività aziendali ed il conseguente rispetto dei principi di tracciabilità degli atti, di oggettivazione del processo decisionale e previsione di adeguati presidi di controllo;
- l'effettiva e concreta applicazione del principio generale di separazione dei compiti;
- l'esistenza di livelli autorizzativi a garanzia di un adeguato controllo del processo decisionale;
- l'esistenza di specifiche attività di controllo e di monitoraggio sulle attività "critiche" in relazione al Decreto.

L'analisi e la valutazione del sistema di controllo interno sono state espressamente svolte in ottemperanza a quanto previsto dal Decreto ed è stata predisposta una descrizione dei principi di controllo preventivi esistenti all'interno della società tenendo in specifica considerazione gli *standard* di controllo suggeriti dalle Linee Guida di Confindustria.

7.3 Il sistema di controllo interno e le modalità di gestione dei rischi

Alla luce della mappatura delle attività sensibili, dell'identificazione dei rischi e dell'analisi del sistema di controllo interno, per ciascuna attività aziendale sono stati valutati i "rischi" e descritti gli elementi qualificanti del sistema di controllo interno proprio della Società, le regole comportamentali e le attività di controllo e monitoraggio svolte.

Per le attività aziendali che non risultano espressamente citate nel presente Modello, si è ritenuto strumento idoneo alla prevenzione del rischio il Codice Etico e la sua effettiva applicazione, non risultando evidenze circa la necessità di implementazione di ulteriori sistemi di controllo in considerazione del livello remoto di rischio rappresentato da tali attività.

L'analisi del sistema di controllo interno di 7Layers è stata condotta per verificare che lo stesso sia disegnato per rispettare i seguenti principi di controllo:

- ***Esistenza di procedure/linee guida formalizzate:*** esistenza di specifici documenti volti a disciplinare principi di comportamento e modalità operative per lo svolgimento dell'attività, caratterizzati da una chiara ed esaustiva definizione di ruoli e responsabilità e da un'appropriatezza delle modalità previste per l'archiviazione della documentazione rilevante.
- ***Tracciabilità e verificabilità ex-post delle transazioni tramite adeguati supporti documentali/informatici:*** verificabilità, documentabilità, coerenza e congruenza di operazioni, transazioni e azioni, al fine di garantire un adeguato supporto documentale che consenta di poter effettuare specifici controlli.
- ***Separazione dei compiti:*** l'esistenza di una preventiva ed equilibrata distribuzione delle responsabilità e previsione di adeguati livelli autorizzativi anche all'interno di una stessa unità organizzativa, idonei ad evitare commistione di ruoli potenzialmente incompatibili o eccessive concentrazioni di responsabilità e poteri in capo a singoli soggetti.
- ***Esistenza di un sistema di deleghe coerente con le responsabilità organizzative assegnate:*** l'attribuzione di poteri esecutivi, autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali assegnate nell'ambito dell'attività descritta, oltre che chiaramente definiti e conosciuti all'interno della Società.

8. L'ORGANISMO DI VIGILANZA

8.1. Identificazione dell'Organismo di Vigilanza

L'OdV è individuato in un organismo collegiale composto da due componenti esterni ed è incaricato, in ottemperanza a quanto previsto dal Decreto (art. 6, lettera b), a vigilare sull'efficacia, sul funzionamento e sull'osservanza del Modello e a curarne l'aggiornamento.

Tale organismo è caratterizzato da tutti i requisiti indicati dalla Linee Guida di Confindustria ed in particolare:

- la professionalità, in quanto l'OdV presenta competenze multidisciplinari relative ai temi della *governance* societaria e del controllo interno: in particolare i componenti presentano una conoscenza approfondita ed una consolidata esperienza in materia penalistica sul tema della criminalità di impresa, nelle attività ispettive, nelle tecniche di analisi e nella valutazione dei rischi;
- la continuità di azione, in quanto l'OdV svolge in modo continuativo e sistematico le attività necessarie per la vigilanza sull'applicazione ed il rispetto del Modello, utilizzando i poteri d'indagine a questo affidati;
- l'autonomia e l'indipendenza, in quanto tale organismo non presenta riporti gerarchici a ruoli aziendali che svolgono attività operative. Inoltre ciascun componente dell'OdV presenta i caratteri dell'autonomia e dell'obiettività di giudizio, in quanto nessuno svolge incarichi operativi, né assume decisioni riferibili alle attività operative della Società.

Sempre al fine di garantire il maggior grado di indipendenza possibile, nel contesto di formazione del *budget* aziendale, il Consiglio di Amministrazione approva una dotazione adeguata di risorse finanziarie, proposta dall'Organismo di Vigilanza stesso, della quale quest'ultimo potrà disporre per ogni esigenza necessaria al corretto svolgimento dei compiti (es. consulenze specialistiche, trasferte, ecc.).

Inoltre la nomina quale componente dell'Organismo di Vigilanza è condizionata all'assenza dei motivi di ineleggibilità, quali:

- l'esistenza di relazioni di parentela, coniugio o affinità entro il IV grado con componenti del Consiglio di Amministrazione titolari di deleghe esecutive o con il sindaco unico della Società;
- la titolarità di conflitti di interesse con la Società tali da pregiudicare l'indipendenza richiesta dal ruolo e dai compiti propri dell'Organismo di Vigilanza;

- la titolarità, diretta o indiretta, di partecipazioni azionarie di entità tale da permettere di esercitare una notevole influenza sulla Società;
- l’aver svolto un rapporto di pubblico impiego presso amministrazioni centrali o locali nei tre anni precedenti alla nomina quale membro dell’Organismo di Vigilanza ovvero all’instaurazione del rapporto di consulenza/collaborazione con lo stesso Organismo;
- l’aver riportato una sentenza di condanna, anche non passata in giudicato, ovvero sentenza di applicazione della pena su richiesta (il c.d. patteggiamento), in Italia o all’estero, per delitti dolosi richiamati dal D.Lgs. 231/2001 od altri delitti comunque incidenti sulla moralità professionale;
- l’aver riportato una sentenza di condanna, anche non passata in giudicato, ovvero con provvedimento che comunque ne accerti la responsabilità, a una pena che importa l’interdizione, anche temporanea, dai pubblici uffici, ovvero l’interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

Laddove alcuno dei sopra richiamati motivi di ineleggibilità dovesse configurarsi in capo ad un soggetto già nominato, opererà una decadenza automatica.

Il Consiglio di Amministrazione può disporre con adeguata motivazione e sentito sindaco unico la revoca del mandato esclusivamente nel caso di grave inadempimento dei compiti affidati ai componenti dell’OdV.

Il Consiglio di Amministrazione stabilisce il compenso per i componenti dell’OdV.

8.2. Durata in carica e sostituzione dei membri dell’Organismo di Vigilanza

La durata in carica dei componenti dell’Organismo deriva dalla delibera di nomina adottata dal Consiglio di Amministrazione.

In caso di rinuncia, sopravvenuta incapacità o decadenza di un membro dell’Organismo, quest’ultimo ne darà comunicazione tempestiva al Consiglio di Amministrazione il quale provvederà senza indugio alla sua sostituzione. È fatto obbligo a ciascun membro dell’OdV di comunicare tempestivamente al Consiglio di Amministrazione il verificarsi di una delle ipotesi dalle quali derivi la necessità di sostituire un membro dell’OdV.

8.3. Compiti dell’Organismo di Vigilanza

All’OdV è affidato il compito di vigilare:

1. sull’effettività e adeguatezza del Modello, in relazione alla struttura aziendale, in funzione dell’effettiva capacità di prevenire la commissione dei reati di cui al D.Lgs. 231/2001;
2. sull’osservanza del Modello da parte dei Destinatari;

3. sull'aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni, quali esempio includono significative modifiche dell'assetto interno della Società e/o delle modalità di svolgimento delle attività dell'azienda e modifiche normative.

Su un piano più specificamente operativo all'OdV sono affidati i seguenti compiti:

1. attivare le procedure di controllo previste dal Modello, restando precisato che in ogni caso le attività di controllo sono demandate alla responsabilità primaria del *management* operativo e sono considerate parte integrante di ogni processo aziendale ("controllo di linea");
2. effettuare ricognizioni dell'attività aziendale ai fini dell'aggiornamento della mappatura delle aree di attività a rischio nell'ambito del contesto aziendale;
3. coordinarsi con le altre funzioni aziendali per il monitoraggio delle attività nelle aree a rischio prevedendo lo svolgimento periodico di controlli di routine e di controlli a sorpresa nei confronti delle attività aziendali sensibili;
4. verificare le esigenze di aggiornamento del Modello;
5. effettuare verifiche periodiche su operazioni od atti specifici posti in essere nelle aree di attività a rischio;
6. raccogliere, elaborare e conservare le informazioni rilevanti in funzione del rispetto del Modello, nonché condividere con i responsabili interni la lista delle informazioni che devono essere obbligatoriamente trasmesse all'OdV o tenute a sua disposizione;
7. controllare l'effettiva presenza e la regolare tenuta ed efficacia della documentazione richiesta in relazione a quanto previsto nel Modello per le diverse tipologie di reato;
8. riferire periodicamente agli organi sociali di 7Layers così come meglio specificato al paragrafo 8.4 in merito all'attuazione delle politiche aziendali a supporto dell'attività *ex* D.Lgs. 231/2001.

Il sistema di controllo a presidio di ogni processo sensibile ai sensi del Decreto viene verificato dall'OdV sulla base dei principi di controllo enunciati al paragrafo 7.3.

Nell'ambito dell'attività di coordinamento dell'applicazione del Modello da parte delle società del Gruppo Fastweb, l'OdV di 7Layers si coordina con gli OdV delle società del Gruppo, ai fini della realizzazione di un coerente sistema di controllo.

8.4. Attività e *reporting* dell'Organismo di Vigilanza

L'OdV ha due linee di *reporting*:

- la prima, su base continuativa, verso gli Amministratori Delegati;
- la seconda, almeno su base annuale, verso il Consiglio di Amministrazione e il sindaco unico.

L'OdV, nello svolgimento della propria attività, effettua incontri periodici con gli organi sociali di gestione e di controllo: degli incontri viene redatto verbale e copia dei verbali è custodita dall'OdV e dagli organismi interessati.

8.5. Reporting nei confronti dell'Organismo di Vigilanza

I dipendenti e gli amministratori di 7Layers hanno l'obbligo di riferire all'Organismo di Vigilanza ogni notizia rilevante relativa all'applicazione, all'interpretazione ed alla violazione del Modello che possa portare alla commissione di reati o relativa al tentativo o alla commissione di reati della quale dovessero venire a conoscenza.

La tipologia e la periodicità delle informazioni da inviare all'Organismo di Vigilanza sono condivise dall'Organismo stesso con i rispettivi responsabili interni dei Processi Sensibili, che si attengono alle modalità ed alle tempistiche concordate.

Le comunicazioni possono essere effettuate utilizzando l'indirizzo *e-mail* dell'Organismo di Vigilanza (organismo.vigilanza@7layers.it). L'OdV non è tenuto a prendere in considerazione le segnalazioni anonime che appaiano ad un primo esame irrilevanti, destituite di fondamento o non circostanziate.

L'omessa comunicazione di informazioni rilevanti potrà essere sanzionata secondo quanto previsto dal presente Modello.

Oltre alle segnalazioni indicate, con riferimento ai reati sono trasmesse all'OdV le informazioni concernenti:

- i provvedimenti e/o le notizie aventi ad oggetto l'esistenza di un procedimento penale, anche nei confronti di ignoti, relativo a fatti di interesse per la Società;
- le richieste di assistenza legale inoltrate alla Società dal personale in caso di avvio di procedimenti penali o civili nei loro confronti;
- le segnalazioni predisposte dai responsabili delle funzioni aziendali nell'ambito della loro attività di controllo dalle quali possano emergere fatti che presentino profili rilevanti ai fini del rispetto del Modello.

L'indirizzo *e-mail* dell'Organismo di Vigilanza è utilizzato per la trasmissione delle segnalazioni ai sensi dell'art. 6, comma 2-*bis*, D.Lgs. 231/2001 (cd. "whistleblowing"), aventi ad oggetto condotte illecite rilevanti ai sensi del Decreto o la violazione del Modello di Organizzazione, Gestione e Controllo, di procedure e regole interne, nonché di fatti che possano far ipotizzare la commissione dei reati previsti dal D.Lgs. 231/2001.

Le segnalazioni devono essere circostanziate e fondate su elementi di fatto precisi e concordanti e devono avere ad oggetto notizie o comportamenti conosciuti in ragione delle funzioni ricoperte o delle attività aziendali svolte.

8.6. Verifiche periodiche

Le verifiche sul Modello sono svolte periodicamente effettuando specifici approfondimenti, analisi e controlli, sia di routine che a sorpresa, sulle procedure

esistenti, sugli atti societari e sui contratti di maggior rilevanza nelle aree di attività a rischio anche a richiesta delle funzioni competenti.

8.7. Raccolta e conservazione delle informazioni

Ogni informazione, segnalazione, *report* previsto nel presente Modello è conservato dall'Organismo di Vigilanza in un apposito *database* (informatico o cartaceo) per un periodo di almeno 5 anni.

Le informazioni contenute nel *database* e nella *mailbox* dedicata sono consultabili esclusivamente dai membri dell'OdV e da persone dallo stesso autorizzate.

Essendo la migliore attuazione del Modello un obiettivo primario della Società, tutti sono tenuti a collaborare con l'OdV rispettando le scadenze previste e fornendo ogni eventuale suggerimento utile in termini di miglioramento dell'efficacia del Modello per il conseguimento del suo scopo.

Le segnalazioni ricevute alla casella *e-mail* dell'OdV ai sensi dell'art. 6, comma 2-*bis*, D.Lgs. 231/2001 (cd. "whistleblowing") come suindicato, sono sottoposte al regime di riservatezza previsto per la documentazione cui hanno accesso l'Organismo di Vigilanza ed eventuali soggetti da questo autorizzati.

9. INFORMAZIONE E FORMAZIONE DEI DIPENDENTI

9.1. Comunicazione

Ai fini dell'efficacia del presente Modello 7Layers assicura, sia alle risorse già presenti all'interno dell'organizzazione aziendale sia a quelle che vi saranno inserite, una corretta conoscenza delle regole di condotta ivi contenute in relazione al diverso livello di coinvolgimento delle risorse medesime nei processi ed attività sensibili.

9.2. Formazione

Il sistema di formazione è realizzato dalle strutture aziendali competenti, che informano l'Organismo di Vigilanza in merito alle attività svolte, ed è finalizzato a consentire ai diversi destinatari la piena consapevolezza delle disposizioni aziendali che sono tenuti a rispettare.

L'attività di formazione, finalizzata a diffondere la conoscenza della normativa di cui al D.Lgs. 231/2001 e successive modifiche, è differenziata per una maggiore efficacia nei contenuti e nelle modalità di attuazione in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui questi operano, dello svolgimento da parte degli stessi di funzioni di rappresentanza della Società e dell'attribuzione di eventuali poteri.

Tutti i programmi di formazione hanno un contenuto minimo comune consistente nell'illustrazione dei principi del D.Lgs. 231/2001, degli elementi costitutivi il Modello, delle singole fattispecie di reato previste dal D.Lgs. 231/2001 e dei comportamenti considerati sensibili in relazione al compimento dei sopracitati reati.

In aggiunta a questa matrice comune, ogni programma di formazione sarà modulato al fine di fornire ai suoi fruitori gli strumenti necessari per il pieno rispetto del dettato del Decreto in relazione all'ambito di operatività e alle mansioni dei soggetti destinatari del programma stesso.

In particolare, a tutti i neoassunti viene consegnata copia dei regolamenti aziendali, del Codice Etico e del Modello 231 e viene richiesto di partecipare alle iniziative informative e formative in aula o in modalità e-learning.

La formazione viene erogata e programmata con il supporto Payroll and General Affairs e Legal&Back Office ed in ogni caso a seguito di modifiche normative al regime della responsabilità degli enti e/o a seguito di aggiornamenti rilevanti dei contenuti del presente Modello.

La partecipazione ai programmi di formazione sopra descritti è obbligatoria e il controllo circa l'effettiva frequenza è demandato all'Organismo di Vigilanza.

10.DESTINATARI E CAMPO DI APPLICAZIONE

Il Modello comprende tutti i processi ed attività svolti dalla Società ed i Destinatari sono individuati nei componenti degli organi sociali, in coloro che svolgono funzioni di gestione, amministrazione, direzione o controllo della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale e nei dipendenti della Società ed in generale in quanti si trovino ad operare sotto la direzione e/o vigilanza delle persone suindicate (tutti detti collettivamente "i Destinatari").

I principi e gli *standard* di controllo contenuti nel Modello si applicano altresì, nei limiti del rapporto contrattuale 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: tali soggetti per effetto di apposite clausole contrattuali si impegnano a tenere, nell'ambito dei rapporti istituiti con la Società, comportamenti corretti e rispettosi delle disposizioni normative vigenti e comunque idonei a prevenire la commissione, anche tentata, dei reati in relazione ai quali si applicano le sanzioni previste nel Decreto.

11. PROCEDURA DI ADOZIONE DEL MODELLO

Essendo il Modello un “atto di emanazione dell’organo dirigente”, in conformità con la disposizione di cui all’articolo 6, comma 1, lettera *a*) del Decreto, le modifiche ed integrazioni sono rimesse alla competenza del Consiglio di Amministrazione di 7Layers o degli Amministratori Delegati, salvo successiva ratifica da parte dello stesso Consiglio in quanto depositario del potere originario di disporre in relazione al Modello.

Le modifiche e/o le integrazioni al Modello che non presuppongono la necessità di attività di *risk assessment* possono essere promosse dall’Organismo di Vigilanza della Società, che ne darà successiva informazione agli Amministratori Delegati, il quale ne disporranno l’approvazione in attesa della ratifica da parte del Consiglio di Amministrazione.

12. SISTEMA DISCIPLINARE

12.1. Principi generali

L’effettività del Modello è legata anche all’adeguatezza del sistema disciplinare e sanzionatorio, che presiede all’effettivo rispetto delle regole di condotta e, in generale, delle procedure e dei regolamenti interni.

L’applicazione di sanzioni disciplinari per violazione delle regole di condotta ed inosservanza delle disposizioni aziendali è indipendente dal giudizio penale e dal suo esito, in quanto tali normative sono assunte dalla Società in piena autonomia a prescindere dal carattere di illecito penale che la condotta possa configurare.

La sanzione è commisurata alla gravità dell’infrazione ed alla eventuale reiterazione della stessa; della recidività si tiene conto anche ai fini della comminazione della sanzione consistente nel licenziamento.

Un’errata interpretazione dei principi e delle regole stabiliti dal Modello da parte del soggetto sottoposto a procedimento può costituire esimente soltanto nei casi di comportamenti tenuti in buona fede, in cui i vincoli posti dal Modello dovessero eccedere i limiti di approfondimento richiesti ad una persona di buona diligenza con riferimento alla specifica mansione svolta.

All’OdV viene data comunicazione dell’apertura di ogni procedimento disciplinare e di ogni provvedimento di archiviazione e di sanzione inerente i procedimenti di cui al presente capitolo. Nessun provvedimento disciplinare per violazione delle disposizioni del Modello nei confronti di qualsivoglia soggetto può essere adottato senza la preventiva consultazione dell’OdV.

Al fine di promuovere l'efficacia del canale *whistleblowing*, in conformità a quanto previsto dalle norme e dal Codice Etico della Società, è sancito il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi che siano collegati, direttamente o indirettamente, alla segnalazione stessa, nonché sanzioni nei confronti di chi viola le misure di tutela del segnalante.

7Layers inoltre intende favorire il sistema di *whistleblowing* ed evitare strumentalizzazioni dello stesso che ne minerebbero la credibilità: a questo fine sono previste sanzioni disciplinari per chi effettuasse con dolo o colpa grave segnalazioni che si rivelano infondate.

12.2. Sanzioni per i lavoratori subordinati cui si applicano i Contratti Collettivi Nazionali di Lavoro relativi alle imprese esercenti commercio, terziario, distribuzione e servizi

Ai lavoratori subordinati si applicano le sanzioni previste nei rispettivi CCNL di categoria, nel rispetto delle procedure previste dall'articolo 7 dello Statuto dei lavoratori.

In applicazione delle norme relative alla disciplina del lavoro contenute nei vigenti CCNL, si prevede che:

1. incorre nei provvedimenti di ammonizione verbale, ammonizione scritta, multa (non superiore a 4 ore della retribuzione base), sospensione dal lavoro e dalla retribuzione (per un periodo non superiore a 10 giorni di effettivo lavoro) il lavoratore che violi le procedure interne previste dal Modello (ad esempio, che non osservi le procedure prescritte, ometta di dare comunicazione all'OdV delle informazioni prescritte, ometta di svolgere controlli, ecc.) o comunque adottati, nello svolgimento di attività nell'ambito di Processi Sensibili, un comportamento non conforme alle prescrizioni del Modello; ai medesimi provvedimenti e al licenziamento per giusta causa sarà sottoposto colui che viola le disposizioni previste a tutela del segnalante e la graduazione della sanzione da applicare sarà attribuita sulla base della gravità della condotta finalizzata a ledere la tutela del segnalante;
2. incorre nel provvedimento di licenziamento disciplinare (ai sensi dell'art. 48 del CCNL applicabile) il lavoratore che, nell'espletamento dei Processi Sensibili: a) compia atti non conformi alle prescrizioni del Modello e diretti in modo univoco al compimento di un reato sanzionato dal D.Lgs. 231/2001, ravvisandosi in tale comportamento un'infrazione alla disciplina e ai doveri d'ufficio così grave da non consentire la prosecuzione nemmeno provvisoria del rapporto di lavoro, o, b) abbia riportato condanna passata in giudicato per uno dei reati. Ad analoga sanzione è sottoposto il lavoratore che compia atti di ritorsione o discriminatori, diretti o indiretti, nei confronti di chi abbia effettuato segnalazioni mediante i canali predisposti per il *whistleblowing* per motivi che siano collegati, direttamente o indirettamente, alla segnalazione stessa;

3. incorre nel provvedimento di licenziamento disciplinare (ai sensi dell'art. 48 del CCNL applicabile) il lavoratore che effettui con dolo o colpa grave segnalazioni mediante i canali a ciò predisposti.

Prima dell'adozione di qualsiasi provvedimento disciplinare nei confronti del lavoratore a questi sarà contestato l'addebito e lo stesso sarà sentito a sua difesa. Ad eccezione del richiamo verbale, tutte le contestazioni avvengono per iscritto e i provvedimenti disciplinari non potranno essere applicati prima che siano trascorsi 5 giorni, nel corso dei quali il lavoratore potrà presentare le sue giustificazioni.

L'adozione del provvedimento è motivata e comunicata per iscritto al destinatario.

La contestazione delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni rientrano, nei limiti della competenza, nelle attribuzioni dei soggetti ai quali vengono dal vertice aziendale conferiti i relativi poteri.

12.4. Misure nei confronti degli Amministratori

In caso di violazione del Modello da parte di taluno dei membri del Consiglio di Amministrazione, l'OdV ne darà immediata informazione al Consiglio di Amministrazione ed al sindaco unico, i quali adotteranno i provvedimenti del caso nell'ambito delle rispettive attribuzioni, ivi compresa l'eventuale convocazione dell'assemblea dei soci con l'eventuale proposta di revoca dalla carica. Le relative comunicazioni saranno indirizzate direttamente a tutti i componenti del Consiglio di Amministrazione ed al sindaco unico.

Salva ogni altra azione a tutela di 7Layers, è passibile di revoca del mandato l'amministratore che compia atti di ritorsione o discriminatori, diretti o indiretti, nei confronti di chi abbia effettuato segnalazioni mediante i canali *whistleblowing* per motivi che siano collegati, direttamente o indirettamente, alla segnalazione stessa. Analoga sanzione è prevista per l'amministratore che effettui con dolo o colpa grave segnalazioni che si rivelano infondate.

12.5. Misure nei confronti del Sindaco

In caso di violazione del Modello da parte del sindaco o di adozione, nell'esercizio delle proprie attribuzioni, di provvedimenti che contrastino con le disposizioni o principi del Modello, l'OdV ne darà immediata informazione al Consiglio di Amministrazione, che adotterà i provvedimenti del caso, ivi compresa l'eventuale convocazione dell'assemblea dei soci con la proposta di eventuale revoca dalla carica. Le relative comunicazioni saranno indirizzate direttamente a tutti i componenti del Consiglio di Amministrazione.

Salva ogni altra azione a tutela di 7Layers, è passibile di revoca dell'incarico il sindaco che compia atti di ritorsione o discriminatori, diretti o indiretti, nei confronti di chi abbia effettuato segnalazioni mediante i canali *whistleblowing* per motivi che

siano collegati, direttamente o indirettamente, alla segnalazione stessa. Analoga sanzione è prevista per il componente del Collegio Sindacale che effettui con dolo o colpa grave che si rivelano infondate.

12.6. Misure nei confronti dell'Organismo di Vigilanza

In caso di violazione del presente Modello da parte di uno o più membri dell'OdV, gli altri membri dell'OdV o gli Amministratori, informeranno immediatamente il sindaco unico ed il Consiglio di Amministrazione: quest'ultimo, previa contestazione della violazione e concessione degli adeguati strumenti di difesa, prenderà gli opportuni provvedimenti tra cui, ad esempio, la revoca dell'incarico ai membri dell'OdV che abbiano violato il Modello e la conseguente nomina di nuovi membri in sostituzione degli stessi ovvero la revoca dell'incarico all'intero organo e la conseguente nomina di un nuovo OdV.

Salva ogni altra azione a tutela di 7Layers, è passibile di revoca dell'incarico il componente dell'OdV che compia atti di ritorsione o discriminatori, diretti o indiretti, nei confronti di chi abbia effettuato segnalazioni mediante i canali *whistleblowing* per motivi che siano collegati, direttamente o indirettamente, alla segnalazione stessa. Analoga sanzione è prevista per il componente dell'OdV che effettui con dolo o colpa grave segnalazioni che si rivelano infondate.

12.7. Misure nei confronti di Partner

La commissione dei reati di cui al D.Lgs. 231/2001 da parte di Partner, così come ogni violazione da parte degli stessi delle regole di cui al Modello e del Codice Etico, comporta, per le funzioni aziendali che con gli stessi intrattengono rapporti, l'obbligo di azionare tutti gli strumenti contrattuali e di legge a disposizione per la tutela dei diritti della Società, ivi compresi ove del caso la risoluzione del contratto ed il risarcimento dei danni.

13. NORME E STANDARD DI COMPORTAMENTO NELLE RELAZIONI CON DIPENDENTI E CON *STAKEHOLDER* ESTERNI

Nello svolgimento delle proprie attività, oltre alle regole di cui al Modello e, in particolare, a quelle indicate ai paragrafi precedenti, gli amministratori, i dirigenti e i dipendenti di 7Layers, nonché i Partner nell'ambito delle attività da essi svolte devono conoscere e rispettare:

- la normativa applicabile;
- il Codice Etico;

- il sistema di controllo interno, e quindi le procedure/linee guida aziendali, la documentazione e le disposizioni inerenti la struttura organizzativa aziendale e il sistema di controllo della gestione.

I divieti di carattere generale appresso specificati si applicano in via diretta agli amministratori, ai dipendenti di 7Layers, nonché ai Partner, in forza di apposite clausole contrattuali.

È fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle previste dal Decreto; è fatto altresì divieto di porre in essere comportamenti in violazione dei principi procedurali previsti nella Parte Speciale.

Con riferimento al rischio di commissione dei **reati contro la Pubblica Amministrazione** è fatto divieto, in particolare, di:

- effettuare elargizioni in denaro a pubblici funzionari italiani o stranieri;
- distribuire e/o ricevere omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo offerto eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale); in particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere benefico o culturale, o l'immagine dei servizi offerti da 7Layers (*brand image*). I regali offerti - salvo quelli di modico valore - devono essere documentati in modo adeguato per consentire le verifiche da parte dell'Organismo di Vigilanza, come previsto dalla Direttiva Anti-corruzione;
- accordare o promettere vantaggi di qualsiasi natura in favore di rappresentanti della Pubblica Amministrazione italiana o straniera che possano determinare le stesse conseguenze previste al precedente punto (il presente riferimento ai rapporti con la Pubblica Amministrazione e quelli successivi indicati nel testo valgono in relazione ai rapporti con gli enti pubblici e con i soggetti incaricati di pubblico servizio);
- esaminare o proporre opportunità di impiego e/o commerciali che possano avvantaggiare dipendenti delle istituzioni o pubblici funzionari a titolo personale;
- sollecitare o ottenere informazioni riservate che possano compromettere l'integrità o la reputazione di entrambe le parti o che comunque violino la parità di trattamento e le procedure di evidenza pubblica attivate dalle Istituzioni o da Pubblici Funzionari;
- assegnare o delegare l'uso di auto aziendali a soggetti diversi da quelli espressamente autorizzati dalla Società;

- ricevere prestazioni da parte di Partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale con gli stessi;
- riconoscere compensi in favore di Partner che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire finanziamenti, contributi o erogazioni di qualsiasi natura;
- destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti a scopi diversi da quelli per cui sono stati erogati.

In merito alla commissione di **reati informatici**, sono previsti i seguenti obblighi:

- proteggere l'integrità delle informazioni contenute nei sistemi della Società;
- adottare tutte le misure necessarie per garantire la protezione delle credenziali di accesso ai sistemi dei clienti;
- inclusione negli accordi con terze parti e nei contratti di lavoro di clausole di non divulgazione delle informazioni;
- accedere ai sistemi dei clienti esclusivamente nell'ambito del perimetro di attività oggetto del contratto di fornitura;
- inserimento nei contratti con i fornitori per servizi da erogare alla clientela di apposite clausole con le quali lo stesso si impegna a svolgere le proprie attività nell'ambito del perimetro autorizzato;
- garantire la tracciabilità degli accessi e delle attività svolte sui sistemi informatici dei clienti;
- rispettare le leggi e i regolamenti applicabili alla materia della protezione e della sicurezza di dati personali e sistemi informatici.

È fatto divieto di:

- violare i sistemi di controllo predisposti a tutela dei dati e dei sistemi del cliente;
- utilizzare le credenziali dei sistemi di clienti al di fuori delle attività consentite e svolgere operazioni non autorizzate;
- utilizzare le informazioni acquisite dai sistemi dei clienti per fornirle a terzi soggetti, in violazione degli accordi di riservatezza;
- acquisire, fare copia o manipolare indebitamente dati, documenti o programmi presenti all'interno dei sistemi informatici del cliente.

Con riferimento al rischio di commissione dei **reati societari** sono stabiliti i seguenti obblighi:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al

fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;

2. tenere comportamenti corretti, nel rispetto delle norme di legge e delle procedure aziendali interne, ponendo la massima attenzione ed accuratezza nell'acquisizione, elaborazione ed illustrazione dei dati contabili, necessari per consentire giudizio una rappresentazione chiara della situazione patrimoniale, economica e finanziaria della società e sull'evoluzione della sua attività;
3. osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
4. salvaguardare il regolare funzionamento della società e degli organi sociali garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
5. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalle regole interne al fine di permettere il *reporting* verso le società che esercitano il controllo su 7Layers;
6. tenere un comportamento corretto nelle transazioni commerciali e nei rapporti di collaborazione, evitando di dare o promettere denaro o altra utilità al fine di indurre la controparte a compiere e/o ad omettere atti con violazione dei propri obblighi e con indebito interesse e/o vantaggio a favore di 7Layers.

Nell'ambito dei suddetti comportamenti è fatto divieto di:

con riferimento al precedente punto 1:

- a) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società;
- b) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;

con riferimento al precedente punto 2:

- a) illustrare i dati e le informazioni utilizzati in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della società e sull'evoluzione della sua attività;

con riferimento all'obbligo di cui al precedente punto 3:

- a) restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- b) ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- c) acquistare o sottoscrivere azioni della società o di società controllate fuori dai casi previsti dalla legge, con lesione dell'integrità del capitale sociale;

- d) effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- e) procedere a formazione o aumento fittizi del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale;

con riferimento al precedente punto 4:

- a) porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione da parte del sindaco;
- b) determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare.

Con riferimento al rischio di commissione dei **reati contro la personalità individuale** sono stabiliti i seguenti obblighi:

- gli amministratori, i dirigenti ed in genere i dipendenti applicano le misure organizzative e contrattuali per verificare il rispetto da parte dei *partner* commerciali delle norme di legge in materia di lavoro minorile, di lavoro femminile e di rispetto dei lavoratori ai sensi della normativa vigente, nonché delle norme igienico-sanitarie nel luogo di lavoro;
- i *Partner* commerciali si attengono al rispetto delle disposizioni normative vigenti.

Con riferimento al rischio di commissione dei **reati di ricettazione, riciclaggio, impiego di denaro o altra utilità di provenienza illecita e di autoriciclaggio** sono stabiliti i seguenti obblighi:

- non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, all'usura;
- non realizzare operazioni finanziarie e/o commerciali con controparti che utilizzano strutture societarie opache e/o che impediscono l'identificazione univoca dell'assetto societario (proprietà) e/o dei reali beneficiari dell'operazione;
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori/clienti/*partner* stranieri;
- segnalare all'Organismo di Vigilanza ogni operazione che presenti caratteri di anomalia, motivi di sospetto o elementi di attenzione con riguardo alla legittimità della provenienza delle somme oggetto di transazione o all'affidabilità e trasparenza della controparte;
- rispettare la disciplina generale in tema di mezzi di pagamento prevista dal D.Lgs. 231/2007;

- non accettare pagamenti in contanti e valutare l'affidabilità dei clienti che effettuano pagamenti da istituti di credito esteri, soprattutto qualora gli stessi abbiano sede in paradisi fiscali;
- attuare una periodica formazione ed informazione degli esponenti aziendali sui temi relativi alla prevenzione dei fenomeni di riciclaggio;
- dare evidenza delle attività e dei controlli svolti.

Con riferimento al rischio di commissione dei **reati contro l'industria ed il commercio** sono stabiliti i seguenti obblighi:

- inserire nei contratti di acquisizione di prodotti tutelati da diritti di proprietà industriale specifiche clausole con cui la controparte attesta:
 - o di essere il legittimo titolare dei diritti di sfruttamento economico sui marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione o comunque di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi;
 - o che i marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione o di concessione in uso non violano alcun diritto di proprietà industriale in capo a terzi.

È fatto divieto di:

- utilizzare segreti aziendali altrui;
- porre in essere atti fraudolenti idonei a produrre uno sviamento della clientela altrui e un danno per imprese concorrenti alla Società;
- riprodurre abusivamente, imitare, manomettere marchi, segni distintivi, brevetti, disegni industriali o modelli in titolarità di terzi;
- fare uso, in ambito industriale e/o commerciale, di marchi, segni distintivi, brevetti, disegni industriali o modelli contraffatti da soggetti terzi;
- introdurre nel territorio dello Stato per farne commercio, detenere per vendere o mettere in qualunque modo in circolazione prodotti industriali con marchi o segni distintivi contraffatti o alterati da soggetti terzi.

Con riferimento al rischio di commissione dei **reati in materia di violazione del diritto di autore** sono stabiliti i seguenti divieti:

- procurarsi illegalmente, conservare, riprodurre, diffondere, distribuire e/o utilizzare nelle attività della Società (es.: preparazione di materiale per convention, meeting, eventi istituzionali e/o di promozione commerciale, ecc.) materiale ottenuto in violazione delle norme in materia di protezione del diritto d'autore;
- utilizzare, riprodurre o distribuire *software* in violazione delle licenze d'uso;
- ostacolare o omettere, anche con artifici e raggiri, l'adempimento degli obblighi derivanti dalla normativa in materia di protezione del diritto d'autore.

Con riferimento al rischio di commissione dei **reati tributari** sono stabiliti i seguenti obblighi:

- rispettare i ruoli e le attribuzioni aziendali individuate per il calcolo delle imposte, reddituali e patrimoniali e in generale per la gestione ed il monitoraggio degli adempimenti fiscali e per la successiva trasmissione telematica;
- rispettare i ruoli e le attribuzioni aziendali individuate per la determinazione, comunicazione e pagamento della posizione IVA della Società;
- programmare adeguatamente le tempistiche e le scadenze per gli adempimenti fiscali e gestire tempestivamente le eventuali problematiche connesse al calcolo delle imposte derivanti da operazioni con controparti anche internazionali;
- assicurare la corretta e completa tenuta della documentazione obbligatoria e delle scritture contabili.

È inoltre fatto divieto di:

- presentare dichiarazioni fiscali e tributarie non veritiere o incomplete;
- utilizzare, nelle dichiarazioni sui redditi o sul valore aggiunto, fatture o altri documenti relativi ad operazioni non effettivamente svolte, ovvero che descrivano genericamente l'oggetto della prestazione (o che non lo descrivano affatto) o che non siano attribuibili all'emittente del documento;
- porre in essere comportamenti che, mediante l'occultamento o la distruzione in tutto o in parte delle scritture contabili o dei documenti di cui è obbligatoria la conservazione, non consentano la ricostruzione dei redditi o del volume d'affari da parte dell'Amministrazione Finanziaria;
- ricevere denaro in contanti oltre i limiti stabiliti dalle disposizioni normative vigenti.