HUAWEI TECHNOLOGIES ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del Decreto legislativo 8 giugno 2001, n. 231)

Parte Generale

Approvato dal Consiglio di Amministrazione

di Huawei Technologies Italia S.r.l. in data 5/01/2018

INDICE

Definizioni

***Attività sensibili*:** le attività aziendali nel cui ambito potrebbero potenzialmente crearsi le occasioni, le condizioni e gli strumenti per la commissione dei reati.

Huawei Technologies Italia S.r.l.: la Società con sede a Milano, Via Lorenteggio, 257 - 20152, che ha adottato il presente Modello di Organizzazione, Gestione e Controllo.

***CCNL*:** il Contratto Collettivo Nazionale di lavoro per il personale dipendente da imprese esercenti servizi di telecomunicazione.

Business Code of Conduct: il Codice di Condotta adottato da Huawei Technologies Italia S.r.l.

***Consiglio di Amministrazione (anche CdA o Organo Dirigente)*:** il Consiglio di Amministrazione di Huawei Technologies Italia S.r.l..

***Collaboratori, Consulenti o Partner commerciali*:** i soggetti che intrattengono con la Società rapporti di collaborazione senza vincolo di subordinazione, di rappresentanza commerciale ed altri rapporti che si concretino in una prestazione professionale non a carattere subordinato, sia continuativa sia occasionale nonché quanti, in forza di specifici mandati e procure, rappresentano la Società verso terzi.

***Decreto o D.lgs. 231/2001*:** il Decreto legislativo 8 giugno 2001 n. 231, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300*", nel contenuto di tempo in tempo vigente.

***Destinatari*:** i soggetti ai quali si applicano le disposizioni del presente Modello.

***Dipendenti*:** le persone fisiche sottoposte alla direzione o alla vigilanza di soggetti che rivestono funzioni di rappresentanza, amministrazione o di direzione della Società[1], ossia tutti i soggetti che intrattengono un rapporto di lavoro subordinato, di qualsivoglia natura, con la Società, nonché i lavoratori con contratti di lavoro parasubordinato.

***Fornitori*:** coloro che forniscono beni o servizi in favore di Huawei Technologies Italia S.r.l..

***Gruppo Huawei (anche Gruppo)*:** il Gruppo che fa capo a Huawei Investment & Holding Co. Ltd con sede a Shenzhen (Cina).

[1] Art. 5.1, lett. a) e b) del Decreto legislativo 8 giugno 2001, n. 231.

***Modello di Organizzazione, Gestione e Controllo (anche Modello)*:** il presente Modello di Organizzazione, Gestione e Controllo adottato ai sensi degli artt. 6 e 7 del D.lgs. 231/2001 ed i relativi allegati.

***Organismo di Vigilanza (anche Organismo o OdV)*:** l'Organismo dell'Ente dotato di autonomi poteri di iniziativa e controllo, con il compito di vigilare sull'adeguatezza, sul funzionamento, sull'osservanza del Modello nonché di curarne l'aggiornamento.

Pubblica Amministrazione, PA o Enti Pubblici: la Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio.

Pubblici Ufficiali: ai sensi dell'art.357 del codice penale, sono "*coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della Pubblica Amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi*".

Reati: i reati di cui al D.Lgs. 231/2001.

***Società*:** Huawei Technologies Italia S.r.l. con sede legale a Milano, Via Lorenteggio, 257 - 20152.

Premessa

Huawei Technologies Italia S.r.l.

Huawei Technologies Italia S.r.l. (d'ora in avanti "la Società" o "Huawei") è una Società operante in Italia nel settore dei servizi per le telecomunicazioni; la Società sviluppa soluzioni tecnologiche e servizi per le reti di telecomunicazione di nuova generazione, per comunicazioni fisse, mobili e di dati; Huawei affianca a tale attività lo svolgimento di servizi alle imprese, intese in senso più generale, per la fornitura di soluzioni per infrastrutture di *information and communication technologies* progettate su misura per singolo cliente e, infine, la commercializzazione di propri apparati telefonici e digitali.

Nello specifico, la Società ha per oggetto le seguenti attività:

- la produzione, l'importazione, l'esportazione l'acquisto e la vendita anche per corrispondenza ovvero tramite commercio elettronico, via internet o qualsiasi altro mezzo telematico, di sistemi di telecomunicazioni, di apparecchiature per la comunicazione e trasmissione dati, di tecniche di sviluppo ed implementazione di sistemi ("system integration"), di computer ed apparecchiature accessorie, nonchè ogni altra apparecchiatura di telecomunicazione e di trasmissione dati, inclusi il software associato, la manutenzione, la consulenza tecnica e servizi accessori di assistenza;

- l'installazione, il collaudo e la manutenzione di ogni tipo di sistema e di apparecchiatura di telecomunicazione e di trasmissione dati nonché di beni e servizi correlati;

- l'istituzione di centri di ricerca per lo sviluppo di software e hardware;

- l'istituzione e gestione di centri per la formazione inerente il prodotto e di centri di assistenza per la manutenzione del prodotto;

- la partecipazione a *"joint ventures"* o ad altri raggruppamenti di aziende, la costituzione o l'acquisto di società o rami d'azienda per l'esecuzione di progetti nell'ambito delle telecomunicazioni.

- la progettazione, realizzazione, anche "chiavi in mano", costruzione, installazione, manutenzione ed ottimizzazione di: infrastrutture, impianti, sistemi e reti di telecomunicazioni e di telefonia di ogni genere, nonché di sistemi di trasmissione e trattamento dati, video e telefonia nazionale e internazionale, impianti elettrici, elettronici e di elaborazione dati, impianti telefonici, radiotelefonici e televisivi, compresi tutti gli impianti connessi ed accessori;
- in via esemplificativa, ma non limitativa, essa potrà svolgere in particolare la costruzione, la fornitura, il montaggio, la manutenzione o ristrutturazione e qualsiasi altra attività riguardante:

- impianti pneumatici e di antintrusione e sicurezza;
- impianti tecnologici;
- impianti per la produzione, la trasformazione e la distribuzione dell'energia elettrica
- impianti elettromeccanici trasportatori;
- impianti di segnaletica luminosa per la sicurezza del traffico;
- sistemi per l'automazione dei processi produttivi;
- lavori di ingegneria civile ed industriale comprendenti lavori di movimento terra incluse ogni eventuale opera connessa relativamente a sistemi di telecomunicazione e/o produzione e distribuzione di energia;
- la fornitura di soluzioni e piattaforme per la gestione di contenuti lineari via IP e di servizi per la gestione e la vendita, da terze parti, di contenuti globali;

In generale, la Società può compiere tutte le operazioni commerciali, immobiliari e finanziarie così come qualsiasi altra operazione su beni mobili o immobili che siano connesse direttamente o indirettamente, in tutto o in parte, con l'oggetto sociale di cui sopra, ovvero con altro fine simile o connesso allo stesso che possa facilitare l'espansione e lo sviluppo della Società, fermo restando che le attività finanziarie saranno svolte solamente in via collaterale o accessoria all'attività principale e comunque non nei confronti del pubblico.

La sede legale societaria è sita in Milano, via Lorenteggio, 257; sono, inoltre, presenti unità locali a destinazione commerciale nelle principali regioni italiane e un centro di ricerca e sviluppo a Segrate (MI).

La Società è controllata da Huawei Technologies Cooperatief U.A., società di diritto olandese che fa capo a Huawei Investment & Holding Co. Ltd con sede a Shenzhen (Cina). Il Gruppo, leader mondiale nella fornitura di prodotti e soluzioni in ambito Information & Communication Technology (ICT), è stato fondato nel 1987 ed opera in oltre 170 paesi con circa 180.000 dipendenti.

La *Corporate Governance* di Huawei Technologies Italia S.r.l.

La Società ha una struttura organizzativa verticistica di tipo tradizionale. Il Consiglio di Amministrazione è composto da tre membri e riveste un ruolo centrale nel sistema di governo societario, deliberando in merito alle operazioni che assumono un significativo rilievo strategico, economico o finanziario.

Il Consiglio è investito dei più ampi poteri per la gestione ordinaria e straordinaria ed ha la facoltà di compiere tutti gli atti ritenuti opportuni per l'attuazione ed il

raggiungimento degli scopi sociali, esclusi soltanto quelli che la legge riserva in modo tassativo all'esclusiva competenza dei Soci o dell'Assemblea.

E' presente un Collegio Sindacale, composto da tre membri effettivi e due supplenti.

Il Collegio Sindacale vigila sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione ed in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile, adottato dalla Società e sul suo concreto funzionamento.

Il Collegio Sindacale, per l'affinità professionale e i compiti che gli sono attribuiti dalla legge, è uno degli interlocutori privilegiati e istituzionali dell'Organismo di Vigilanza *ex* D.Lgs. 231/2001.

Il bilancio civilistico di Huawei Technologies Italia è certificato dalla Società di Revisione secondo quanto previsto dalle normative e dai principi di riferimento; la stessa certifica, altresì, il *reporting* finanziario redatto secondo i principi contabili internazionali ai fini del consolidato di Gruppo.

Il sistema di controllo interno

Nella costruzione del Modello di Huawei si è tenuto conto degli strumenti di governo dell'organizzazione societaria che ne garantiscono il funzionamento.

Questi possono essere così riassunti:

- **Statuto** – che, 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.

- **Sistema delle deleghe e delle procure** – per mezzo del quale il Consiglio di Amministrazione e l'Amministratore Delegato conferiscono le deleghe ed i poteri di firma, in coerenza con le responsabilità organizzative e gestionali, con una puntuale indicazione delle soglie di approvazione delle spese.

- **Business Code of Conduct** – contenente le regole di comportamento ed i principi di carattere generale che tutti i soggetti interni ed esterni, che hanno direttamente o indirettamente una relazione con Huawei, devono rispettare e la cui violazione comporta l'applicazione delle misure sanzionatorie previste dal Sistema disciplinare del presente Modello.

- **Anti-Bribery Policy** – che identifica la posizione della Società in tema di anticorruzione e definisce le responsabilità in materia di ciascun dipendente Huawei e di ogni persona fisica o giuridica che operi a favore o per conto della Società.

- **Sistema procedurale** – costituito da procedure, *policy*, regolamenti, manuali, istruzioni operative e comunicazioni interne volte a regolamentare in modo chiaro ed efficace i processi rilevanti ed a fornire modalità operative e presidi di controllo per lo svolgimento delle attività aziendali.

Il sistema di controllo interno della Società si basa, oltre che sugli strumenti di governo di cui sopra, sui seguenti elementi qualificanti:

- sistema di controllo di gestione e *reporting*;

- sistemi informatici già orientati alla segregazione delle funzioni e regolati da procedure interne che garantiscono sicurezza, *privacy* e corretto utilizzo da parte degli utenti nonché un elevato livello di protezione delle informazioni in essi contenute;

- comitati interni funzionali alla messa a punto ed allo sviluppo dei processi aziendali che richiedono la partecipazione di più funzioni/competenze e l'adozione di determinazioni collegiali. Mediante la costituzione di tali comitati la Società persegue, inoltre, l'obiettivo di garantire una ulteriore e più efficiente applicazione del principio di *segregation of duties*.

Inoltre, con particolare riferimento ai reati commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-*septies* D.Lgs. 231/2001) e ai reati ambientali (art. 25-*undecies* D.Lgs. 231/2001), la Società si è dotata di un sistema integrato di gestione della salute e sicurezza sul lavoro e ambientale ("Sistema di Gestione HSE"), corredati da specifiche procedure e certificato in conformità:

- al British Standard OHSAS 18001:2007 ("*Occupational Health & Safety Management System*"), in linea con le indicazioni date dall'art. 30 del D.Lgs. 81/2008;

- alla norma ISO 14001 ("*Environmental Management System*").

In particolare, lo standard OHSAS stabilisce quali sono i criteri per un sistema di gestione della salute e sicurezza sul lavoro al fine di consentire all'organizzazione aziendale di controllare i propri rischi di igiene e sicurezza e migliorare le proprie prestazioni.

Per quanto concerne i delitti informatici (art. 25-*bis*), la Società si è dotata di un sistema di gestione della sicurezza delle informazioni (ISMS) certificato ISO/IEC 27001:2005, corredato da un set di procedure specifiche.

Lo standard ISO 27001 fornisce i requisiti per adottare un ISMS finalizzato ad una corretta gestione dei dati sensibili della Società.

Nell'ottica di garantire una più efficace attuazione dei sistemi di controllo, la Società ha ottenuto la certificazione anche per i seguenti sistemi:

- ISO 9001, sistema di gestione della qualità;
- ISO 22301, sistema di gestione della continuità operativa.

Per il tramite dei sistemi di gestione sopra citati, Huawei è in grado di assicurare, attraverso la predisposizione delle apposite procedure, la conformità dei propri comportamenti agli obblighi giuridici posti dalla legislazione vigente nonché agli standard di controllo della migliore prassi internazionale, tracciandone, con apposita registrazione, l'avvenuta effettuazione.

Le regole e i principi contenuti nella documentazione sopra elencata, pur non essendo riportati dettagliatamente nel presente Modello, costituiscono uno strumento a presidio di comportamenti illeciti in generale, inclusi quelli di cui al D.Lgs. 231/2001 che fa parte del più ampio sistema di organizzazione, gestione e controllo che il Modello intende integrare e che tutti i soggetti destinatari sono tenuti a rispettare, in relazione al tipo di rapporto in essere con la Società.

Tutto il sistema di controllo interno della Società è sottoposto a verifiche periodiche da parte della funzione Internal Audit di Gruppo.

Il Business Code of Conduct di Huawei Technologies Italia S.r.l.

Huawei Technologies Italia S.r.l. intende operare secondo principi etici diretti ad improntare lo svolgimento dell'attività, il perseguimento dello scopo sociale e la crescita della Società al rispetto delle leggi vigenti. A tal fine ha adottato un Business Code of Conduct volto a definire delle *guidelines* di deontologia aziendale che la Società riconosce come proprie e delle quali esige l'osservanza da parte di:

- tutti i dipendenti, inclusi i lavoratori locali che operano nei territori dell'UE, presso Head Quarter, etc.;
- tutti i dipendenti espatriati in Italia dotati di un permesso di lavoro / visto di lavoro, inclusi i dipendenti espatriati che lavorano nei territori della UE, presso Head Quarter, etc.;
- i collaboratori, i lavoratori a progetto, gli agenti e tutti coloro che operano per conto di Huawei.

Tale Business Code of Conduct costituisce parte integrante del sistema di organizzazione, gestione e controllo nonché di prevenzione adottato dalla Società. In particolare il Business Code of Conduct rappresenta l'insieme dei diritti, dei doveri e delle responsabilità di Huawei nei confronti di dipendenti, clienti, fornitori, Pubblica Amministrazione (in generale, quindi, con riferimento a soggetti portatori di interesse nei confronti della Società); il Business Code of Conduct mira quindi a raccomandare, promuovere o vietare determinati comportamenti, indipendentemente ed anche al di là di quanto previsto dal Decreto o dalla normativa vigente.

Inoltre, ogni area di business ha adottato un proprio Code of Conduct for Partners, che definisce i principi etici e gli standard di compliance a cui tutti i partner di Huawei, inclusi appaltatori, agenti e distributori, si devono attenere nella conduzione dei rapporti commerciali con la Società. Anti-Bribery Policy

Huawei riconosce che la corruzione ha un effetto negativo sulla Società, danneggiando lo sviluppo sociale ed economico ed ostacolando la libera e leale concorrenza.

Huawei è impegnata a promuovere le proprie attività in modo etico ed onesto, in linea con i principi di business che rappresentano le fondamenta della Società.

Huawei non tollera alcun tipo di attività di natura corruttiva; la Società rispetta tutte le normative applicabili a livello nazionale e internazionale ed applica le migliori best practices in materia di anticorruzione in tutti i paesi nei quali opera.

Tutti i destinatari sono tenuti ad aderire ed osservare i seguenti principi chiave:

- condurre l'attività in maniera corretta, onesta e trasparente;
- non promettere, offrire o accettare benefici di natura corruttiva, o consentire l'offerta di benefici per conto della Società, in modo da ottenere un vantaggio per la stessa;
- evitare di intrattenere rapporti con soggetti che non accettano o osservano i principi di Huawei in materia di anticorruzione e che potrebbero danneggiarne la reputazione;
- mantenere registrazioni contabili trasparenti ed aggiornate;
- assicurare la conoscenza e l'adesione, in qualunque situazione, da parte di tutti i destinatari dei principi di anticorruzione.

Rientrano nell'ambito delle cd. "Anti-Bribery related policies" le seguenti linee guida:

- Anti-Bribery and Corruption Policy;

- Gift and Hospitality Policy;
- Business Code of Conduct Policy;
- Code of Conduct for Partners;
- Staffs Expenses Claim Managemen
- Staff Working Guidelines;
- Anti Corruption and Compliance Commitment;
- Internal Control & Audit Management Guideline;
- Whistle Blowing Policy.

BCG Complain

Huawei, al fine di garantire una più efficace attuazione dei propri principi, ha adottato una procedura di *whistleblowing* e ha messo a disposizione un canale di comunicazione riservato ("BCG Complain") attraverso il quale tutti i dipendenti possono segnalare, anche in forma anonima, eventuali violazioni o presunte violazioni del Business Code of Conduct, della Anti-Bribery policy e della Gifts and Hospitality Policy.

La struttura organizzativa di Huawei Technologies Italia S.r.l.

Un'organizzazione chiara ed adeguata alle necessità, formalizzata e comunicata al personale è un elemento di controllo essenziale; Huawei nella definizione della propria organizzazione adotta criteri che consentono:

- la chiara definizione delle responsabilità attribuite al personale e delle linee di dipendenza fra le posizioni organizzative;
- l'esistenza della contrapposizione di funzioni e segregazione dei compiti o, in alternativa, l'esistenza di misure organizzative e di controllo compensative;
- la rispondenza tra le attività effettivamente svolte e quanto previsto dalla formalizzazione dell'organizzazione.

Al fine di rendere chiaro i ruoli e le responsabilità nell'ambito del processo decisionale aziendale, la Società si è dotata di:

- un organigramma aziendale, atto a specificare le aree in cui si suddivide l'attività aziendale, le linee di dipendenza gerarchica delle singole unità aziendali, nonché il titolo della posizione dei soggetti che operano nelle singole aree;

- una descrizione delle posizioni organizzative e del relativo contenuto lavorativo (*job description*);

- sistema delle deleghe e delle procure.

La responsabilità della predisposizione e dell'aggiornamento dei documenti organizzativi è attribuita alla funzione HR, la quale provvede anche alla loro comunicazione e pubblicazione sulla intranet aziendale.

L'assetto organizzativo di Huawei Technologies Italia S.r.l. in materia di salute e sicurezza sul lavoro

Al fine di garantire il più adeguato presidio delle tematiche di salute e sicurezza, la Società si è dotata di una propria struttura organizzativa con specifici compiti e responsabilità in materia HSE, definiti formalmente in coerenza con lo schema organizzativo e funzionale dell'azienda, a partire dal datore di lavoro (così come definito dall'art. 2, comma 1, lett. b) del D.lgs. 81/2008) sino al singolo lavoratore, con particolare riguardo alle figure specifiche operanti in tale ambito (RSPP - Responsabile del Servizio di Prevenzione e Protezione, MC - Medico Competente, RLS - Rappresentante dei lavoratore per la sicurezza, preposti, Responsabile Ambiente e Sicurezza).

In questo modo, la Società ha previsto una propria articolazione di funzioni atta ad assicurare la salvaguardia degli interessi protetti per il tramite della cooperazione di più soggetti che - sulla base della valorizzazione delle necessarie competenze differenziate - si dividono il lavoro ripartendosi i compiti, ai sensi di quanto viene puntualmente richiesto dal comma 3 dell'art. 30 del D.Lgs. 81/2008 in materia di salute e sicurezza sul lavoro.

Specifiche deleghe di funzione sono attribuite dal Datore di Lavoro, ai sensi di quanto previsto dalla normativa.

Il sistema di gestione implementato dalla Società ha ottenuto la certificazione OHSAS 18001 in materia di salute e sicurezza sul lavoro.

Il sistema procedurale

Huawei Technologies Italia S.r.l. si è dotata, per la gestione dei processi aziendali, di un insieme di normative e procedure, nonché istruzioni operative di dettaglio, volte a regolamentare lo svolgimento delle attività interne, nel rispetto dei principi indicati dalla normativa generale e di settore e dalle regole di Gruppo.

La Società opera avvalendosi di procedure interne formalizzate, aventi le seguenti caratteristiche:

- adeguata diffusione nell'ambito delle strutture aziendali coinvolte nelle attività;
- regolamentazione delle modalità di svolgimento delle attività;
- definizione delle responsabilità delle attività;
- tracciabilità degli atti, delle operazioni e delle transazioni attraverso adeguati supporti documentali attestanti le caratteristiche e le motivazioni dell'operazione e che individuino i soggetti a vario titolo coinvolti nell'operazione.

Il sistema procedurale, i cui principi generali sono definiti dal Gruppo, prevede:

- policy e procedure di Gruppo, in inglese, che devono essere adottate così come definite da Casamadre e definiscono principi generali e di comportamento cui tutti si devono attenere;
- policy e procedure locali, in italiano e/o in inglese, sviluppate sulla base degli analoghi documenti di Gruppo, che regolamentano i processi operativi di Huawei Technologies Italia S.r.l.;
- procedure e istruzioni operative, in italiano e/o in inglese, che disciplinano aspetti specifici dei processi aziendali.

Tutto il sistema procedurale viene diffuso attraverso i canali di comunicazione interni ed è a disposizione di tutti i dipendenti in specifiche sezioni della intranet aziendale.

Da ultimo, si segnala come lo svolgimento dei processi operativi e delle azioni di governo aziendale sia supportato da sistemi informativi integrati, orientati alla segregazione delle funzioni, nonché ad un elevato livello di standardizzazione dei processi e alla protezione delle informazioni in essi contenuti.

1. Il Decreto Legislativo 8 giugno 2001, n. 231

1.1 I principi generali

Il Decreto legislativo 8 giugno 2001, n. 231 (di seguito il "Decreto" o "D.lgs. 231/2001") ha introdotto nel nostro ordinamento la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica (di seguito "Enti") in caso di commissione o tentata commissione di alcune tipologie di reati o di illeciti amministrativi nell'interesse o a vantaggio dell'Ente da parte di:

- soggetti 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 fisiche che esercitano, anche di fatto, la gestione e il controllo dello stesso (c.d. "Apicali");

- soggetti "Sottoposti" alla direzione o alla vigilanza delle persone di cui al punto precedente.

Si tratta di una responsabilità che, nonostante sia stata definita dal legislatore "amministrativa", presenta alcuni caratteri della responsabilità penale perché:

- consegue alla realizzazione di reati;
- è accertata dal giudice penale (nel corso di un procedimento nel quale all'Ente si applicano, ove compatibili, le disposizioni processuali relative all'imputato).

Il Decreto ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali a cui l'Italia aveva già da tempo aderito.

La responsabilità dell'Ente, ai sensi del Decreto, si aggiunge e non si sostituisce a quella (penale) dell'autore del reato: tanto la persona fisica quanto quella giuridica saranno, pertanto, sottoposti a giudizio penale.

1.2 Il "catalogo" dei reati e degli illeciti amministrativi rilevanti ai fini del Decreto

La responsabilità dell'ente sussiste solamente per quei reati (consumati o tentati) espressamente previsti dal legislatore.

In particolare, si tratta dei seguenti reati ed illeciti amministrativi:

Reati contro la Pubblica Amministrazione ed il suo patrimonio (artt. 24 e 25 del Decreto)

- Malversazione a danno dello Stato o di altro ente pubblico (art. 316-*bis* c.p.);
- Indebita percezione di contributi, finanziamenti o altre erogazioni a danno dello Stato o di un altro ente pubblico o delle Comunità Europee (art. 316-*ter* c.p.);
- Truffa a danno dello Stato o di un altro ente pubblico o delle Comunità Europee (art. 640, comma 2, n. 1, c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis* c.p.);
- Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-*ter* c.p.);
- Concussione (art. 317 c.p.);
- Corruzione per l'esercizio della funzione (artt. 318 e 321 c.p.);
- Corruzione per un atto contrario ai doveri di ufficio (artt. 319, 319-*bis* e 321 c.p.);
- Circostanze aggravanti (art. 319-*bis* c.p.);
- Corruzione in atti giudiziari (artt. 319-*ter* e 321 c.p.);
- Induzione indebita a dare o promettere utilità (art. 319-*quater* c.p.);
- Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.);
- Pene per il corruttore (art. 321 c.p.);
- Istigazione alla corruzione (art. 322 c.p.);
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri (art. 322-*bis* c.p.).

Delitti informatici e trattamento illecito di dati (art. 24-*bis* del Decreto)

- Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-*bis* c.p.);
- Accesso abusivo ad un sistema informatico o telematico (615-*ter* c.p.);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (615-*quater* c.p.);
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (615-*quinquies* c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* c.p.);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-*ter* c.p.);
- Danneggiamento di sistemi informatici o telematici (art. 635-*quater* c.p.);

- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies* c.p.);
- Frode informatica del certificatore di firma elettronica (art. 640-*quinquies* c.p.).

Delitti di criminalità organizzata (art. 24-*ter* del Decreto)

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso (art. 416-*bis*);
- Scambio elettorale politico-mafioso (art. 416-*ter* c.p.);
- Sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 309/1990);
- Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo (art. 407, comma 2, lettera a], numero 5], c.p.p.).

Reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-*bis* del Decreto)

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
- Alterazione di monete (art. 454 c.p.);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.);
- Uso di valori di bollo contraffatti o alterati (art. 464 c.p.);
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

Delitti contro l'industria e il commercio (art. 25-*bis*.1 del Decreto)

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-*bis* c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);

- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-*ter* c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-*quater* c.p.).

Reati societari (art. 25-*ter* del Decreto)

- False comunicazioni sociali (art. 2621 c.c.);
- Fatti di lieve entità (art. 2621-*bis* c.c.);
- False comunicazioni sociali delle società quotate (art. 2622 c.c.);
- Impedito controllo (art. 2625 c.c.);
- Indebita restituzione dei conferimenti (art. 2626 c.c.);
- Illegale ripartizione di utili e riserve (art. 2627 c.c.);
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Omessa comunicazione del conflitto di interessi (art. 2629-*bis* c.c.);
- Formazione fittizia del capitale sociale (art. 2632 c.c.);
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- Corruzione fra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635-*bis* c.c.);
- Illecita influenza sull'assemblea (art. 2636 c.c.);
- Aggiotaggio (art. 2637 c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).

Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-*quater* del Decreto)

- Associazioni sovversive (art. 270 c.p.);
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270-*bis* c.p.);
- Assistenza agli associati (art. 270-*ter* c.p.);
- Arruolamento con finalità di terrorismo anche internazionale (art. 270-*quater* c.p.);
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-*quinquies* c.p.);
- Condotte con finalità di terrorismo (art. 270-*sexies* c.p.);
- Attentato per finalità terroristiche o di eversione (art. 280 c.p.);
- Atto di terrorismo con ordigni micidiali o esplosivi (art. 280-*bis* c.p.);
- Atti di terrorismo nucleare (art. 280-*ter* c.p.);
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289-*bis* c.p.);
- Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo (art. 302 c.p.);
- Cospirazione politica mediante accordo (art. 304 c.p.);

- Cospirazione politica mediante associazione (art. 305 c.p.);Banda armata: formazione e partecipazione (art. 306 c.p.);
- Assistenza ai partecipi di cospirazione o di banda armata (art. 307 c.p.);
- Impossessamento, dirottamento e distruzione di un aereo (L. n. 342/1976, art. 1);
- Danneggiamento delle installazioni a terra (L. n. 342/1976, art. 2);
- Sanzioni (L. n. 422/1989, art. 3);
- Pentimento operoso (D. Lgs. N. 625/1979, art. 5);
- Convenzione di New York del 9 dicembre 1999 (art. 2).

Reato di pratiche di mutilazione degli organi genitali femminili (art. 25-*quater*.1 del Decreto)

- Pratiche di mutilazione degli organi genitali femminili (art. 583-*bis* c.p.).

Delitti contro la personalità individuale (art. 25-*quinquies* del Decreto)

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
- Prostituzione minorile (art. 600-*bis* c.p.);
- Pornografia minorile (art. 600-*ter* c.p.);
- Detenzione di materiale pornografico (art. 600-*quater* c.p.);
- Pornografia virtuale (art. 600-*quater* 1 c.p.);
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-*quinquies* c.p.);
- Tratta di persone (art. 601 c.p.);
- Alienazione e acquisto di schiavi (art. 602 c.p.);
- Intermediazione illecita e sfruttamento del lavoro (art. 603-*bis* c.p.);
- Adescamento di minorenni (art. 609-*undecies* c.p.).

Reati di abuso di mercato

Reati (art. 25-*sexies* del Decreto):

- Abuso di informazioni privilegiate (art. 184, D.lgs. 58/1998 - TUF);
- Manipolazione del mercato (art. 185, D.lgs. 58/1998 - TUF).

Illeciti Amministrativi (art. 187-*quinquies* TUF):

- Abuso di informazioni privilegiate (art. 187-*bis*, D.lgs. 24 febbraio 1998, n. 58 - TUF);
- Manipolazione del mercato (art. 187-*ter*, D.lgs. 24 febbraio 1998, n. 58 - TUF).

Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme a tutela della salute e sicurezza sul lavoro (art. 25-*septies* del Decreto)

- Omicidio colposo (art. 589 c.p.);
- Lesioni personali colpose (art. 590 c.p.).

Reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-*octies* del Decreto)

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-*bis* c.p);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.);
- Autoriciclaggio (art. 648-*ter*.1 c.p.).

Delitti in materia di violazioni del diritto d'autore (art. 25-*novies* del Decreto)

- Protezione penale dei diritti di utilizzazione economica e morale (art. 171, comma 1, lett. a]-*bis* e comma 3, Legge n. 633/1941);
- Tutela penale del *software* e delle banche dati (art. 171-*bis*, comma 1, Legge n. 633/1941);
- Tutela penale delle opere audiovisive (art. 171-*ter*, Legge n. 633/1941);
- Responsabilità penale relativa ai supporti (art. 171-*septies*, Legge n. 633/1941);
- Responsabilità penale relativa a trasmissioni audiovisive ad accesso condizionato (art. 171-*octies*, Legge n. 633/1941).

Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-*decies* del Decreto)

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* c.p.).

Reati ambientali (art. 25-*undecies* del Decreto)

- Inquinamento ambientale (art. 452-*bis* c.p.);
- Disastro ambientale (art. 452-*quater* c.p.);
- Delitti colposi contro l'ambiente (art. 452-*quinquies* c.p.);
- Traffico ed abbandono di materiale ad alta radioattività (art. 452-*sexies* c.p.);
- Circostanze aggravanti (art. 452-*octies* c.p.);
- Uccisione, distruzione, cattura, prelievo detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-*bis* c.p.);
- Distruzione o deterioramento di *habitat* all'interno di un sito protetto (art. 733-*bis* c.p.).

- Importazione, esportazione, detenzione utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. n. 150/1992, art. 1, art. 2, art.3-*bis* e art. 6);
- Scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili (D.Lgs. 152/2006, art. 137);
- Attività di gestione di rifiuti non autorizzata (D.Lgs. 152/2006, art. 256);
- Bonifica dei siti (D.Lgs. 152/2006, art. 257);
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D.Lgs. 152/2006, art. 258, comma 4, secondo periodo);
- Traffico illecito di rifiuti (D.Lgs. 152/2006, art. 259, comma 1);
- Attività organizzate per il traffico illecito di rifiuti (D.Lgs. 152/2006, art. 260, commi 1 e 2);
- Sistema informatico di controllo della tracciabilità dei rifiuti (D.Lgs. 152/2006, art. 260-*bis*, commi 6 e 7, secondo e terzo periodo, e comma 8, primo e secondo periodo);
- Reati in materia di emissioni (D.Lgs. 152/2006, art. 279, comma 5);
- Inquinamento doloso provocato da navi (D.Lgs. N. 202/2007, art. 8);
- Inquinamento colposo provocato da navi (D.Lgs. N. 202/2007, art. 9);
- Cessazione e riduzione dell'impiego delle sostanze lesive (L. n. 549/1993, art. 3).

Delitto di impiego di cittadini di stati terzi il cui soggiorno è irregolare (art. 25-*duodecies* del Decreto)

- Lavoro subordinato a tempo determinato e indeterminato (art. 22, comma 12-*bis*, D.lgs. 286/1998 – Testo Unico sull'immigrazione).

Reati transnazionali (art. 10 – Legge n. 146/2006)

Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale:

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso, anche straniera (art. 416-*bis* c.p.);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-*quater* del Testo Unico di cui al D.P.R. 23 gennaio 1973, n. 43);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del Testo Unico di cui al D.P.R. 9 ottobre 1990, n. 309);
- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-*bis*, 3-*ter* e 5, del Testo Unico di cui al D.lgs. 286/1998);

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* c.p.);
- Favoreggiamento personale (art. 378 c.p.).

I reati e gli illeciti amministrativi sopra richiamati possono comportare la responsabilità amministrativa dell'Ente che, pur avendo sede principale nel territorio italiano, sono stati commessi all'estero.

I presupposti su cui si fonda la responsabilità dell'ente per reati commessi all'estero sono i seguenti:

- l'ente può rispondere solo nei casi e alle condizioni previste dagli artt. 7, 8, 9, 10 c.p. (nei casi in cui la legge prevede che il colpevole - persona fisica - sia punito a richiesta del Ministro della Giustizia, si procede contro l'ente solo se la richiesta è formulata anche nei confronti dell'ente stesso);

- sussistendo i casi e le condizioni di cui ai predetti articoli del codice penale, nei confronti dell'ente non procedano le Autorità dello Stato del luogo in cui è stato commesso il fatto.

1.3 Il sistema sanzionatorio previsto dal Decreto

Le sanzioni previste dal Decreto a carico degli Enti sono: i) sanzioni pecuniarie, ii) sanzioni interdittive, iii) confisca del prezzo o del profitto del reato, iv) pubblicazione della sentenza di condanna.

Le **sanzioni pecuniarie** si applicano ogniqualvolta venga accertata la responsabilità della persona giuridica e sono determinate dal giudice penale attraverso un sistema basato su «quote». Nello specifico, nella commisurazione della sanzione pecuniaria 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 della quota è fissato, invece, sulla base delle condizioni economiche e patrimoniali dell'ente.

Le **sanzioni interdittive** possono trovare applicazione per alcune tipologie di reato e per le ipotesi di maggior gravità. Si traducono nell'interdizione dall'esercizio dell'attività aziendale; nella sospensione e nella revoca delle autorizzazioni, delle licenze o delle concessioni funzionali alla commissione dell'illecito; nel divieto di contrattare con la pubblica amministrazione (salvo che per ottenere le prestazioni di un pubblico servizio); nell'esclusione da agevolazioni, finanziamenti, contributi o sussidi e nell'eventuale revoca di quelli concessi; nel divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive non si applicano (o sono revocate, se già applicate in via cautelare) qualora l'Ente, prima della dichiarazione di apertura del dibattimento di primo grado, abbia:

- risarcito il danno o lo abbia riparato;
- eliminato le conseguenze dannose o pericolose del reato (o, almeno, si sia adoperato in tal senso);
- messo a disposizione dell'Autorità Giudiziaria, per la confisca, il profitto del reato;
- eliminato le carenze organizzative che hanno determinato il reato, adottando modelli organizzativi idonei a prevenire la commissione di nuovi reati.

La **confisca** consiste nell'acquisizione del prezzo o del profitto del reato da parte dello Stato o nell'acquisizione di somme di danaro, beni o altre utilità di valore equivalente al prezzo o al profitto del Reato: non investe, tuttavia, quella parte del prezzo o del profitto del Reato che può restituirsi al danneggiato. La confisca è sempre disposta con la sentenza di condanna.

La **pubblicazione della sentenza** può essere inflitta quando all'Ente è applicata una sanzione interdittiva. E' effettuata mediante affissione nel comune ove l'Ente ha la sede principale nonché mediante la pubblicazione sul sito *internet* del Ministero della Giustizia.

1.4 Il Modello di organizzazione, gestione e controllo come esimente della responsabilità prevista dal Decreto

Il Decreto prevede che la società non sia passibile di sanzione se provi di aver adottato ed efficacemente attuato **Modelli Di Organizzazione, Gestione e Controllo idonei a prevenire la commissione dei reati verificatisi**, ferma restando la responsabilità personale di chi ha commesso il fatto.

Il legislatore, pertanto, ha attribuito un valore esimente ai modelli di organizzazione, gestione e controllo della società nel caso in cui siano idonei alla prevenzione del rischio, nonché adottati ed efficacemente attuati. Nel decreto si specificano altresì le esigenze cui devono rispondere i modelli.

Segnatamente:

- individuare le attività nel cui ambito possano essere commessi i reati previsti dal Decreto;

- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;

- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;

- prevedere obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;

- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Se il reato è commesso da soggetti 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 soggetti che esercitano, anche di fatto, la gestione e il controllo dello stesso, l'Ente non risponde se prova che:

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi;

- il compito di vigilare sul funzionamento e l'osservanza del Modello e di curare il suo aggiornamento è stato affidato a un Organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;

- i soggetti hanno commesso il reato eludendo fraudolentemente il Modello;

- non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di controllo in ordine al Modello.

Nel caso in cui, invece, il reato sia commesso da soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati, la persona giuridica è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Detta inosservanza è, in ogni caso, esclusa qualora l'Ente, prima della commissione del reato, abbia adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi.

2. Il Modello di Organizzazione, Gestione e Controllo di Huawei Technologies Italia S.r.l.

2.1 Adozione e aggiornamenti del Modello organizzativo di Huawei Technologies Italia S.r.l.

Huawei ha adottato la prima edizione del Modello Di Organizzazione, Gestione e Controllo con delibera del Consiglio di Amministrazione in data 09/11/2014 ed ha provveduto al suo successivo aggiornamento in data 5/01/2018

Il Consiglio di Amministrazione apporta le modifiche e le integrazioni al presente Modello organizzativo, anche su informativa dell'Organismo di Vigilanza che ne cura l'aggiornamento, in relazione a;

- significative violazioni delle prescrizioni del Modello adottato;
- modifiche normative che comportano l'estensione della responsabilità amministrativa degli enti ad altre tipologie di reato per le quali si reputi sussistente un rischio di commissione nell'interesse o a vantaggio della Società;
- significative modifiche intervenute nella struttura organizzativa, nel sistema dei poteri e nelle modalità operative di svolgimento delle attività a rischio e dei controlli a presidio delle stesse.

Il Consiglio di Amministrazione della Società prende decisioni relativamente all'attuazione del Modello, mediante valutazione ed approvazione delle azioni necessarie per l'implementazione degli elementi costitutivi dello stesso.

2.2 Gli obiettivi e le finalità perseguiti con l'adozione e il conseguente aggiornamento del Modello organizzativo di Huawei Technologies Italia S.r.l.

Con l'adozione del Modello di Organizzazione, Gestione e Controllo e con il conseguente aggiornamento la Società si propone di:

- rendere consapevoli tutti coloro che lavorano in nome e per conto della Società, con particolare riferimento a coloro che operano nelle c.d. "aree sensibili", di poter incorrere, in caso di violazioni delle disposizioni riportate nel Modello, nella commissione di illeciti passibili di sanzioni penali nei loro stessi confronti, e di sanzioni "amministrative" irrogabili alla Società;

- rendere consapevoli tali soggetti che i comportamenti illeciti sono condannati con forza dalla Società, in quanto gli stessi sono sempre e comunque contrari alle disposizioni di legge, alla cultura aziendale ed ai principi etici assunti come proprie linee guida nell'attività d'impresa;

- consentire alla Società di intervenire tempestivamente per prevenire o contrastare la commissione di reati o quanto meno di ridurre sensibilmente il danno dagli stessi arrecato;

- migliorare la *governance* societaria e l'immagine della Società.

La predisposizione del presente Modello è ispirata alle Linee Guida emanate da **Confindustria** nel marzo 2002 e da ultimo aggiornate nel marzo 2014.

2.3 I "Destinatari" del Modello organizzativo di Huawei Technologies Italia S.r.l.

I principi e le disposizioni del presente documento devono essere rispettate da:

- componenti del Consiglio di Amministrazione, del Collegio Sindacale e Revisore Legale dei Conti;

- Dirigenti;

- Dipendenti;

- Consulenti, Collaboratori, Fornitori, Agenti ed eventuali *Partners* nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle quali sia ipotizzabile la commissione di uno dei reati presupposto di cui al Decreto;

- nonché da quanti agiscono sotto la direzione o la vigilanza dei vertici aziendali nell'ambito dei compiti e delle funzioni assegnate.

I soggetti così individuati sono, di seguito, definiti "Destinatari".

2.4 La costruzione e il conseguente aggiornamento del Modello organizzativo di Huawei Technologies Italia S.r.l.

L'attività di lavoro finalizzata alla predisposizione del presente Modello ed al suo conseguente aggiornamento ha tenuto conto delle esigenze previste dal Decreto (art. 6 comma 2) e, segnatamente, la Società ha proceduto a:

a. "individuare le attività nel cui ambito possono essere commessi i reati"

A tal fine, la Società ha:

- identificato i settori/attività/aree sensibili, con riferimento ai reati richiamati dal Decreto attraverso l'analisi dei documenti aziendali resi disponibili dalla Società (a titolo esemplificativo: statuto, visura camerale, verbali degli organi societari, ecc.);

- analizzato i settori/attività/aree sensibili, con prefigurazione delle modalità e degli strumenti attraverso i quali sarebbe possibile commettere i reati elencati nel Decreto da parte dell'impresa, dai suoi organi amministrativi, dai dipendenti ed, in generale, dalle figure contemplate dall'art. 5 del Decreto (anche attraverso incontri e colloqui con i soggetti interessati);

- individuato delle regole interne e dei protocolli esistenti – siano essi formalizzati o meno – in riferimento alle sole aree individuate come a rischio di reato.

b. "prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire"

Con riguardo a tale esigenza sono stati previsti protocolli sia di carattere generale che protocolli specifici nelle singole Parti Speciali del Modello organizzativo societario.

c. "individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati"

In relazione a tale esigenza sono stati previsti protocolli specifici alla sezione "*Gestione dei flussi finanziari e dei rapporti* intercompany" di cui alla Parte Speciale A del presente Modello organizzativo societario.

d. "prevedere obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli"

Relativamente a tale esigenza, sono stati previsti specifici flussi informativi distinti in "informazioni" e "*Segnalazioni*" oltre che *report* da inviare periodicamente all'Organismo di Vigilanza.

e. "introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello"

Con riferimento a tale esigenza è stato introdotto lo specifico sistema sanzionatorio sotto enucleato.

2.6 La struttura del Modello organizzativo di Huawei Technologies Italia S.r.l.

Il Modello si compone di una Parte Generale e delle seguenti Parti Speciali finalizzate al presidio delle attività a rischio precedentemente individuate:

- **Parte Speciale A**: Reati contro la Pubblica Amministrazione e il suo patrimonio, Reato di corruzione fra privati e Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria;
- **Parte Speciale B**: Delitti informatici e trattamento illecito di dati e Reati in materia di violazione del diritto d'autore;
- **Parte Speciale C:** Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio, Delitti di criminalità organizzata e Delitti con finalità di terrorismo o di eversione dell'ordine democratico;
- **Parte Speciale D:** Reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento;
- **Parte Speciale E:** Delitti contro l'industria e il commercio;
- **Parte Speciale F:** Reati societari;
- **Parte Speciale G:** Delitti di omicidio colposo e lesioni personali gravi o gravissime commesse con violazione delle norme a tutela della salute e sicurezza sui luoghi di lavoro;
- **Parte Speciale H**: Reati ambientali;
- **Parte Speciale I**: Delitti contro la personalità individuale e Delitto di impiego di cittadini di stati terzi il cui soggiorno è irregolare.

I profili di rischio inerenti i delitti di pratiche di mutilazione degli organi genitali femminili ed i reati di abuso di mercato, si reputano complessivamente presidiati dalle disposizioni di cui al Business Code of Conduct e dai presidi generali di cui al Modello organizzativo della Società.

2.7 I rapporti con le Società del Gruppo

Huawei Technologies Italia S.r.l. riceve ed eroga servizi a Società del Gruppo, aventi sede legale all'estero, che possono interessare attività ed operazioni a rischio di cui alle Parti Speciali del presente Modello.

In particolare i rapporti *intercompany* riguardano le seguenti attività:

- acquisto a livello locale dei prodotti Huawei;
- servizi di ricerca e sviluppo erogati da Huawei Technologies Italia S.r.l. a favore delle altre società del Gruppo;
- servizi di gestione di clienti globali tramite Key Account Department stabiliti a livello locale.

Le prestazioni di servizi:

- avvengono in conformità a quanto previsto dal Business Code of Conduct e dal Modello adottati dalla Società;
- devono essere disciplinate da apposito accordo scritto, comunicato all'Organismo di Vigilanza della Società.

3. L'Organismo di Vigilanza di Huawei Technologies Italia S.r.l.

La Società ha attribuito il compito di vigilare sul funzionamento e sull'osservanza dello stesso all'**Organismo di Vigilanza** (anche "OdV"), dotato dei requisiti di seguito indicati e volto ad assicurare un'effettiva ed efficace attuazione del Modello.

3.1 I requisiti dell'Organismo di Vigilanza di Huawei Technologies Italia S.r.l.

I componenti dell'Organismo di Vigilanza devono essere dotati dei requisiti dettati dalle Linee Guida Confindustria. In particolare:

AUTONOMIA E INDIPENDENZA: l'Organismo deve restare estraneo ad ogni forma di interferenza e pressione da parte dei vertici operativi e non essere in alcun modo coinvolto nell'esercizio di attività operative e decisioni gestorie. L'Organismo di Vigilanza non deve trovarsi in situazione di conflitto di interesse e non devono essere attribuiti all'Organismo nel suo complesso, ma anche ai singoli componenti, compiti operativi che ne possano minare l'autonomia.

Il requisito dell'autonomia e dell'indipendenza deve intendersi anche quale assenza di legami parentali e vincoli di dipendenza gerarchica con il vertice della Società o con soggetti titolari di poteri operativi all'interno della stessa.

L'Organismo di Vigilanza deve riportare al massimo vertice operativo aziendale e con questo deve poter dialogare "alla pari".

PROFESSIONALITÀ: ovvero possesso del bagaglio di strumenti e tecniche necessari per lo svolgimento concreto ed efficace dell'attività assegnata. La professionalità e l'autorevolezza dell'Organismo sono poi connesse alle sue esperienze professionali. In tal senso, la Società ritiene di particolare rilevanza l'attento esame dei *curricula* dei possibili candidati, e le precedenti esperienze, privilegiando profili che abbiano maturato una specifica professionalità in materia.

CONTINUITÀ D'AZIONE: l'OdV svolge in modo continuativo le attività necessarie per la vigilanza del Modello con adeguato impegno e con i necessari poteri di indagine, riunendosi con cadenza almeno trimestrale.

ONORABILITÀ: in relazione alla previsione di cause di ineleggibilità, revoca, sospensione o decadenza dalla funzione di Organismo di Vigilanza come di seguito specificate.

La Società, conformemente alle prescrizioni normative contenute nel Decreto, si è orientata nella scelta di un Organismo collegiale, composto da tre a cinque membri

per la maggioranza esterni alla Società; l'OdV provvede alla nomina di un Presidente, tra i componenti esterni, che viene comunicato al CdA.

I requisiti sopra descritti devono essere verificati in sede di nomina da parte del Consiglio di Amministrazione.

3.2 Le cause di ineleggibilità, revoca, sospensione e decadenza

Nel nominare i componenti dell'Organismo di Vigilanza, il Consiglio di Amministrazione della Società ha espressamente stabilito le seguenti cause di **ineleggibilità** per i medesimi membri dell'OdV.

Non possono dunque essere eletti:

- coloro i quali siano stati condannati con sentenza ancorché non definitiva, o con sentenza di applicazione della pena su richiesta (cd. patteggiamento) e anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:

1. alla reclusione per un tempo non inferiore ad un anno per uno dei delitti previsti dal regio decreto 16 marzo 1942, n. 267;

2. a pena detentiva per un tempo non inferiore ad un anno per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;

3. alla reclusione per un tempo non inferiore ad un anno per un delitto contro la pubblica amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica, per un delitto in materia tributaria;

4. per un qualunque delitto non colposo alla pena della reclusione per un tempo non inferiore a due anni;

5. per uno dei reati previsti dal titolo XI del libro V del codice civile così come riformulato del Decreto Legislativo 11 aprile 2002, n. 61;

6. per un reato che importi e abbia importato la condanna ad una pena da cui derivi l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;

7. per uno o più reati tra quelli tassativamente previsti dal Decreto, anche se con condanne a pene inferiori a quelle indicate ai punti precedenti;

8. coloro nei cui confronti sia stata applicata in via definitiva una delle misure di prevenzione previste dall'art. 10, comma 3, della legge 31 maggio 1965, n. 575, come sostituito dall'articolo 3 della legge 19 marzo 1990, n. 55 e successive modificazioni;

9. coloro nei cui confronti siano state applicate le sanzioni amministrative accessorie previste dall'art. 187-quater Decreto Legislativo 24 febbraio 1998, n. 58.

I componenti dell'Organismo di Vigilanza devono autocertificare con dichiarazione sostitutiva di notorietà di non trovarsi in alcuna delle condizioni suindicate, impegnandosi espressamente a comunicare eventuali variazioni rispetto al contenuto di tali dichiarazioni.

L'eventuale revoca dei componenti dell'Organismo dovrà essere deliberata dal Consiglio di Amministrazione della Società e potrà esclusivamente disporsi per ragioni connesse a gravi inadempimenti rispetto al mandato assunto, ivi comprese le violazioni degli obblighi di riservatezza di seguito indicati, oltre che per le intervenute cause di decadenza di seguito riportate.

I componenti dell'Organismo di Vigilanza **decadono** inoltre dalla carica nel momento in cui successivamente alla loro nomina:

- siano condannati con sentenza definitiva o di patteggiamento per uno dei reati indicati ai numeri 1, 2, 3, 4, 5, 6 e 7 delle condizioni di ineleggibilità innanzi indicate;

- allorquando abbiano violato gli obblighi di riservatezza strettamente connessi allo svolgimento del loro incarico.

I componenti dell'Organismo di Vigilanza sono inoltre sospesi dall'esercizio delle funzioni nelle ipotesi di:

- condanna con sentenza non definitiva per uno dei reati indicati nei numeri da 1 a 7 delle condizioni di ineleggibilità innanzi indicate;

- applicazione su richiesta delle parti di una delle pene di cui ai numeri da 1 a 7 delle condizioni di ineleggibilità innanzi indicate;

- applicazione di una misura cautelare personale;

- applicazione provvisoria di una delle misure di prevenzione previste dall'art. 10, comma 3, della legge 31 maggio 1965, n. 575, come sostituito dall'articolo 3 della legge 19 marzo 1990, n. 55 e successive modificazioni.

L'Organismo di Vigilanza dura in carica tre anni, decade con la data di approvazione del bilancio relativo al terzo anno di esercizio ed è rieleggibile. La retribuzione dell'Organismo viene determinata dal CdA all'atto della nomina per l'intero periodo di durata dell'ufficio.

3.3 I compiti e i poteri dell'Organismo di Vigilanza di Huawei Technologies Italia S.r.l.

L'OdV, quale organo collegiale, dispone di autonomi poteri di iniziativa e controllo, che si estendono a tutti i settori e funzioni della Società, poteri che devono essere esercitati al fine di svolgere efficacemente e tempestivamente le funzioni previste nel Modello e dalle norme di attuazione del medesimo.

Per lo svolgimento dei propri compiti il Consiglio di Amministrazione attribuisce all'Organismo di Vigilanza un *budget* di spesa annuo. Tuttavia, l'Organismo di Vigilanza può autonomamente impegnare risorse che eccedano i propri poteri di spesa, nel rispetto delle procedure aziendali, qualora l'impiego delle stesse sia necessario per fronteggiare situazioni eccezionali e urgenti. In questi casi l'Organismo deve informarne senza ritardo il Consiglio di Amministrazione.

L'Organismo di Vigilanza per l'espletamento dei compiti ad esso demandati si avvale di tutte le funzioni aziendali.

L'Organismo di Vigilanza svolge le seguenti attività di:

- vigilanza sull'effettività del Modello, verificando in particolare la coerenza tra il Modello medesimo e le concrete regole adottate nelle aree a rischio;

- verifica periodica che il Modello sia rispettato da parte di tutte le singole unità/aree aziendali a rischio, al fine di accertare che le regole definite ed i presidi approntati siano seguiti nel modo più fedele possibile e risultino in concreto idonei a prevenire i rischi della commissione dei reati evidenziati;

- vigilanza affinché il Business Code of Conduct e tutte le disposizioni in esso contenute siano rispettate da tutti i soggetti a qualsiasi titolo operanti nella Società;

- segnalazione al Consiglio di Amministrazione degli eventuali aggiornamenti ed adeguamenti del Modello in conformità alle evoluzioni della legge e della giurisprudenza, oltre che in conseguenza di modifiche intervenute all'organizzazione aziendale;

- vigilanza sul corretto funzionamento delle attività di controllo per ciascuna area a rischio, segnalando tempestivamente anomalie e disfunzioni del Modello, previo confronto con le aree/funzioni interessate;

- valutazione e proposta di irrogazione di eventuali sanzioni disciplinari, previo il necessario coordinamento con i responsabili delle competenti funzioni/aree aziendali.

Nello svolgimento delle proprie attività di indagine, analisi e controllo, l'Organismo di Vigilanza ha accesso senza limitazioni alle informazioni aziendali. Qualunque funzione aziendale, dipendente e/o componente degli organi sociali, a fronte di richieste da parte dell'Organismo di Vigilanza, o al verificarsi di eventi o circostanze rilevanti, è, pertanto, tenuta all'obbligo di collaborazione ed informazione.

3.4 L'attività di *reporting* dell'Organismo di Vigilanza di Huawei Technologies Italia S.r.l.

Al fine di garantire la sua piena autonomia e indipendenza nello svolgimento delle proprie funzioni, l'Organismo di Vigilanza riporta direttamente al Consiglio di Amministrazione della Società e riferisce in merito all'attuazione del Modello ed all'emersione di eventuali criticità attraverso due linee di *reporting:*

1. la prima su **base continuativa**;

2. la seconda a **cadenza annuale**, attraverso una relazione scritta che dovrà indicare con puntualità l'attività svolta nel periodo, sia in termini di controlli effettuati e degli esiti ottenuti che in ordine alle eventuali necessità di aggiornamento del Modello.

L'OdV deve, altresì, predisporre annualmente un piano di attività previste per l'anno successivo, in cui si individuano le attività da svolgere e le aree che saranno oggetto di verifiche, oltre alle tempistiche e alla priorità degli interventi.

L'Organismo di Vigilanza può, comunque, effettuare, nell'ambito delle attività aziendali sensibili e qualora lo ritenga necessario ai fini dell'espletamento delle proprie funzioni, controlli non previsti nel piano di intervento (cosiddetti "controlli a sorpresa").

L'Organismo potrà chiedere di essere sentito dal Consiglio di Amministrazione ogniqualvolta ritenga opportuno interloquire con detto organo; del pari, all'OdV è riconosciuta la possibilità di chiedere chiarimenti ed informazioni al Consiglio di Amministrazione.

D'altra parte, l'Organismo di Vigilanza potrà essere convocato in ogni momento dal Consiglio di Amministrazione per riferire su particolari eventi o situazioni inerenti al funzionamento ed al rispetto del Modello.

I predetti incontri devono essere verbalizzati e copia dei verbali deve essere custodita dall'OdV (nonché dagli organismi di volta in volta coinvolti).

3.5 Obblighi di informativa nei confronti dell'OdV di Huawei Technologies Italia S.r.l.

L'OdV è destinatario di qualsiasi informazione, documentazione e/o comunicazione, proveniente anche da terzi attinente il rispetto del Modello.

Tutti i Destinatari del presente Modello sono tenuti ad un obbligo di informativa verso l'Organismo di Vigilanza, da svolgersi a seguito di:

i) segnalazioni;

ii) informazioni.

L'Organismo di Vigilanza assicura la **massima riservatezza** in ordine a qualsiasi notizia, informazione, segnalazione, **a pena di revoca del mandato e delle misure disciplinari di seguito definite**, fatte salve le esigenze inerenti lo svolgimento delle indagini nell'ipotesi in cui sia necessario il supporto di consulenti esterni all'OdV o di altre strutture societarie.

Ogni informazione e segnalazione di cui al presente Modello è conservata dall'Organismo di Vigilanza in un apposito archivio informatico e cartaceo, in conformità alle disposizioni contenute nel Decreto Legislativo 30 giugno 2003, n. 196 (*Privacy*): gli atti dell'Organismo di Vigilanza devono essere conservati presso gli uffici della Società e contenuti in armadi separati e chiusi, accessibili ai suoi soli componenti e per le sole ragioni connesse all'espletamento dei compiti innanzi rappresentati, a pena di decadenza immediata dall'ufficio.

i) Le segnalazioni

Tutti i Destinatari sono tenuti a segnalare prontamente all'Organismo di Vigilanza di Huawei Technologies Italia S.r.l. ogni deroga, violazione o sospetto di violazione di propria conoscenza di norme comportamentali di cui al Business Code of Conduct della Società nonché dei principi di comportamento e delle modalità esecutive di svolgimento delle attività identificate "a rischio" e disciplinate nel Modello.

Le segnalazioni, qualora indirizzate all'Organismo di Vigilanza di Huawei Technologies Italia S.r.l., possono essere effettuate, anche in forma anonima, sia a mezzo di posta fisica all'indirizzo:

Organismo di Vigilanza di Huawei Technologies Italia S.r.l.

Via Lorenteggio, 257 – 20152 Milano

che di posta elettronica all'indirizzo:

231whistleblowing@huaweipec.it

L'Organismo di Vigilanza valuta tutte le segnalazioni ricevute e intraprende le conseguenti iniziative a sua ragionevole discrezione e responsabilità nell'ambito delle proprie competenze, ascoltando eventualmente l'autore della segnalazione ed il responsabile della presunta violazione. Ogni conseguente decisione sarà motivata; gli eventuali provvedimenti conseguenti saranno applicati in conformità a quanto previsto al capitolo sul Sistema Disciplinare.

L'Organismo agisce in modo da garantire gli autori delle segnalazioni contro qualsiasi forma di ritorsione, discriminazione, penalizzazione o qualsivoglia conseguenza derivante dalle stesse, assicurando loro la riservatezza circa l'identità, fatti comunque salvi gli obblighi di legge e la tutela dei diritti di Huawei o delle persone accusate erroneamente o in mala fede.

ii) Le informazioni

L'Organismo di Vigilanza stabilisce nella propria attività di controllo la documentazione che, su base periodica, deve essere sottoposta alla sua attenzione.

All'Organismo di Vigilanza debbono essere obbligatoriamente trasmessi:

- 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 le fattispecie di reato previste dal Decreto, riguardanti la Società;

- in via periodica, visite, ispezioni ed accertamenti avviati da parte degli enti competenti (regioni, enti regionali ed enti locali) e, alla loro conclusione, eventuali rilievi e sanzioni comminate;

- richieste di assistenza legale avanzate dai soggetti interni alla Società, in caso di avvio di un procedimento giudiziario per uno dei reati previsti dal Decreto;

- rapporti predisposti dalle strutture aziendali nell'ambito della loro attività di controllo, dai quali emergano elementi di criticità rispetto alle norme del Decreto;

- in via periodica, informativa da parte del Collegio Sindacale e della Società di Revisione, in merito all'esito delle attività di propria competenza;

- in via periodica, notizie relative all'effettiva attuazione del Modello in tutte le aree/funzioni aziendali a rischio;

- in via periodica, notizie relative all'effettivo rispetto del Business Code of Conduct a tutti i livelli aziendali;

- informazioni sull'evoluzione delle attività attinenti le aree a rischio;

- il sistema delle deleghe e delle procure adottato dalla Società.

In caso di informazioni e/o notizie, anche ufficiose, relative alla commissione dei reati previsti dal Decreto o comunque riguardanti possibili violazioni del Modello e del Business Code of Conduct, ciascuno deve rivolgersi immediatamente all'OdV.

I flussi informativi debbono pervenire all'Organismo, mediante le modalità e gli indirizzi innanzi indicati.

4. Formazione ed informazione

4.1 Disposizioni generali

La Società intende garantire una corretta e completa conoscenza del Modello, del contenuto del Decreto e degli obblighi dallo stesso derivanti tra quanti operano per la Società.

A tal fine, l'attività di comunicazione e formazione, sviluppata a seconda dei Destinatari cui essa si rivolge e dei livelli e funzioni dagli stessi rivestite, è improntata ai principi di completezza, chiarezza, accessibilità e continuità al fine di consentire ai diversi Destinatari la piena consapevolezza di quelle disposizioni aziendali che sono tenuti a rispettare e delle norme etiche che devono ispirare i loro comportamenti.

Sessioni formative sono organizzate nel tempo dalla Società, in forza dei criteri di obbligatorietà e reiterazione, nonché di quello eventuale della diversificazione.

La formazione e l'informativa sono gestite dalla funzione Risorse Umane, coadiuvata dalla funzione Legale ed in coordinamento con l'Organismo di Vigilanza, in stretta collaborazione con i responsabili delle aree/funzioni coinvolte nell'applicazione del Modello. In particolare, la funzione Risorse Umane:

- inserisce, tra i criteri di selezione del personale, la condivisione dei valori espressi dal presente Modello e la predisposizione ad osservare gli stessi;
- diffonde la conoscenza del presente Modello attraverso i seguenti momenti formativi:
    - seminario iniziale (esteso annualmente a tutti i neoassunti), per i Responsabili e altri dipendenti con funzioni di rappresentanza o poteri di firma ad efficacia esterna;
    - informativa nella lettera di assunzione per i neo-assunti con obbligo per gli stessi, di sottoscrivere una dichiarazione di osservanza dei contenuti del Modello;
    - seminari di aggiornamento;
    - comunicazioni occasionali di aggiornamento in caso di necessità o urgenza, anche tramite collocazione di tali comunicazioni in apposita sezione del sito intranet aziendale.

La Società ha istituito una specifica sezione della *intranet* aziendale, dedicata al tema e aggiornata periodicamente, al fine di consentire ai soggetti interessati di conoscere in tempo reale eventuali modifiche, integrazioni o implementazioni del Business Code of Conduct e del Modello. Copia cartacea del Modello è altresì disponibile nelle bacheche aziendali e presso la funzione Legal.

4.2 Comunicazione iniziale

Il presente Modello è comunicato a tutte le risorse aziendali dall'Amministratore Delegato.

Tutti i Dipendenti e gli Apicali, all'atto dell'assunzione, sottoscrivono una dichiarazione di conoscenza ed accettazione del Modello e del Business Code of Conduct, di cui hanno a disposizione una copia cartacea o su supporto informatico.

Tutte le successive modifiche ed informazioni concernenti il Modello sono comunicate alle risorse aziendali attraverso i canali informativi ufficiali.

4.3 Formazione del personale

La **partecipazione alle attività formative** finalizzate a diffondere la conoscenza della normativa di cui al Decreto, del Modello di organizzazione, gestione e controllo, del Business Code of Conduct è da ritenersi **obbligatoria**. In particolare, ogni Dipendente ha l'obbligo di:

- acquisire consapevolezza dei contenuti del Modello e partecipare – con obbligo di frequenza – ai momenti formativi organizzati dalla Società;

- conoscere le modalità operative con le quali deve essere realizzata la propria attività;

- contribuire attivamente, in relazione al proprio ruolo e alle proprie responsabilità, all'efficace attuazione del Modello, segnalando eventuali carenze riscontrate nello stesso.

La formazione tiene conto, nei contenuti e nelle modalità di erogazione dei relativi corsi, della qualifica dei Destinatari, del livello di rischio dell'area in cui operano e dell'attribuzione o meno di funzioni di rappresentanza

L'assenza non giustificata alle sessioni formative è considerata illecito disciplinare, in accordo con quanto previsto dal Sistema Disciplinare di seguito enucleato.

Huawei prevede l'attuazione di corsi di formazione che illustrano, secondo un approccio modulare:

- il contesto normativo;
- il Business Code of Conduct, il Modello di Organizzazione, Gestione e Controllo adottato dalla Società e i contenuti del Sistema di Gestione HSE e ISMS;
- il ruolo dell'Organismo di Vigilanza ed i compiti ad esso assegnati dalla Società;
- le Parti Speciali del Modello, inclusive delle attività sensibili e dei relativi protocolli di controllo identificati.

Al termine di ciascuna sessione formativa è prevista una verifica del grado di apprendimento mediante erogazione di specifici test.

L'attività formativa viene erogata attraverso le seguenti modalità:

- sessioni in aula, con incontri dedicati o mediante l'introduzione di moduli specifici nell'ambito di altre sessioni formative, a seconda dei contenuti e dei destinatari di queste ultime;
- e-learning, destinato a tutti i dipendenti.

L'Organismo di Vigilanza cura che i programmi di formazione siano qualitativamente adeguati ed efficacemente attuati.

4.4 Informativa ai "Terzi Destinatari"

La Società impone la conoscenza e l'osservanza del Modello ai c.d. "Terzi Destinatari", quali Consulenti, Collaboratori, Fornitori, Agenti e *Partners* commerciali attraverso l'apposizione di specifiche clausole contrattuali.

5. Sistema Disciplinare

5.1 Profili generali

La previsione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle regole indicate nel Modello è condizione richiesta dal D.lgs. 231/2001 per l'esenzione della responsabilità amministrativa degli Enti e per garantire l'effettività del Modello medesimo.

Il sistema stesso è diretto a sanzionare il mancato rispetto dei principi ed obblighi di comportamento previsti nel presente Modello Organizzativo. L'irrogazione di sanzioni disciplinari per violazione dei principi e delle regole di comportamento indicati nel Modello Organizzativo prescinde dall'eventuale instaurazione di un procedimento penale e dall'esito del conseguente giudizio per la commissione di una delle condotte illecite previste dal Decreto.

A seguito della comunicazione all'OdV della violazione del Modello, viene avviata una procedura d'accertamento in conformità a quanto stabilito dal CCNL di riferimento del dipendente; tale procedura d'accertamento è condotta dagli organi sociali preposti all'irrogazione delle sanzioni disciplinari, tenuto conto della gravità del comportamento, della eventuale recidiva della mancanza o del grado della colpa.

Huawei, attraverso gli organi e le funzioni a ciò appositamente preposte, provvede quindi ad irrogare, con coerenza, imparzialità, ed uniformità, sanzioni proporzionate alle rispettive violazioni del Modello e conformi alle vigenti disposizioni in materia di regolamentazione dei rapporti di lavoro; le misure sanzionatorie per le diverse figure professionali sono di seguito indicate.

5.2 Le sanzioni nei confronti dei lavoratori dipendenti non Dirigenti

I comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali dedotte nel presente Modello, nel Business Code of Conduct, nelle regole e nei protocolli aziendali adottati dalla Società sono definiti illeciti disciplinari.

Le sanzioni irrogabili nei riguardi dei lavoratori dipendenti sono adottate nel rispetto delle procedure previste dalla normativa applicabile.

Si fa espresso riferimento alle categorie di fatti sanzionabili previste dall'apparato sanzionatorio esistente e cioè le norme pattizie di cui al Contratto Collettivo Nazionale per le imprese esercenti servizi di telecomunicazione (di seguito CCNL).

In applicazione del principio di proporzionalità, a seconda della gravità dell'infrazione commessa, sono previste le seguenti sanzioni disciplinari:

Richiamo verbale: si applica nel caso delle più lievi inosservanze dei principi e delle regole di comportamento previsti dal presente Modello, correlandosi detto comportamento ad una **lieve inosservanza** delle norme contrattuali o delle direttive ed istruzioni impartite dalla direzione o dai superiori. A titolo esemplificativo e non esaustivo, è punibile con il richiamo verbale il dipendente che, per negligenza, trascuri di conservare in maniera accurata la documentazione di supporto necessaria per ricostruire l'operatività della Società nelle aree a rischio 231

Ammonizione scritta: si applica in caso di recidiva delle infrazioni di cui al punto precedente.

Multa in misura non eccedente l'importo di 3 ore della retribuzione base: si applica in caso di inosservanza dei principi e delle regole di comportamento previste dal presente Modello, per un comportamento **non conforme o non adeguato** alle prescrizioni del Modello in misura tale da essere considerata di una certa gravità, anche se dipendente da recidiva. Tra tali comportamenti rientra la violazione degli obblighi di informazione nei confronti dell'Organismo in ordine alla commissione dei reati, ancorché tentati, nonché ogni violazione del Modello.

La stessa sanzione sarà applicata in caso di mancata reiterata partecipazione (fisica o in qualunque modo richiesta dalla Società), senza giustificato motivo alle sessioni formative che nel tempo verranno erogate dalla Società relative al D.lgs. 231/2001, al Modello di organizzazione, gestione e controllo e del Codice Etico adottato dalla Società o in ordine a tematiche relative.

Sospensione dal lavoro e dalla retribuzione fino ad un massimo di giorni 3: si applica nel caso di violazioni più gravi rispetto alle infrazioni di cui al punto precedente.

Licenziamento con o senza preavviso: si applica in caso di adozione di un **comportamento consapevole in contrasto con le prescrizioni** del presente Modello che, **ancorché sia solo suscettibile di configurare uno dei reati sanzionati** dal Decreto, **leda l'elemento fiduciario** che caratterizza il rapporto di lavoro ovvero risulti talmente grave da non consentirne la prosecuzione, neanche provvisoria. Tra le violazioni passibili della predetta sanzione rientrano i seguenti comportamenti intenzionali:

- redazione di documentazione incompleta o non veritiera (ad esempio, documenti indirizzati alla Pubblica Amministrazione, documenti contabili, ecc.);
- omessa redazione della documentazione prevista dal modello;

- violazione o elusione del sistema di controllo previsto dal modello in qualsiasi modo effettuata, incluse la sottrazione, distruzione o alterazione della documentazione inerente alla procedura, l'ostacolo ai controlli, l'impedimento di accesso alle informazioni e alla documentazione da parte dei soggetti preposti ai controlli o alle decisioni.

5.3 Le sanzioni nei confronti dei Dirigenti

La violazione dei principi e delle regole di comportamento contenute nel presente Modello da parte dei dirigenti, ovvero l'adozione di un **comportamento non conforme** alle richiamate prescrizioni sarà assoggettata a misura disciplinare modulata a seconda della gravità della violazione commessa. Per i casi più gravi è prevista la risoluzione del rapporto di lavoro, in considerazione dello speciale vincolo fiduciario che lega il dirigente al datore di lavoro.

Costituisce illecito disciplinare anche:

- la **mancata vigilanza** da parte del personale dirigente sulla corretta applicazione, da parte dei lavoratori gerarchicamente subordinati, delle regole previste dal Modello;

- la **violazione degli obblighi di informazione** nei confronti dell'Organismo di Vigilanza in ordine alla commissione dei reati rilevanti, ancorché tentata;

- la **violazione delle regole di condotta** ivi contenute da parte dei dirigenti stessi;

- **l'assunzione,** nell'espletamento delle rispettive mansioni, **di comportamenti** che **non** siano **conformi** a condotte ragionevolmente attese da parte di un dirigente, in relazione al ruolo rivestito ed al grado di autonomia riconosciuto.

5.4 Le sanzioni nei confronti dei componenti del Consiglio di Amministrazione e dei membri del Collegio Sindacale

Nei confronti degli Amministratori che abbiano commesso una violazione del presente Modello, il Consiglio di Amministrazione, prontamente informato dall'OdV, può applicare ogni idoneo provvedimento consentito dalla legge, fra cui le seguenti sanzioni, determinate a seconda della gravità del fatto e della colpa, nonché delle conseguenze che sono derivate:

- richiamo formale scritto;

- sanzione pecuniaria pari all'importo **da due a cinque volte** gli emolumenti calcolati su base mensile;

- revoca, totale o parziale, delle eventuali procure.

Il Consiglio di Amministrazione, qualora si tratti di violazioni tali da integrare giusta causa di revoca, propone all'Assemblea l'adozione dei provvedimenti di competenza e provvede agli ulteriori incombenti previsti dalla legge.

In caso di violazione da parte di un componente del Collegio Sindacale, l'OdV deve darne immediata comunicazione al Presidente del Consiglio di Amministrazione, mediante relazione scritta. Il Presidente del Consiglio di Amministrazione, qualora si tratti di violazioni tali da integrare giusta causa di revoca, convoca l'Assemblea inoltrando preventivamente ai soci la relazione dell'Organismo di Vigilanza. L'adozione del provvedimento conseguente la predetta violazione spetta comunque all'Assemblea.

5.5 Le sanzioni nei confronti dei "Terzi Destinatari"

Ogni violazione delle prescrizioni di cui al Modello da parte di Consulenti, Collaboratori, Fornitori ed eventuali *Partners* e da quanti siano di volta in volta contemplati tra i "Destinatari" dello stesso, è sanzionata dagli organi competenti in base alle regole societarie interne, secondo quanto previsto dalle clausole contrattuali inserite nei relativi contratti, ed in ogni caso con l'applicazione di penali convenzionali, che possono comprendere anche l'automatica risoluzione del contratto (ai sensi dell'art. 1456 c.c.), fatto salvo il risarcimento del danno.