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 02/02/2021

INDICE

Definizioni

Huawei Technologies Italia S.r.l.: la Società con sede a Milano, Via Lorenteggio, 240 - 20147, 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.

Reati: i reati per i quali è applicabile la disciplina prevista dal D. Lgs. 231/2001;

Attività Sensibili: attività di Huawei Technologies Italia s.r.l. nel cui ambito ricorre il rischio di commissione dei reati per i quali è applicabile la disciplina prevista dal D. Lgs. 231/2001;

Area di rischio: area/settore aziendale a rischio di commissione dei reati per i quali è applicabile la disciplina prevista dal D. Lgs. 231/2001;

Sistemi di controllo: sistema di controllo predisposto dalla società al fine di prevenire, attraverso l'adozione di appositi protocolli, i rischi di commissione dei reati per i quali è applicabile la disciplina prevista dal D. Lgs. 231/2001;

Linee Guida Confindustria: le Linee Guida emanate da Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. 231/2001, approvate dal Ministero della Giustizia in data 24 maggio 2004 e successivi aggiornamenti.

***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*:** tutti coloro che operano per il conseguimento dello scopo e degli obiettivi di Huawei Technologies Italia s.r.l. Fra i Destinatari del Modello sono annoverati i componenti dell'Organo Amministrativo e il Sindaci, i Dipendenti (ivi inclusi i Dirigenti) anche se distaccati, i Partners e, in generale, tutti coloro che operano in nome e/o per conto della Società.

***Dipendenti*:** tutti i soggetti che intrattengono un rapporto di lavoro subordinato, di qualsivoglia natura, con la Società.

***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 Investmente & Holding Co. Ltd con sede a Shenzhen (Cina).

***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 o Huawei*:** Huawei Technologies Italia S.r.l. con sede legale a Milano, Via Lorenteggio, 240 - 20147.

Premessa

Huawei Technologies Italia S.r.l.

Huawei Technologies Italia S.r.l. 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 di dati, di tecniche di sviluppo e di implementazione di sistemi (*"system integration"*) di computer ed apparecchiature accessorie, nonché 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 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;

- l'importazione, l'esportazione, l'acquisto e la vendita, il noleggio, la commercializzazione e la distribuzione anche per corrispondenza ovvero tramite commercio elettronico, via internet o qualsiasi altro mezzo telematico di qualsiasi tipo di materiale elettrico, incluso, ma non limitato a inverter, moduli fotovoltaici, stazione di trasformazione, interruttori elettrici, batterie, dispositivi smart di ricarica e modulo, ottimizzatore, smart logger, smart p.v. kit (ac box, ecc.), smart acu, ppc (power plant controller) software associato (sistema di gestione, rete eco, scada, ecc.) e relativi prodotti ausiliari (accessori, staffa, cavo, emi (strumento per monitoraggio ambientale), ecc.) incluso il software associato e tutte le attività correlate, nonchè l'installazione, test, formazione, manutenzione, support tecnico, consulenza, servizi tecnici, integrazione del sistema e soluzioni e altri servizi relativi al prodotto;

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.

Huawei è articolata come di seguito riportato:

- CNBG che si occupa di fornire prodotti e servizi ai lavoratori licenziatari;
- EBG che si rivolge a clienti B2B di varie dimensioni e tipologie (es. multinazionali, grosse aziende, pubblica amministrazione, istituti bancari/finanziari). La BG Solar Power, sebbene formalmente sia un BG separata, per le esigue dimensioni viene attualmente considerata sotto EBG;
- CBG che si occupa di fornire prodotti e assistenza post-vendita di prodotti elettronici B2C (telefoni, pc, altro) anche attraverso una rete di esercizi commerciali convenzionati;
- R&D che si occupa di attività di ricerca e sviluppo
- Funzioni di PLATFORM, che, per quanto di competenza, forniscono servizi di supporto alle unità di business;

La sede legale societaria è sita in Milano, via Lorenteggio, 240; 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 Investmente & 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.

È 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 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 dal General Manager 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 & Corruption program** –sistema documentale che prevede una serie di policy e procedure atte a garantire la conformità alle leggi applicabili in tema di corruzione (tra cui a titolo esemplificativo ma non esaustivo rientrano il D.Lgs. 231/2001, la L. 190/2012, il D.Lgs 28/2017). Tra le procedure rilevanti del program si riportano, a titolo esemplificativo, l'Anti-Bribery & Corruption Policy, "Code of Conduct for Partners of Huawei Italy" "Internal Control & Audit Guideline; Gift and Hospitality Policy; Staff expenses Claim Management; Staff working guidelines; Anticorruption and compliance commitment; Internal Control &Audit Management Guidelines; whistleblowing policy.

- **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*.

A titolo esemplificativo si riportano: il Senior Decision Team (c.d. "SDT") che si occupa dell'approvazione delle offerte, dei progetti e dei contratti sulla base delle indicazioni fornite da quattro moduli funzionali aziendali; la Compliance Committee e il Compliance Supervisory Board per la regolamentazione ed il monitoraggio della Compliance interna;

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 ("*Enviromental Management System*").

- alla norma ISO 45001 ("Occupational health and safety management systems -- Requirements with guidance for use")

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.

Le seguenti aree di business hanno 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: CBG, EBG.

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 practice in materia di anticorruzione in tutti i paesi nei quali opera.

Tutti i destinatari sono tenuti a 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:

BCG Complain e Whistleblowing.

Huawei ha adottato una Procedura Whistleblowing[1] e ha messo a disposizione un canale di comunicazione riservato attraverso il quale tutti i Destinatari possono segnalare, anche in forma anonima, qualsiasi condotta o presunta condotta rilevante ai sensi del D. Lgs. n. 231/2001.

Inoltre, anche in un'ottica di integrazione con altri strumenti adottati a livello di Gruppo potrà essere utilizzato il canale di comunicazione ("BCG Complain") attraverso il quale tutti i Dipendenti possono segnalare eventuali violazioni o presunte violazioni del Business Code of Conduct, dell'Anti-bribery policy e della Gift and Hospitality Policy.

[1] La procedura è consultabile al seguente link http://w3.huawei.com/info/en/doc/viewDoc.do?did=3911903&cata=185683

Per il coordinamento e l'integrazione tra i due canali di comunicazione si rinvia a quanto riportato nella procedura Whistleblowing.

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

Un'organizzazione chiara e 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;
- una descrizione delle posizioni organizzative e del relativo contenuto lavorativo (*job description*);
- un sistema delle deleghe e delle procure.

La responsabilità della predisposizione e dell'aggiornamento dei documenti organizzativi è attribuita al Dipartimento HR, il 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, HSE Manager).

In questo modo, la Società ha previsto una propria articolazione di Dipartimenti 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.

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:

- 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 e/o Regional, in inglese, che devono essere adottate così come definite da Casa madre 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.

I file delle policies sono classificati e gestiti per aree di business al fine di raggiungere i seguenti obiettivi:

1. semplificare le policies sulla base della categoria e del livello di business, chiarire cosa risulta mancante, assicurare chiarezza ed evitare ripetizioni e contrasti;

2. eseguire una chiara delimitazione del confine del business e chiarire la responsabilità di una policy;

3. Ricercare e utilizzare le policies in una dimensione di business in modo tale da supportare una corretta esecuzione delle policies e il rispetto delle stesse.

La categorizzazione delle policies per aree di business è svolta secondo I seguenti principi:

1. Fare riferimento alla principale "industry practice";

2. Evitare un frequente mutamento della categorizzazione e dei file relativi alle policies dovuto al riassetto organizzativo;

3. Il livello di business e la categorizzazione siano chiari e coerenti con la realtà;

4. Categorizzare adeguatamente le policies in base a numeri per andare incontro alle esigenze di gestione;

5. Il dipartimento di gestione della industry è responsabile per definire e ottimizzare la categorizzazione, così che tutti i dipartimenti la adottino e la seguano;

6. Se i dipartimenti entrano in contrasto in merito alla categorizzazione, il dipartimento di gestione della industry dirime tali contrasti in contraddittorio.

I documenti riguardanti le policies sono controllati a diversi livelli. Ogni livello è strutturato con quattro ruoli: (i) "document control owner", (ii) "document control rappresentative", (iii) "document controller", (iv) "document administrator".

Tutto il sistema procedurale viene diffuso attraverso i canali di comunicazione interni – in particolare, le procedure vengono trasmesse, in lingua inglese e cinese, a tutto lo staff a mezzo di e-mail - ed è a disposizione di tutti i dipendenti in specifiche sezioni della intranet aziendale denominata BMS. 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 Introduzione

Il Decreto Legislativo 231/2001 ha introdotto in Italia, in attuazione della legge delega 29 settembre 2000, n. 300, la responsabilità amministrativa degli enti ovvero la responsabilità "autonoma" dell'ente, in sede penale, rispetto alla responsabilità della persona fisica che ha commesso il reato.

Per una più ampia trattazione del D.Lgs. 231/2001 si rinvia all'Appendice A.

1.2 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.

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

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

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

b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;

c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;

d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate".

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

L'efficace attuazione del Modello, inoltre, richiede:

a) una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;

b) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

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 gennaio 2018 e successivamente in data 2/02/2021.

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;

- commissione dei reati richiamati dal D.Lgs. n. 231/2001 da parte dei destinatari delle previsioni del Modello o, più in generale, 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;
- identificazione di nuove attività sensibili, o variazione di quelle precedentemente identificate, anche eventualmente connesse all'avvio di nuove attività;
- riscontro di carenze e/o lacune nelle previsioni del Modello a seguito di verifiche sull'efficacia del medesimo.

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.

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

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.

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

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

Il Modello si applica altresì, nei limiti del rapporto in essere, a coloro i quali, pur non appartenendo alla Società, operano su mandato o per conto della stessa o sono comunque legati alla Società da rapporti giuridici rilevanti.

In particolare, con riferimento ad eventuali partners, in Italia e all'estero, con cui la Società può operare, pur nel rispetto dell'autonomia delle singole entità giuridiche, la Società si adopererà, attraverso la previsione di specifiche clausole contrattuali, per garantire che gli stessi uniformino la propria condotta ai principi posti dal Decreto e sanciti nel Modello adottato dalla Società.

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

La Società ha deciso di procedere alla predisposizione e adozione del Modello di organizzazione, gestione e controllo ex D.Lgs. 231/2001 in quanto consapevole che tale sistema, rappresenta un'opportunità per rafforzare la sua cultura di governance, cogliendo al contempo l'occasione dell'attività svolta (inventariazione delle Attività Sensibili, analisi dei rischi potenziali, valutazione e adeguamento del sistema dei controlli già esistenti sulle Attività Sensibili) per sensibilizzare le risorse impiegate rispetto ai temi del controllo dei processi, finalizzati a una prevenzione "attiva" dei Reati.

Nel 2020 la Società ha avviato un progetto interno (di seguito il Progetto) finalizzato a garantire l'aggiornamento del Modello in conseguenza delle modifiche normative che hanno interessato il catalogo dei reati presupposto e delle modifiche organizzative intervenute all'interno della stessa.

I principali elementi di innovazione apportati dal Progetto sono:

- l'aggiornamento delle previsioni di cui al D.Lgs. n. 231/2001 alla luce dell'evoluzione normativa, sia con riferimento all'ampliamento del catalogo dei reati presupposto sia con riferimento alle disposizioni introdotte dalla L. n. 179/2017 in materia whistleblowing;

- la ridefinizione dell'approccio metodologico operativo secondo una logica per processo che ha condotto alla stesura di un'unica Parte Speciale riferita a tutte le categorie di reati presupposto del D.Lgs. n. 231/2001 ritenute rilevanti per la Società. Tale approccio metodologico è stato adottato al fine di dotare i Destinatari di uno strumento più facilmente consultabile e conseguentemente agevolarne l'efficace attuazione.

2.5. La metodologia nell'attività di risk assessment

L'approccio operativo e metodologico del Progetto ha compreso:

- l'individuazione delle aree di rischio e delle attività sensibili;

- l'individuazione dei meccanismi correttivi attraverso l'analisi di comparazione della situazione esistente rispetto a quella prospettata nel Modello;
- modalità di adeguamento e aggiornamento del Modello.

Le fasi in cui si è articolato il processo di mappatura del rischio sono svolte attraverso analisi documentali e incontri con i responsabili delle strutture e sono:

- individuazione dei processi a rischio;
- individuazione della fattispecie di reato astrattamente applicabile;
- definizione del rischio inerente;
- individuazione dei controlli esistenti;
- definizione del rischio residuo;
- individuazione delle eventuali aree di miglioramento.

Il rischio è stato analizzato sulla base di due componenti fondamentali, che ne consentono una valutazione e orientano le attività di mitigazione del rischio da porre in essere:

- la probabilità che l'illecito possa effettivamente verificarsi;
- le conseguenze e l'impatto dell'evento;

dalla connessione delle quali emerge l'esposizione al rischio, rappresentata dall'interrelazione tra la probabilità che il rischio si concretizzi e il suo impatto potenziale sulla società.

La valutazione del rischio è stata mossa dall'individuazione di due tipologie di rischio:

- inerente: calcolato ipotizzando la totale assenza di controlli;
- residuale: calcolato in base all'esistenza dei controlli rilevati durante il risk assessment.

La valutazione dell'adeguatezza del sistema di controllo interno esistente è stata esaminata in relazione al livello auspicabile e ritenuto ottimale di efficacia ed efficienza di protocolli e standard di controllo e si sono presi, come riferimento:

- **standard di controllo generali** di trasparenza delle attività posti alla base degli strumenti e delle metodologie utilizzate per strutturare gli standard di

controllo specifici, che devono essere sempre presenti in tutte le Attività Sensibili prese in considerazione dal Modello, quali:

a. esistenza di procedure formalizzate;

b. tracciabilità e verificabilità ex post delle transazioni;

c. segregazione dei compiti o controlli alternativi di back-up;

d. esistenza di un sistema di deleghe e procure coerente con le responsabilità organizzative assegnate.

- **Standard di controllo specifici** applicabili a singole Attività Sensibili, elaborati sulla base degli standard di controllo generali sopra riportati, quali misure di presidio individuate per mitigare il rischio specifico di commissione del singolo reato/categoria di reato.

Il livello di rischio residuale è stato valutato al fine di implementare un sistema di prevenzione tale da poter essere eluso solo fraudolentemente che prenda in considerazione l'intensità e la pervasività dei controlli, al fine di evitare di non appesantire le attività operative attraverso l'istituzione di procedure eccessivamente rigide che avrebbero l'effetto di rallentarne il regolare svolgimento.

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

Il Modello è articolato nella presente "Parte Generale", che ne contiene i principi fondamentali e in una "Parte Speciale".

La Parte Generale, dopo aver fornito le "definizioni" dei principali istituti e concetti presi in considerazione nel Modello, illustra dapprima gli strumenti di governance, il sistema di controllo e l'assetto societario della Società,

Il presente documento, successivamente a quanto sopra citato, individua i principi generali, i criteri ed i presupposti per l'attribuzione della responsabilità amministrativa degli Enti (individuazione dei soggetti attivi del reato- presupposto; loro "legame" con l'Ente; concetti di "interesse" o "vantaggio" dell'Ente; catalogo dei reati-presupposto della responsabilità amministrativa degli Enti; etc.), per poi chiarire quali sono le condizioni per l'esonero della responsabilità amministrativa degli Enti.

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

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

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

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

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

- le Attività Sensibili, ovvero quelle attività presenti nella realtà aziendale nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati di cui al punto precedente;

- gli standard di controllo generali delle attività posti alla base degli strumenti e delle metodologie utilizzate per strutturare gli standard di controllo specifici, che devono essere sempre presenti in tutte le Attività Sensibili prese in considerazione dal Modello;

- gli standard di controllo specifici, applicabili a singole attività sensibili, elaborati sulla base degli standard di controllo generali sopra riportati, quali misure di presidio individuate per mitigare il rischio specifico di commissione del singolo reato/categoria di reato.

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.

A tal fine sono stati adottati i seguenti strumenti per la corretta gestione dei contratti infragruppo:

a. formale identificazione di ruoli aziendali responsabili della stesura/verifica dei contratti infragruppo;

b. esecuzione di verifiche formali e sostanziali sui flussi finanziari aziendali, con riferimento a pagamenti/operazioni infragruppo;

c. esistenza di apposti format per la predisposizione del contratto per l'identificazione dei servizi da erogare che prevedono, tra l'altro:

I. inserimento di clausole specifiche nell'ambito delle quali le società si impegnano, l'una nei confronti dell'altra, al rispetto più rigoroso dei propri Codici di Condotta e Modelli di compliance (ove adottati), che le parti dichiarano di ben conoscere e accettare;

II. applicazione di sanzioni (ivi inclusa l'eventuale risoluzione del contratto) in caso di violazioni alle suddette prescrizioni;

III. modalità per il controllo dell'adempimento delle parti e le modalità per la risoluzione dell'obbligazione.

IV. formale definizione degli obblighi e delle responsabilità della società mandante e della società mandataria;

d. monitoraggio e aggiornamento dei corrispettivi previsti nei contratti;

verifica preliminare circa l'insussistenza di conflitti di interesse nella gestione dei rapporti infragruppo.

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

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

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

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 essere inserito come unità di staff in una posizione gerarchica la più elevata possibile e deve essere previsto un riporto al massimo vertice aziendale attraverso un'attività di reporting così come descritta nel successivo paragrafo 3. 4.. 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 metterebbero a repentaglio l'obiettività di giudizio.

Il requisito dell'autonomia e dell'indipendenza deve intendersi anche quale assenza di qualsiasi forma di interferenza e condizionamento da parte dell'ente, e, in particolare, del management aziendale.

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; l'OdV provvede alla nomina di un Presidente, che viene comunicato al CdA.

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

I suoi membri restano in carica per la durata di 12 mesi e sono rinnovabili per successivi periodi annuali, fino a una durata massima triennale, previa semplice comunicazione scritta della Società, salvo dimissioni.

Alla scadenza del termine, i membri dell'Organismo di Vigilanza rimangono in carica fino a quando intervengano nuove nomine deliberate dal Consiglio di Amministrazione che confermino / sostituiscano in tutto o in parte i membri dell'Organismo di Vigilanza. Se nel corso della carica, uno o più membri dell'Organismo di Vigilanza cessano per qualsiasi motivo dal loro incarico, il Consiglio di Amministrazione provvede senza indugio alla loro sostituzione con propria delibera.

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

3.2. Le cause di ineleggibilità, rinuncia, revoca, sospensione e decadenza

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

a) l'assunzione di incarichi di amministratore di società che detengono una partecipazione nella Huawei, o in società da quest'ultima partecipate;

b) l'esistenza di relazioni di parentela, coniugio o affinità entro il IV grado con componenti del Consiglio di Amministrazione della Società nonché relazioni di parentela, coniugio o affinità entro il IV con componenti del Consiglio di Amministrazione delle società da questa controllate, delle società nonché relazioni di parentela, coniugio o affinità entro il IV grado con componenti del CdA delle Società, da queste controllate, delle società che la controllano e di quelle sottoposte a comune controllo; persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua struttura organizzativa dotata di autonomia finanziaria e funzionale, nonché persone che esercitano – anche di fatto – la gestione e il controllo della Società, sindaci della Società e la società di revisione nonché gli altri soggetti indicati dalla legge;

c) l'esistenza di situazioni di conflitti di interesse, anche potenziali, con la Società o con società controllate, che ne compromettano l'indipendenza;

d) avere la titolarità, diretta o indiretta, di partecipazioni azionarie di entità tali da permettere di esercitare una notevole influenza sulla Società o su società controllate;

e) svolgere funzioni di amministratore esecutivo ricoperte, nei tre esercizi precedenti alla nomina quale Organismo di Vigilanza, in imprese sottoposte a fallimento, liquidazione coatta amministrativa o procedure equiparate;

f) avere un rapporto di pubblico impiego presso amministrazioni centrali o locali nei tre anni precedenti alla nomina quale Organismo di Vigilanza;

g) aver subito un provvedimento di condanna, anche non passato in giudicato, ovvero di applicazione della pena su richiesta (c.d. "patteggiamento") in Italia o all'estero, per le violazioni rilevanti ai fini della responsabilità amministrativa degli enti ex D.Lgs. n. 231/2001;

h) aver subito un provvedimento di condanna, anche non passato in giudicato, ovvero di applicazione della pena su richiesta a una pena che imposta l'interdizione, anche temporanea, da pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;

i) essere stato dichiarato, inabilitato, fallito, o essere stato condannato ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità di esercitare uffici direttivi;

j) aver posto in essere comportamenti contrari al codice etico di Huawei, anche mediante la violazione di doveri o prescrizioni contenute in strumenti normativi e/o organizzativi interni;

k) essere legato alla Società o alle società da questa controllate o alle società che la controllano o a quelle sottoposte a comune controllo da un rapporto di lavoro o da un rapporto continuativo di consulenza o di prestazione d'opera retribuita, ovvero da altri rapporti che ne compromettano l'indipendenza;

l) aver posto in essere grave inadempimento dei doveri propri dell'OdV.

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

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

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

I componenti dell'Organismo di Vigilanza possono essere revocati nel corso del mandato esclusivamente per giusta causa, mediante un'apposita delibera del Consiglio di Amministrazione. A tale proposito, per giusta causa di revoca dovrà intendersi, a titolo esemplificativo:

- l'interdizione o l'inabilitazione, ovvero una grave infermità che renda il componente dell'Organismo di Vigilanza inidoneo a svolgere le proprie funzioni di vigilanza, o un'infermità che, comunque, comporti la sua assenza per un periodo superiore a sei mesi;

- l'attribuzione al componente dell'Organismo di Vigilanza di funzioni e responsabilità operative, ovvero il verificarsi di eventi, incompatibili con i requisiti di autonomia di iniziativa e di controllo, indipendenza e continuità di azione, che sono propri dell'Organismo di Vigilanza;

- la perdita dei requisiti soggettivi di onorabilità, integrità, rispettabilità e indipendenza presenti in sede di nomina;

- la sussistenza di una o più delle citate cause di ineleggibilità e incompatibilità;

- una grave negligenza nell'assolvimento dei compiti connessi con l'incarico professionale.

- l'omessa o insufficiente vigilanza da parte dell'OdV – secondo quanto previsto dall'art. 6, comma 1, lett. d), D.Lgs. 231/2001 – risultante da una sentenza, anche in primo grado, emessa nei confronti della Società ai sensi del D.Lgs. 231/2001 ovvero da sentenza di applicazione della pena su richiesta (il c.d. patteggiamento)";

- la violazione del divieto di divulgazione delle informazioni di cui al par. 3.5.

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

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

L'Organismo di Vigilanza potrà giovarsi – sotto la sua diretta sorveglianza e responsabilità – nello svolgimento dei compiti affidatigli, della collaborazione di tutte le funzioni e strutture della società ovvero di consulenti esterni – previa sottoscrizione di apposito contratto – avvalendosi delle rispettive competenze e professionalità.

All'Organismo di Vigilanza di Huawei è affidato il compito:

- di vigilare e verificare sull'osservanza delle prescrizioni del Modello attraverso: una costante ricognizione delle attività della Società allo scopo di monitorare ed eventualmente integrare le aree a rischio-reato, individuando le implementazioni e/o integrazioni da apportare al Modello stesso; una verifica sull'adeguatezza del Modello o sulla sua idoneità a prevenire il verificarsi di comportamenti illeciti; una vigilanza sull'osservanza delle prescrizioni del Modello da parte dei destinatari, segnalando tempestivamente eventuali violazioni o tentativi di violazione; una gestione dei flussi informativi; una raccomandazione delle azioni di miglioramento e supporto alle funzioni interne o ai consulenti esterni nella conduzione delle verifiche ispettive;

- di aggiornare il Modello ossia supportarne l'aggiornamento, proponendo, se necessario, l'adeguamento dello stesso al fine di migliorare l'efficacia anche in considerazione di eventuali nuovi interventi normativi;

- di partecipare a riunioni almeno mensili, salva la sussistenza di situazioni di eccezionalità ed urgenza che impongono convocazioni immediate nonché la redazione dei relativi report e verbali;

- di partecipare a due meeting annuali con il top management della Società e la redazione dei conseguenti report quali minute degli incontri sopra indicati;

- di partecipare ad altre eventuali riunioni operative, incluse le riunioni con l'Organo Amministrativo, il Collegio Sindacale e la società di revisione;

- di redigere un programma delle attività da svolgere annualmente;

- di redigere i pareri che si rendano necessari in base a quanto emerga nel corso della vigilanza;

- di produrre risposte verbali e/o scritte a specifiche richieste da parte dei destinatari del Modello o in relazione alle verifiche ispettive condotte;

- di analizzare le segnalazioni ed i flussi informativi provenienti dai destinatari del Modello e/o dai whistleblower;

- di analizzare e revisionare i report delle verifiche ispettive.

Per svolgere i propri compiti, i membri dell'Organismo di Vigilanza hanno libero accesso presso tutti i Dipartimenti della Società e alla documentazione aziendale, senza necessità di alcun consenso preventivo. Il Consiglio di Amministrazione curerà l'adeguata comunicazione alle strutture dei compiti dell'Organismo di Vigilanza e dei suoi poteri.

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

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

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:*

- la prima su **base continuativa** al Presidente del Consiglio di Amministrazione;
- la seconda a **cadenza semestrale**, nei confronti del Consiglio di Amministrazione e del Collegio Sindacale.

L'Organismo di Vigilanza:

- riporta al Presidente rendendolo edotto, ogni qual volta lo ritenga opportuno, su circostanze e fatti significativi del proprio ufficio. L'OdV comunica immediatamente il verificarsi di situazioni straordinarie (ad esempio: significative violazioni dei principi contenuti nel Modello emerse a seguito dell'attività di vigilanza, innovazioni legislative in materia di responsabilità amministrativa degli enti, ecc.) e le segnalazioni ricevute che rivestono carattere d'urgenza;
- presenta una relazione scritta, su base periodica semestrale, al Consiglio di Amministrazione e al Collegio Sindacale, che deve contenere, quanto meno, le seguenti informazioni:

a) la sintesi delle attività svolte nel corso del semestre;

b) eventuali problematiche o criticità che siano scaturite nel corso dell'attività di vigilanza;

c) qualora non oggetto di precedenti e apposite segnalazioni:

- le azioni correttive da apportare al fine di assicurare l'efficacia e/o l'effettività del Modello, ivi incluse quelle necessarie a rimediare alle carenze organizzative o procedurali accertate e idonee ad esporre la Società al pericolo che siano commessi reati rilevanti ai fini del Decreto, inclusa una descrizione delle eventuali nuove attività "sensibili" individuate;
- sempre nel rispetto dei termini e delle modalità indicati nel sistema disciplinare adottato dalla Società ai sensi del Decreto, l'indicazione dei comportamenti accertati e risultati non in linea con il Modello;

d) il resoconto delle segnalazioni ricevute, ivi incluso quanto direttamente riscontrato, in ordine a presunte violazioni delle previsioni del presente Modello, dei protocolli di prevenzione e delle relative procedure di attuazione e l'esito delle conseguenti verifiche effettuate;

e) informativa in merito all'eventuale commissione di reati rilevanti ai fini del Decreto;

f) i provvedimenti disciplinari e le sanzioni eventualmente applicate dalla Società, con riferimento alle violazioni delle previsioni del presente Modello, dei protocolli di prevenzione e delle relative procedure di attuazione;

g) una valutazione complessiva sul funzionamento e l'efficacia del Modello con eventuali proposte di integrazioni, correzioni o modifiche;

h) la segnalazione degli eventuali mutamenti del quadro normativo e/o significative modificazioni dell'assetto interno della Società che richiedono un aggiornamento del Modello;

i) il rendiconto delle spese sostenute.

L'Organismo di Vigilanza predispone con cadenza annuale:

a) una relazione riepilogativa dell'attività svolta nell'anno in corso e un piano delle attività previste per l'anno successivo, da presentare al Consiglio di Amministrazione e al Collegio Sindacale;

b) una nota informativa delle variazioni apportate al Modello al fine di farne oggetto di ratifica da parte del Consiglio di Amministrazione.

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

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. e Procedura Whistleblowing.

L'OdV è destinatario di qualsiasi informazione, documentazione e/o comunicazione, proveniente anche da terzi attinente al rispetto del Modello e comunque abbia rilevanza ai sensi del D. Lgs. N. 231/2001.

Come meglio disciplinato anche nella Procedura Whistleblowing, tutti i Destinatari del presente Modello hanno un diritto/dovere 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 allo 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*) e nel Regolamento 679/2016/UE: 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 condotta o presunta condotta rilevante ai sensi del D. Lgs. n. 231/2001, fatto salvo quanto specificato nella Procedura Whistleblowing con riferimento al canale denominato "BCG Complain". È garantito un adeguato flusso informativo tra l'Organismo di Vigilanza e i Dipartimenti deputati alla ricezione delle segnalazioni inoltrate tramite il canale "BCG Complain".

Le segnalazioni di condotte anche presunte rilevanti ai sensi del D.Lgs. n. 231/2001 sono 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, 240 – 20147 Milano

che di posta elettronica all'indirizzo:

231whistleblowing@huaweipec.it

Le modalità di gestione delle segnalazioni e della eventuale successiva istruttoria sono illustrate dalla Procedura Whistleblowing della Società.

La Società ha adottato misure adeguate a tutelare l'identità del segnalante e a mantenere la riservatezza dell'informazione in ogni contesto successivo alla segnalazione.

Huawei Technologies Italia S.r.l. sancisce, in conformità alla legge, il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante, per motivi collegati, direttamente o indirettamente alla segnalazione. A tal fine la Società nel sistema di sanzioni disciplinari adottato ha previsto sanzioni nei confronti di chi viola gli obblighi di riservatezza o compie atti di ritorsione o discriminatori nei confronti del segnalante.

È fatto salvo il diritto dei soggetti segnalati quali autori di violazioni e/o condotte illecite, di tutelarsi qualora siano accertate in capo al segnalante responsabilità di natura penale o civile legate alla falsità della dichiarazione.

La tutela del segnalante sarà supportata anche da un'efficace attività di sensibilizzazione e comunicazione per i dipendenti sui diritti e gli obblighi relativi alla divulgazione delle azioni illecite.

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'OdV deve essere tempestivamente informato in merito agli atti, comportamenti o eventi che possono determinare una violazione del Modello o che, più in generale, sono rilevanti ai fini della migliore efficacia ed effettività del Modello.

Tutti i Destinatari del Modello comunicano all'OdV ogni informazione utile per le verifiche sulla corretta attuazione del Modello.

Le informazioni affluiscono all'OdV principalmente:

a) **in forma strutturata.** A tal fine devono essere comunicate, con la necessaria tempestività, all'OdV, tramite nota scritta, ogni informazione riguardante:

- i rapporti predisposti dagli organi sociali/Dipartimenti e dalla società di revisione nell'ambito delle loro attività di verifica, dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto e/o delle previsioni del Modello;

- i procedimenti avviati per violazioni del Modello, i provvedimenti di archiviazione di tali procedimenti e le relative motivazioni, l'applicazione di sanzioni per violazione del Business Code of Conduct, del Modello o delle procedure stabilite per la sua attuazione;

- ricezione di atti e contestazioni da parte delle autorità di vigilanza (es. notifiche Garante privacy, etc.);

- violazioni della sicurezza informatica;

- qualsiasi altro atto o documento con profili di criticità rispetto all'osservanza del presente Modello.

- 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/Dipartimenti 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 alle 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 formalizzati 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 dal Dipartimento HR, coadiuvato dal Dipartimento Legal Affairs ed in coordinamento con l'Organismo di Vigilanza, in stretta collaborazione con i responsabili delle aree/funzioni coinvolte nell'applicazione del Modello. In particolare, il Dipartimento HR:

- 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 neoassunti 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 il Dipartimento Legal & Affairs.

4.2 Comunicazione iniziale

Il presente Modello è comunicato a tutte le risorse aziendali dal General Manager.

Tutti i Dipendenti, 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;

- la Procedura Whistleblowing.

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"

I principi e i contenuti del Modello sono portati a conoscenza di tutti coloro con i quali la Società intrattiene relazione contrattuali. L'impegno all'osservanza della legge e dei principi di riferimento del Modello da parte dei terzi aventi rapporti contrattuali con la Società è previsto da apposita clausola del relativo contratto ed è oggetto di accettazione da parte del terzo contraente.

5. Sistema Disciplinare

5.1 Profili generali

L'art. 6, comma 2, lett. e) e l'art. 7, comma 4, lett. b) del D.Lgs. 231/2001 indicano, quale condizione per un'efficace attuazione del Modello di organizzazione, gestione e controllo, l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso. Pertanto, la definizione di un adeguato sistema disciplinare costituisce un presupposto essenziale della valenza scriminante del modello di organizzazione, gestione e controllo ex D.Lgs. 231/2001 rispetto alla responsabilità amministrativa degli enti.

Le sanzioni previste saranno applicate in caso di violazione delle disposizioni contenute nel Modello a prescindere dalla commissione di un reato e dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria.

L'Organismo di Vigilanza, nel caso in cui riceva una segnalazione ovvero acquisisca nel corso delle proprie attività di vigilanza e di verifica degli elementi idonei a configurare una possibile violazione del modello, attiva gli opportuni accertamenti e sulla base delle evidenze acquisite coinvolge le direzioni aziendali competenti, tra cui HR, per valutare l'eventuale sanzione disciplinare da applicare alla fattispecie concreta

Per fatti e atti rilevanti ai sensi del D. Lgs.231/01, titolare del potere disciplinare è il datore di lavoro, cui spetta determinare l'entità della sanzione sulla base di quanto stabilito dai rispettivi CCNL.

In ogni caso, le fasi di contestazione della violazione, nonché quelle di determinazione ed effettiva applicazione delle sanzioni, sono svolte nel rispetto delle norme di legge e di regolamento vigenti, delle previsioni della contrattazione collettiva nazionale e della procedura per la segnalazione e gestione delle potenziali violazioni.

A seguito dell'entrata in vigore della Legge 179/2017, Confindustria ha emanato, a gennaio 2018, una Nota Illustrativa dal titolo "La disciplina in materia di whistleblowing" in cui si illustrano i principali contenuti della L.179/17 di maggiore interesse per le imprese.

Pertanto, in attuazione del disposto normativo e secondo le indicazioni contenute nelle Linee Guida Confindustria, la Società ha adottato un sistema di regole in grado di assicurare la tutela della riservatezza del segnalante, garantendone al contempo la protezione da discriminazioni o ritorsioni. In particolare, con riferimento alle segnalazioni di condotte illecite si precisa che il lavoratore che effettua segnalazioni non può essere sanzionato, demansionato, licenziato, trasferito o sottoposto ad altra

misura organizzativa, determinata dalla segnalazione, avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro.

Gli atti discriminatori o ritorsivi eventualmente adottati sono nulli.

Nel caso di controversie legate all'irrogazione di sanzioni disciplinari o all'adozione di ulteriori misure organizzative con effetti negativi sulle condizioni di lavoro del segnalante (demansionamenti, licenziamenti, trasferimenti), il datore di lavoro ha l'onere di dimostrare che esse sono fondate su ragioni estranee alla segnalazione stessa.
Il segnalante e l'organizzazione sindacale di riferimento possono denunciare all'Ispettorato Nazionale del Lavoro le misure discriminatorie eventualmente adottate.

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 Business Code of Conduct 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.