



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
EX D.LGS. N. 231/2001 E
D.LGS. N. 81/2008
di
UNITED PARCEL SERVICE
ITALIA S.r.l.**

INDICE PARTE SPECIALE

- **Parte Speciale A**, relativa ai reati contro la Pubblica Amministrazione;
- **Parte Speciale B**, relativa ai reati societari;
- **Parte Speciale C**, relativa alla corruzione tra privati;
- **Parte Speciale D**, relativa ai reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e auto-riciclaggio, nonché delitti in materia di strumenti di pagamento diversi dai contanti;
- **Parte Speciale E**, relativa ai delitti in materia di violazione del diritto d'autore;
- **Parte Speciale F**, relativa ai delitti contro l'industria e il commercio, nonché in materia di proprietà industriale e contrabbando;
- **Parte Speciale G**, relativa ai reati ambientali;
- **Parte Speciale H**, relativa ai reati in materia di salute e sicurezza sul lavoro;
- **Parte Speciale I**, relativa ai delitti contro la personalità ed il reato di sfruttamento di lavoratori il cui permesso di soggiorno è irregolare;
- **Parte Speciale L**, relativa ai delitti informatici;
- **Parte Speciale M**, relativa al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
- **Parte Speciale N**, relativa ai delitti di criminalità organizzata anche a carattere transnazionale;
- **Parte Speciale O**, relativa ai reati tributari;
- **Parte Speciale P**, relativa ai reati contro il patrimonio culturale.

PARTE GENERALE

Indice

1. LA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI EX D.LGS. 231/2001 E LA SUA EVOLUZIONE. IL TESTO UNICO N. 81/2008 IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO Error! Bookmark not defined.	
1.1. Il Decreto Legislativo n. 231 dell'8 giugno 2001	6
1.2. I reati presupposto	7
1.3. Le sanzioni	7
2. L'ADOZIONE E L'ATTUAZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO QUALE ESIMENTE DELLA RESPONSABILITÀ AMMINISTRATIVA DA REATO EX ART. 6 DEL D.LGS. N. 231/2001 E ART. 30 DEL D.LGS. N. 81/2008	Error! Bookmark not defined.
2.1. Le previsioni del Decreto	9
2.2. Le Linee Guida elaborate dalle associazioni di categoria.....	13
2.3. Le istruzioni del Ministero del Lavoro e delle Politiche Sociali.....	14
3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI UPS EX ART. 6 DEL DECRETO E ART. 30 DEL TU SS Error! Bookmark not defined.	
3.1. UPS nel mondo ed in Italia	15
3.2. La <i>mission</i> di UPS.....	16
3.3. L'adeguamento di UPS alle previsioni del Decreto	18
3.3.2. I lavori preparatori agli aggiornamenti del Modello. L'attività del Gruppo di Lavoro ed i presupposti del Documento di Sintesi	19
3.4. La struttura del Modello	22
4. IL MODELLO DI GOVERNANCE E LA STRUTTURA ORGANIZZATIVA DI UPS	Error! Bookmark not defined.
4.1. Il modello di governance di UPS	25
4.2. La struttura organizzativa	26
5. IL SISTEMA DI DELEGHE E PROCURE	37
5.1. I principi generali	37
5.2. La struttura del sistema di deleghe e procure in UPS	37
6. PROCEDURE MANUALI ED INFORMATICHE Error! Bookmark not defined.	
7. IL BUDGET ED IL CONTROLLO DI GESTIONE Error! Bookmark not defined.	
7.1. Investimenti in materia di Salute e Sicurezza sul lavoro.....	40
8. IL SISTEMA DI CONTROLLO SULLA SALUTE E SICUREZZA SUL LAVORO	Error! Bookmark not defined.
8.1. La gestione operativa in materia di Salute e Sicurezza sul Lavoro	40
8.2. Il sistema di monitoraggio della sicurezza (rinvio)	42

9. L'ORGANISMO DI VIGILANZA	Error! Bookmark not defined.
9.1. La nomina, la composizione dell'Organismo di Vigilanza ed i suoi requisiti.....	42
9.2 I casi di ineleggibilità e decadenza	43
9.3. La durata dell'incarico e le cause di cessazione.....	44
9.4. Le risorse dell'Organismo di Vigilanza	46
9.5. I compiti e i poteri	46
9.6. Il Regolamento dell'OdV.....	49
9.7. Il riporto informativo da e verso l'Organismo di Vigilanza	49
10. IL CODICE DI CONDOTTA	Error! Bookmark not defined.
11. IL SISTEMA DISCIPLINARE DI UPS	Error! Bookmark not defined.
11.1. L'elaborazione e l'adozione del Sistema Disciplinare	56
11.2. La struttura del Sistema Disciplinare	56
12. COMUNICAZIONE E FORMAZIONE SUL MODELLO E SUI PROTOCOLLI	Error! Bookmark not defined.
12.1. La comunicazione ed il coinvolgimento sul Modello e sui Protocolli connessi	65
12.2. La formazione e l'addestramento sul Modello e sui Protocolli connessi	67
13. AGGIORNAMENTO DEL MODELLO	Error! Bookmark not defined.
ALLEGATO 1: I REATI PRESUPPOSTO	Error! Bookmark not defined.

1.1. Il Decreto Legislativo n. 231 dell'8 giugno 2001

Il Decreto Legislativo dell'8 giugno 2001 n. 231, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*" (di seguito, "**Decreto**"), in attuazione della delega legislativa contenuta nell'art. 11 della legge 29 settembre 2000, n. 300, ha introdotto a carico degli enti, un regime di responsabilità amministrativa, assimilabile ad una responsabilità penale, nell'ipotesi in cui alcune specifiche fattispecie di reato vengano commesse nell'interesse o a vantaggio degli enti stessi da parte di:

- a) persone che rivestono funzioni di rappresentanza, sia organica che volontaria, di amministrazione o di direzione dell'ente o di una sua unità organizzativa (dotata di autonomia finanziaria e funzionale) o che esercitano, anche di fatto, la gestione e il controllo dell'ente (soggetti c.d. "**apicali**")¹;
- b) persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a (soggetti c.d. "**subordinati**").

È stato così superato l'antico principio *societas delinquere non potest*² ed enucleata una responsabilità autonoma della persona giuridica.

Quanto ai soggetti destinatari della nuova forma di responsabilità, il Decreto specifica che si tratta di "enti forniti di personalità giuridica, società e associazioni anche prive di personalità giuridica". Sono invece esclusi dal novero dei soggetti destinatari, lo Stato, gli enti pubblici territoriali (Regioni, Province, Comuni e

¹ Possono essere qualificati come apicali i componenti degli organi di amministrazione e controllo dell'Ente, quale che sia il sistema prescelto tra quelli indicati dal Legislatore (amministratore unico, consiglio di amministrazione, amministrazione congiunta o disgiunta). Nel novero dei soggetti in c.d. "posizione apicale", oltre agli amministratori e ai sindaci vanno, inoltre, ricompresi, alla stregua dell'art. 5 del Decreto, il direttore generale, i direttori esecutivi dotati di autonomia finanziaria e funzionale, nonché i preposti alle sedi secondarie ed ai siti/stabilimenti, i quali possono anche assumere la qualifica di "datori di lavoro" ai sensi della normativa prevenzionistica vigente in materia di salute e sicurezza sul lavoro. Tali soggetti possono essere legati alla società sia da un rapporto di lavoro subordinato, sia da altri rapporti di natura privatistica (ad es., mandato, agenzia, preposizione institoria, ecc.).

² Era escluso che una società potesse comparire nella veste di imputato nell'ambito di un processo penale.

Comunità montane), gli enti pubblici non economici e, in generale, tutti gli enti che svolgano funzioni di rilievo costituzionale (Camera dei deputati, Senato della Repubblica, Corte costituzionale, Segretariato generale della Presidenza della Repubblica, C.S.M., CNEL).

1.2. I reati presupposto

Al fine di configurare la responsabilità amministrativa ex Decreto, nella Sezione III del Capo I del Decreto, sono individuate, come rilevanti solo specifiche tipologie di reato (i c.d. reati presupposto)³, meglio indicate nell'**Allegato n. 1**.

1.3. Le sanzioni

Ai sensi dell'art. 9 del Decreto le sanzioni applicabili agli enti, a seguito della commissione del reato sono:

- i. sanzioni pecuniarie: hanno natura afflittiva (sanzionatoria) e non risarcitoria e sono calcolate in base ad un sistema per quote (in un numero non inferiore a cento né superiore a mille), e viene determinata dal giudice sulla base della gravità del fatto e del grado di responsabilità dell'ente, dall'attività svolta dall'ente per eliminare o attenuare le conseguenze del fatto illecito e per prevenire la commissione di ulteriori illeciti. L'importo di ciascuna quota va da un minimo di 258,23 € ad un massimo di 1.549,37 € e viene determinato dal giudice tenendo in considerazione le condizioni economiche e patrimoniali dell'ente. L'ammontare della sanzione pecuniaria, pertanto, viene determinato per effetto della moltiplicazione del primo fattore (numero di quote) per il secondo (importo della quota);
- ii. sanzioni interdittive: sono (art. 9, comma 2):
 - l'interdizione dall'esercizio dell'attività;
 - la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

³ Il "catalogo" dei reati presupposto rilevanti ai sensi del Decreto è in continua espansione. Se, da un lato, vi è una forte spinta da parte degli organi comunitari, dall'altro, anche a livello nazionale, sono stati presentati, numerosi disegni di legge diretti ad inserire ulteriori fattispecie.

- il divieto di contrattare con la pubblica amministrazione, salvo che per l'ottenimento di un servizio pubblico; tale divieto può essere limitato anche a determinati tipi di contratto o a determinate amministrazioni;
- l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi;
- il divieto di pubblicizzare beni o servizi.

iii. confisca (sanzione obbligatoria conseguente all'eventuale sentenza di condanna)

iv. pubblicazione della sentenza

Le sanzioni interdittive hanno la caratteristica di limitare o condizionare l'attività sociale, e nei casi più gravi arrivano a paralizzare l'ente (interdizione dall'esercizio dell'attività); esse hanno altresì la finalità di prevenire comportamenti connessi alla commissione di reati.

Tali sanzioni si applicano, come detto, nei casi espressamente previsti dal Decreto quando ricorrono almeno una delle seguenti condizioni:

- a) l'ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione e, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative,
- b) in caso di reiterazione degli illeciti.

Le sanzioni interdittive hanno una durata non inferiore a tre mesi e non superiore a due anni; è possibile l'applicazione in via definitiva delle sanzioni interdittive, nelle situazioni più gravi descritte nell'art. 16 del Decreto.

Deve essere evidenziato che il Decreto prevede all'art. 15 che in luogo dell'applicazione della sanzione interdittiva che determina l'interruzione dell'attività dell'ente, se sussistono particolari presupposti, il giudice possa nominare un commissario per la prosecuzione dell'attività dell'ente per un periodo pari alla durata della pena interdittiva.

Appare opportuno indicare che l'art. 45 del Decreto prevede l'applicazione delle sanzioni interdittive indicate nell'art. 9, comma 2, anche in via cautelare quando sussistono gravi indizi per ritenere la sussistenza della responsabilità dell'ente per un illecito amministrativo dipendente da reato e vi sono fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa indole di quello per il quale si procede.

Deve, infine, osservarsi che l'Autorità Giudiziaria può, altresì, disporre:

- il sequestro preventivo delle cose di cui è consentita la confisca (art. 53);
 - il sequestro conservativo dei beni mobili e immobili dell'Ente qualora sia riscontrata la fondata ragione di ritenere che manchino o si disperdano le garanzie per il pagamento della sanzione pecuniaria, delle spese del procedimento o di altre somme dovute allo Stato (art. 54).
- **2.1. Le previsioni del Decreto**

2. L'ADOZIONE E L'ATTUAZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO QUALE ESIMENTE DELLA RESPONSABILITÀ AMMINISTRATIVA DA REATO EX ART. 6 DEL D.LGS. N. 231/2001 E ART. 30 DEL D.LGS. N. 81/2008

Il Legislatore riconosce, agli artt. 6 e 7 del Decreto, forme specifiche di esonero della responsabilità amministrativa dell'Ente.

In particolare, l'art. 6, comma I, prescrive che, nell'ipotesi in cui i fatti di reato siano ascrivibili a soggetti in posizione apicale, l'Ente non è ritenuto responsabile se prova che:

- a) ha adottato ed attuato, prima della commissione del fatto, un modello di gestione, organizzazione e controllo (di seguito anche solo "**Modello**") idoneo a prevenire reati della specie di quello verificatosi;
- b) ha nominato un organismo, indipendente e con poteri autonomi, che vigili sul funzionamento e l'osservanza del modello e ne curi l'aggiornamento (di seguito, anche "**Organismo di Vigilanza**" o "**OdV**" o anche solo "**Organismo**");

- c) il reato è stato commesso eludendo fraudolentemente le misure previste nel modello;
- d) non vi è stata omessa o insufficiente vigilanza da parte dell'OdV.

Il contenuto del Modello è individuato dallo stesso art. 6, il quale, al comma II, prevede che l'Ente debba:

- i. individuare le attività nel cui ambito possono essere commessi i reati;
- ii. prevedere specifici protocolli volti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- iii. individuare modalità di gestione delle risorse finanziarie idonee a prevenire i reati;
- iv. prevedere obblighi di informazione nei confronti dell'OdV;
- v. introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate dal Modello.

Nel caso dei soggetti in posizione subordinata, l'adozione e l'efficace attuazione del modello importa che l'Ente sarà chiamato a rispondere solo nell'ipotesi in cui il reato sia stato reso possibile dall'inosservanza degli obblighi di direzione e vigilanza (combinato di cui ai commi I e II dell'art. 7).

I successivi commi III e IV introducono due principi che, sebbene siano collocati nell'ambito della norma sopra rammentata, appaiono rilevanti e decisivi ai fini dell'esonero della responsabilità dell'Ente per entrambe le ipotesi di reato di cui all'art. 5, lett. a) e b). Segnatamente, è previsto che:

- il Modello deve prevedere misure idonee sia a garantire lo svolgimento dell'attività nel rispetto della legge, sia a scoprire tempestivamente situazioni di rischio, tenendo in considerazione il tipo di attività svolta nonché la natura e la dimensione dell'organizzazione;
- l'efficace attuazione del Modello richiede una verifica periodica e la modifica dello stesso qualora siano scoperte significative violazioni delle prescrizioni di legge o qualora intervengano significativi mutamenti nell'organizzazione o normativi; assume rilevanza, altresì, l'esistenza di un idoneo sistema disciplinare (condizione, invero, già prevista dalla lett. e), sub art. 6, comma II).

Un Modello idoneo deve, inoltre, 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, delle quali 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.

Deve aggiungersi, inoltre, che con specifico riferimento alla efficacia preventiva del Modello con riferimento ai reati (colposi) in materia di salute e sicurezza sul lavoro, l'**art. 30 del T.U. n. 81/2008** stabilisce che:

"Il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al decreto legislativo 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

- a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;*
- b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;*
- c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;*
- d) alle attività di sorveglianza sanitaria;*
- e) alle attività di informazione e formazione dei lavoratori;*

- f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
- h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate'.

Sempre secondo la lettera dell'art. 30: *"Il modello organizzativo e gestionale deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività. Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello. Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico. In sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti. Agli stessi fini ulteriori modelli di organizzazione e gestione aziendale possono essere indicati dalla Commissione di cui all'articolo 6"*.

Come noto, sotto un profilo formale l'adozione ed efficace attuazione di un Modello non costituisce un obbligo, ma unicamente una facoltà per gli Enti, i quali ben potrebbero decidere di non conformarsi al disposto del Decreto senza incorrere, per ciò solo, in alcuna sanzione. Ciò varrebbe, in particolare, nel caso delle filiali di società basate in paesi con gli Stati Uniti in cui, da anni, è prevista l'implementazione - anche a vantaggio delle controllate - di *compliance programs* con riferimento a molte delle tematiche rilevanti ai sensi del Decreto (rapporti con Pubblica Amministrazione, tematiche SSL e ambiente, ecc.)

Tuttavia, l'adozione ed efficace attuazione di un Modello idoneo è, per gli Enti, un presupposto molto importante per poter beneficiare dell'esimente prevista dal Legislatore.

È importante, inoltre, tenere in precipuo conto che il Modello non è da intendersi quale strumento statico, ma deve essere considerato, di converso, un apparato dinamico che permette all'Ente di eliminare, attraverso una corretta e mirata implementazione dello stesso nel corso del tempo, eventuali mancanze che, al momento della sua creazione, non era possibile individuare.

2.2. Le Linee Guida elaborate dalle associazioni di categoria

L'art. 6, comma 3 del Decreto prevede che il modello possa essere adottato sulla base di codici di comportamento redatti dalle associazioni di categoria rappresentative degli enti, comunicati al Ministero della Giustizia, il quale può formulare osservazioni.

La prima Associazione a redigere un documento di indirizzo per la costruzione dei modelli è stata Confindustria – cui partecipa AICAI (Associazione Italiana Corrieri Aerei Internazionali), associazione di riferimento di UNITED PARCEL SERVICE ITALIA S.r.l. (di seguito anche "**UPS**" o "**Società**") – che, nel marzo del 2002, ha emanato delle Linee Guida, poi parzialmente modificate e aggiornate prima nel maggio 2004, poi nel marzo 2008, nel marzo 2014 ed, infine, nel giugno 2021 (di seguito, anche "**Linee Guida**")⁴. Successivamente, molte Associazioni settoriali hanno redatto le proprie Linee Guida tenendo in considerazione i principi enucleati dalla Confindustria, le cui Linee Guida costituiscono, dunque, l'imprescindibile punto di partenza per la costruzione del modello.

In sintesi, le Linee Guida suggeriscono di:

⁴ Tutte le versioni delle Linee Guida di Confindustria sono state poi giudicate adeguate dal Ministero di Giustizia (con riferimento alle Linee Guida del 2002, cfr. la "Nota del Ministero della Giustizia" del 4 dicembre 2003; con riferimento ai successivi, cfr. la "Nota del Ministero della Giustizia" del 28 giugno 2004 la "Nota del Ministero della Giustizia" del 2 aprile 2008, la "Nota del Ministero della Giustizia" del 21 luglio 2014 e la "Nota del Ministero della Giustizia" dell'8 giugno 2021).

- mappare le aree aziendali a rischio e le attività nel cui ambito potenzialmente possono essere commessi i reati presupposto mediante specifiche modalità operative;
- individuare e predisporre specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire
- individuare un Organismo di Vigilanza dotato di autonomi poteri di iniziativa e controllo e dotato di un adeguato budget;
- individuare specifici obblighi informativi nei confronti dell'OdV sui principali fatti aziendali e in particolare sulle attività ritenute a rischio e specifici obblighi informativi da parte dell'OdV verso i vertici aziendali e gli organi di controllo;
- adottare un codice etico che individui i principi dell'azienda e orienti i comportamenti dei destinatari del modello;
- adottare un sistema disciplinare, idoneo a sanzionare il mancato rispetto dei principi indicati nel modello.

2.3. Le istruzioni del Ministero del Lavoro e delle Politiche Sociali

In aggiunta alle Linee Guida, con particolare riguardo al Modello esimente in materia di SSL, devono anche prendersi in considerazione le istruzioni fornite dal Ministero del Lavoro e delle Politiche Sociali (di seguito anche 'Ministero') del luglio 2011 aventi ad oggetto *chiarimenti sul sistema di controllo (comma 4 dell'articolo 30 del D. Lgs. 81/2008) ed indicazioni per l'adozione del sistema disciplinare (comma 3 dell'articolo 30 del D. Lgs. 81/2008)*.

Con riferimento al primo punto il Ministero osserva che *qualora un'azienda si sia dotata di un sistema di gestione della salute e sicurezza sul lavoro conforme ai requisiti delle Linee Guida UNI-INAIL o delle BS OHSAS 18001:2007, essa attua il proprio sistema di controllo secondo quanto richiesto al comma 4 dell'articolo 30 del D.Lgs. n. 81/2008 (...). Si evidenzia però come tali processi rappresentino un sistema di controllo idoneo ai fini di quanto previsto al comma 4 dell'articolo 30 del D. Lgs. n. 81/2008 solo qualora prevedano il ruolo attivo e documentato, oltre*

che di tutti i soggetti della struttura organizzativa aziendale per la sicurezza, anche dell'Alta Direzione' (intesa come posizione organizzativa eventualmente soprastante).

Con riferimento al sistema disciplinare, il Ministero evidenzia: esso dovrà essere definito e formalizzato dall'Alta Direzione aziendale e quindi diffuso a tutti i soggetti interessati quali ad esempio:

- *Datore di lavoro (articolo 2, comma 1, lett. b, D. Lgs. n. 81/2008);*
- *Dirigenti (articolo 2, comma 1, lett. d, Digs. n. 81/2008) o altri soggetti in posizione apicale;*
- *Preposti (articolo 2, comma 1, lett. e, D.Lgs. n. 81/2008);*
- *Lavoratori (articolo 2, comma 1, lett. b, D. Lgs. n. 81/2008);*
- *Organismo di Vigilanza (ove istituito un modello ex D.Lgs. n. 231/2001); Auditor/Gruppo di audit.*

Quanto ai terzi, il Ministero specifica che *l'azienda dovrà, inoltre, definire idonee modalità per selezionare, tenere sotto controllo e, ove opportuno, sanzionare collaboratori esterni, appaltatori, fornitori e altri soggetti aventi rapporti contrattuali con l'azienda stessa. Perché tali modalità siano applicabili l'azienda deve prevedere che nei singoli contratti siano inserite specifiche clausole applicative con riferimento ai requisiti e comportamenti richiesti ed alle sanzioni previste per il loro mancato rispetto fino alla risoluzione del contratto stesso.*

Il Ministero elabora, inoltre, una 'tabella di correlazione tra i punti di cui all'art. 30 del TU SSL (che individuano i requisiti del modello esimente) e i punti in tal senso rilevanti secondo i sopra menzionati sistemi di gestione.

3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI UPS EX ART. 6 DEL DECRETO E ART. 30 DEL TU SSL

3.1. UPS nel mondo ed in Italia

UPS Italia è società italiana, facente parte del gruppo multinazionale americano UPS che, con più di 400.000 dipendenti e società in varie nazioni, è società leader mondiale nella spedizione e trasporto.

Operante in Italia sin dal 1986, la Società italiana ha sua sede a Wilmington

Orange Street 1209 (Stati Uniti); nel nostro Paese occupa circa 1200 dipendenti e ubicati presso una serie di unità locali.

La Società italiana è attiva nei seguenti settori:

- ✓ servizi di spedizione e trasporto, per via terrestre, marittima e aerea, di pacchi e merci;
- ✓ attività strumentali e/o accessorie alla spedizione e al trasporto, per via terrestre, marittima e aerea;
- ✓ servizi di logistica. La Società' può operare in qualità di spedizioniere, spedizioniere-vettore, vettore, nonché' avvalersi di sub-vettori nel settore dei trasporti per via terrestre, marittima o aerea.

La Società può anche svolgere tutte le seguenti attività nei settori del trasporto merci, della logistica, della spedizione e dello stoccaggio:

- ✓ attività di information technology;
- ✓ attività di gestione delle risorse umane;
- ✓ attività di gestione contabile;
- ✓ attività di pianificazione di tratte (route planning);
- ✓ attività di plant engineering;
- ✓ attività di industrial engineering;
- ✓ attività di business development;
- ✓ attività di marketing.

3.2. La *mission* di UPS

UPS ha compendiato nei documenti Policy Book e Codice di Condotta gli elementi essenziali della propria *mission* aziendale, destinata a creare valore per la Società, i dipendenti, i clienti e il pubblico in generale.

Rimandando ai sopra indicati documenti per un quadro più completo, la *mission* della Società di può sintetizzare nei termini che seguono:

- ✓ *Guidare con il proprio esempio in qualità di azienda responsabile, attenta e sostenibile che dà un grosso contributo nelle comunità in cui opera;*
- ✓ *Mantenere un'azienda finanziariamente forte, con un'ampia partecipazione dei dipendenti, fornendo un risultato concorrenziale nel lungo termine gli azionisti;*

- ✓ *Incoraggiare i collaboratori e partner a fare del loro meglio, offrendo opportunità di sviluppo e successo personale;*
- ✓ *Far crescere l'attività globale rispondendo alle necessità logistiche dei clienti e offrendo eccellenza e valore in tutto il nostro operato.*

I risultati sopra indicati potranno essere raggiunti mediante la costante applicazione e il rispetto dei valori in cui la Società crede:

- **Integrità** - *È il fondamento di ciò che siamo e di tutto quello che facciamo.*
- **Lavoro di squadra** - *Lavorando insieme, persone determinate possono realizzare qualsiasi cosa.*
- **Servizio** - *Essere al servizio delle necessità dei nostri clienti e delle nostre comunità è fondamentale per il nostro successo.*
- **Qualità ed efficienza** - *Siamo sempre costruttivamente insoddisfatti nella nostra ricerca dell'eccellenza.*
- **Sicurezza** - *Il benessere dei nostri collaboratori, dei nostri partner e del pubblico è di estrema importanza.*
- **Sostenibilità** - *Per garantire una prosperità a lungo termine il nostro impegno verso la gestione responsabile dell'ambientale e la responsabilità sociale deve essere continuo.*
- **Innovazione** - *La creatività e il cambiamento sono fondamentali per crescere.*

Nello svolgimento della propria attività aziendale, in ragione della peculiarità del mercato in cui opera, UPS mantiene una costante attenzione alle attese della collettività e dei clienti, con l'obiettivo di garantire sempre un elevatissimo standard di qualità.

UPS, inoltre, da sempre dedica grande considerazione agli aspetti etici dell'impresa e adotta le migliori tecniche disponibili per la mitigazione degli impatti derivanti dalle proprie attività.

La *mission* aziendale è garantita da un sistema di *corporate governance* conforme alla dimensione e struttura aziendale (sul punto, vedi *infra*, capitolo 4).

3.3. L'adeguamento di UPS alle previsioni del Decreto

3.3.1. I *compliance programs* applicati prima dell'approvazione del Modello

UPS, essendo società di matrice americana, in conformità alle stringenti regolamentazioni in vigore negli Stati Uniti già da tempo ha implementato una serie di *compliance programs* dedicati a regolamentare le attività maggiormente a rischio come, ad es., in materia di gestione dei rapporti con esponenti della Pubblica Amministrazione nonché in materia di salute e sicurezza sui luoghi di lavoro e di ambiente e in ambito antitrust.

Basti pensare che il primo Policy book è stato emanato dalla casa madre nel lontano 1929 e poi, in ragione del mutare del tempo e delle legislazioni, più volte aggiornato nel corso degli anni. Altri "modelli" relativi alla gestione di talune attività a rischio sono stati implementati negli anni successivi.

Quando la Società si è stabilita anche in Italia, nel 1986, dunque, ha potuto contare su un'esperienza e un'attenzione ultradecennale votata alla *compliance* alle normative applicabili alle attività aziendali nonché allo svolgimento di un business di Condotta e consapevole. I *compliance programs* approvati a livello di gruppo, infatti, sono implementati in tutte le nazioni in cui operano le varie filiali, e così è stato in Italia.

Con particolare riferimento alla tematica della salute e sicurezza, UPS oltre a rispettare pedissequamente la normativa italiana dotandosi di tutti gli strumenti a tutela dei lavoratori previsti dalla regolamentazione di settore, ha implementato, a maggior prova dell'attenzione al tema, gli specifici *compliance programs* predisposti dalla casa madre.

In altre parole, UPS è già da tempo dotata di un sistema organizzativo pienamente rispondente ai requisiti di cui agli artt. 30 del TU SSL e 6 del Decreto, anche se non formalizzato in un "modello". Tuttavia, pur non esistendo un documento denominato "modello", già dal 2006 era stato implementato a livello italiano un documento di raccordo - avente sostanzialmente pari valenza del Modello inteso quale fulcro e sintesi dell'organizzazione della società in materia di SSL - denominato "Manuale Globale sulla Sicurezza", oggetto di aggiornamento nel

2008. Il Manuale Globale sulla Sicurezza, infatti, prevedeva una serie di procedure dirette a regolamentare tutti gli aspetti disciplinati dall'art. 30 TU SSL.

Al Manuale Globale sulla Sicurezza si aggiungevano, oltre che le *policies* della casa madre anche la documentazione comprovante l'ottemperanza agli obblighi di legge previsti dalla normativa in materia di prevenzione degli infortuni sul lavoro.

A riprova dell'esistenza di un sistema organizzativo assimilabile a quello formalizzato con il Modello approvato dalla Società, deve evidenziarsi che presso UPS, a livello di gruppo era (ed è) presente un Comitato di Controllo che svolgeva (e svolge) una serie di audit per verificare il rispetto delle procedure in tema SSL. Ulteriori controlli sono effettuati periodicamente da primarie società esterne.

Anche sotto il profilo della vigilanza, il sistema organizzativo di UPS si è dimostrato all'avanguardia e anticipatore dei dettami che sarebbero stati introdotti con il TU SSL.

La Società ha, dunque, sempre assicurato l'adeguatezza e l'effettività dei controlli.

3.3.2. I lavori preparatori agli aggiornamenti del Modello. L'attività del Gruppo di Lavoro ed i presupposti del Documento di Sintesi

UPS, sempre tesa al proprio miglioramento ha, comunque, proceduto alla formalizzazione del suo Modello organizzativo, previa l'esecuzione di un'analisi dell'intera struttura organizzativa aziendale e del proprio sistema di controlli, onde verificarne l'adeguatezza rispetto ai fini di prevenzione dei reati rilevanti.

Così, dopo avere proceduto allo svolgimento di una complessa e articolata attività di *risk assessment* ha nominato un proprio OdV ed adottato il Modello della Società, così adeguandosi anche formalmente (sostanzialmente lo era da sempre) ai dettami del TU SSL e Decreto.

Per procedere alla redazione del documento di sintesi (di seguito, anche 'Documento di Sintesi') affinché questi fosse rappresentativo del Modello in essere, la Società ha programmato l'attuazione di un piano di intervento volto a sottoporre ad una approfondita e complessa analisi l'organizzazione e l'attività della Società con riferimento alla *compliance* alle disposizioni in tema di salute e sicurezza sul

luogo di lavoro.

È stato formato un Gruppo di Lavoro costituito dalle risorse aziendali a ciò qualificate, assistite da consulenti esterni provenienti da primaria Società di consulenza e da uno Studio Legale con provata esperienza nel settore, affinché venissero svolte le attività di *risk mapping* e *risk assessment* secondo le *best practice* indicate dalle Linee Guida delle Associazioni di categoria, tenendo anche in considerazione gli orientamenti giurisprudenziali e dottrinari.

Come suggerito dalle Linee Guida, con riferimento ai **reati colposi**, l'analisi è stata condotta sull'intera struttura aziendale, poiché, rispetto ai reati di omicidio e lesioni colpose gravi o gravissime commessi con violazione delle norme di tutela della salute e sicurezza sul lavoro (di seguito, anche 'SSL'), non è possibile escludere aprioristicamente alcun ambito di attività, atteso che tale casistica di reati può, di fatto, investire la totalità delle componenti aziendali.

L'attività di *risk assessment* ha avuto l'obiettivo di:

- a) individuare i siti caratterizzati dal rischio potenziale di violazioni o inadempienze in materia di SSL che possono comportare, in modo diretto o indiretto, la commissione dei reati previsti dall'art. 25 *septies* del Decreto;
- b) analizzare l'adeguatezza del sistema di controllo interno in materia di SSL;
- c) individuare le azioni da intraprendere per il miglioramento del suddetto sistema di controllo interno e per l'adeguamento alla normativa in materia di SSL;
- d) assegnare una priorità di intervento nell'ambito dei siti oggetto di analisi.

In via preliminare, il gruppo di lavoro ha provveduto a raccogliere e analizzare la documentazione rilevante in materia di SSL (tra i quali, organigrammi, *mission statement*, procedure, documenti di valutazione dei rischi, ecc.) necessaria sia alla comprensione della struttura organizzativa della Società e degli ambiti relativi alla SSL, sia alla definizione dei siti oggetto di analisi.

Sono stati, quindi, considerati i rischi potenziali di commissione dei reati, coincidenti, come suggerito dalle Associazioni di categoria, con la valutazione dei rischi lavorativi effettuata secondo i criteri previsti dal D.Lgs. n. 81/2008 e dalle altre disposizioni normative e regolamentari aventi lo stesso oggetto e profilo.

Nel corso dell'analisi, il Gruppo di Lavoro ha, inoltre:

- verificato, attraverso l'effettuazione di interviste con i responsabili aziendali, (tra cui il responsabile del servizio di prevenzione e protezione), l'evidenza e l'adeguatezza delle valutazioni dei rischi esistenti in materia di SSL ed i controlli a presidio degli stessi – analizzando la struttura organizzativa, la formazione e l'addestramento del personale, la comunicazione ed il coinvolgimento di quest'ultimo, il sistema di controllo di salute e sicurezza (gestione operativa e monitoraggio) (c.d. *as is analysis*). Tale attività è stata svolta attraverso l'utilizzo di questionari specificamente mirati (check list) a verificare l'adeguatezza e l'effettività di applicazione delle prescrizioni in materia di SSL;
- verificato l'esistenza e, eventualmente, l'adeguatezza di un modello gestionale in materia di SSL che presentasse, sotto il profilo della compliance legale, i requisiti previsti dalla Norma British Standard OHSAS 18001: 2007 e dalle Linee Guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001.

Il Gruppo di Lavoro ha, quindi, provveduto alla rilevazione ed alla analisi dei controlli aziendali verificando - oltre ai documenti e agli *output* delle analisi sopra descritte - il sistema delle procure e deleghe, il sistema di controllo di gestione, il codice di Condotta, il sistema disciplinare, il ricco apparato di procedure esistenti e ritenute rilevanti ai fini dell'analisi (c.d. fase *as is analysis*).

Con riferimento ai **reati dolosi**:

- è stato messo a punto un dettagliato e completo elenco delle **aree "a rischio reato"** e/o delle **"attività sensibili"**, ossia dei settori della Società per i quali è stato ritenuto astrattamente sussistente, sulla base dei risultati dell'analisi, il rischio di commissione dei reati teoricamente riconducibili alla tipologia dei c.d. reati presupposto, previsti dal Decreto e rilevanti per la Società;
- per ciascuna "area a rischio reato" e/o "attività sensibile", inoltre, sono state individuate le **fattispecie di reato astrattamente ipotizzabili e/o alcune delle possibili modalità di commissione dei reati** presi in considerazione;
- con riguardo ai reati contro la Pubblica Amministrazione, al reato di corruzione tra privati e ai reati tributari, sono state individuate le c.d. **aree "strumentali"**, ossia le aree che gestiscono strumenti di tipo finanziario

e/o mezzi sostitutivi che possono supportare la commissione dei reati nelle "aree a rischio reato".

Successivamente, sono stati identificati i punti di miglioramento, con la formulazione di appositi suggerimenti, nonché dei piani di azione per l'implementazione dei principi di controllo (c.d. *gap analysis*).

Il risultato del lavoro svolto è riportato nel presente documento di sintesi del Modello (d'ora in poi anche 'Documento di Sintesi').

Nel corso del 2021, considerando le modifiche normative sopraggiunte, la Società ha deciso di procedere ad un aggiornamento del Modello, seguendo la stessa metodologia adottata per l'adozione.

3.4. La struttura del Modello

Una volta concluse le attività preparatorie sopra indicate, si è provveduto alla progettazione, predisposizione dei documenti rappresentativi del Modello.

In particolare, il Modello della Società è costituito da una Parte Generale e da una Parte Speciale (unitariamente denominati: Documento di Sintesi) nonché da ulteriori documenti che, rappresentativi di alcuni protocolli di controllo, completano il quadro.

Nella **Parte Generale**, oltre all'illustrazione dei contenuti del Decreto e della funzione del Modello, sono rappresentati sinteticamente i protocolli sotto indicati (di seguito, anche 'Protocolli'), che – in conformità a quanto previsto dalle Associazioni di categoria – compongono il Modello:

- il sistema organizzativo;
- il sistema di procure e deleghe;
- il sistema di controllo di gestione;
- il sistema di controllo sulla salute e sicurezza sul lavoro;
- il Codice di Condotta;
- il Sistema Disciplinare;

- la comunicazione e la formazione.

La "**Parte Speciale**" è suddivisa in quattordici parti, ciascuna dedicata ad una specifica tipologia di reato, in particolare:

- **Parte Speciale A**, relativa ai reati contro la Pubblica Amministrazione;
- **Parte Speciale B**, relativa ai reati societari;
- **Parte Speciale C**, relativa alla corruzione tra privati;
- **Parte Speciale D**, relativa ai reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e auto-riciclaggio, nonché delitti in materia di strumenti di pagamento diversi dai contanti;
- **Parte Speciale E**, relativa ai delitti in materia di violazione del diritto d'autore;
- **Parte Speciale F**, relativa ai delitti contro l'industria e il commercio, nonché in materia di proprietà industriale e contrabbando;
- **Parte Speciale G**, relativa ai reati ambientali;
- **Parte Speciale H**, relativa ai reati in materia di salute e sicurezza sul lavoro;
- **Parte Speciale I**, relativa ai delitti contro la personalità ed il reato di sfruttamento di lavoratori il cui permesso di soggiorno è irregolare;
- **Parte Speciale L**, relativa ai delitti informatici;
- **Parte Speciale M**, relativa al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
- **Parte Speciale N**, relativa ai delitti di criminalità organizzata anche a carattere transnazionale;
- **Parte Speciale O**, relativa ai reati tributati;
- **Parte Speciale P**, relativa ai reati contro il patrimonio culturale.

Nell'ambito delle Parti Speciali, sono stati indicati, seguendo anche l'approccio metodologico già esposto:

- i) le aree ritenute "a rischio reato" e le attività "sensibili";
- ii) le funzioni e/o i servizi e/o gli uffici aziendali che operano nell'ambito delle aree "a rischio reato" o delle attività "sensibili";
- iii) i reati astrattamente perpetrabili;
- iv) le aree ritenute "strumentali" (con riferimento ai reati contro la Pubblica Amministrazione, al reato di corruzione tra privati e ai reati tributari), nonché i soggetti che in esse agiscono;
- v) la tipologia dei controlli in essere sulle singole aree a "rischio reato" e "strumentali";
- vi) i principi di comportamento da rispettare al fine di ridurre il rischio di commissione dei reati.

Nella Parte Speciale H (salute e sicurezza sui luoghi di lavoro), in particolare, sono stati indicati:

- a) reati di cui all'art. 25 *septies* del Decreto;
- b) i fattori di rischio esistenti nell'ambito dell'attività d'impresa svolta dalla Società;
- c) la struttura organizzativa di UPS in materia di SSL;
- d) i doveri ed i compiti di ciascuna categoria di soggetti operanti nell'ambito della struttura organizzativa UPS in materia di SSL (con uno specifico approfondimento del rapporto con gli appaltatori);
- e) le modalità della sorveglianza sanitaria;
- f) le attività connesse all'informazione e formazione;
- g) le attività di gestione della documentazione e certificazione;
- h) il sistema di controllo sulla SSL, il ruolo dell'Organismo di Vigilanza in materia di salute e sicurezza sul lavoro, nonché il raccordo con le altre funzioni aziendali;
- i) il sistema di registrazione delle attività aziendali in tema di SSL;
- j) il riesame e l'aggiornamento del Modello;
- k) i principi etici e le norme di comportamento in materia di SSL.

4. IL MODELLO DI GOVERNANCE E LA STRUTTURA ORGANIZZATIVA DI UPS

Il modello di *governance* di UPS e, in generale, tutto il suo sistema organizzativo, è interamente strutturato in modo da assicurare alla Società l'attuazione delle strategie ed il raggiungimento degli obiettivi.

La struttura di UPS, infatti, è stata creata tenendo conto della necessità di dotare la Società di una organizzazione tale da garantirle la massima efficienza ed efficacia operativa.

4.1. Il modello di governance di UPS

Alla luce della peculiarità della propria struttura organizzativa e delle attività svolte, UPS ha privilegiato il c.d. sistema tradizionale.

Il sistema di *corporate governance* di UPS risulta, pertanto, attualmente così articolato:

- Assemblea dei Soci:

L'Assemblea dei Soci è competente a decidere, in sede ordinaria e straordinaria, sulle materie alla stessa riservate dalla Legge o dallo Statuto. La UPS è società sottoposta, ai sensi dell'art. 2497 c.c. alla attività di direzione e coordinamento della UPS International Inc., che detiene la partecipazione totalitaria del capitale sociale.

- Consiglio di Amministrazione:

Il Consiglio di Amministrazione è investito dei più ampi poteri per l'amministrazione della Società e per l'attuazione ed il raggiungimento dello scopo sociale, nei limiti di quanto consentito dalla Legge e dallo Statuto. Al Consiglio di Amministrazione risulta, quindi, tra l'altro, conferito il potere di definire gli indirizzi strategici della Società, nonché di verificare l'esistenza e l'efficienza dell'assetto organizzativo ed amministrativo della stessa.

Il Consiglio di Amministrazione può essere composto, a mente dello Statuto, da 3 a 7 consiglieri. Al momento dell'adozione del presente Documento i consiglieri sono 4.

- Revisione legale dei conti:

La revisione legale dei conti è esercitata da un revisore contabile o da una società di revisione iscritta nel registro istituito presso il Ministero della Giustizia.

All'atto dell'adozione del presente Modello, è stata nominata una società di revisione legale dei conti.

4.2. La struttura organizzativa

4.2.1. Definizione dell'organigramma aziendale e dei compiti

Al fine di rendere immediatamente chiaro il ruolo e le responsabilità di ciascuno nell'ambito del processo decisionale aziendale, UPS ha messo a punto un prospetto sintetico nel quale è schematizzata l'intera propria struttura organizzativa (Organigramma).

Tale documento è oggetto di costante e puntuale aggiornamento in funzione dei cambiamenti effettivamente intervenuti nella struttura organizzativa e pubblicato sulla rete intranet aziendale. I cambiamenti sono inoltre oggetto di adeguate comunicazioni organizzative.

La struttura organizzativa della Società è orientata a garantire, da un lato, la separazione di compiti, ruoli e responsabilità tra le funzioni operative e quelle di controllo, dall'altro, la massima efficienza possibile.

La Società ha poi definito delle apposte *job description* che specificano i ruoli, i compiti e le responsabilità delle principali figure impegnate nelle attività di ciascuna Direzione.

4.2.2. I Dipartimenti

La struttura organizzativa della Società è orientata a garantire, da un lato, la separazione di compiti, ruoli e responsabilità tra le funzioni operative e quelle di controllo, dall'altro, la massima efficienza possibile.

In particolare, la struttura organizzativa aziendale, che è improntata ad una precisa definizione delle competenze di ciascuna area aziendale e delle connesse responsabilità, è articolata nei seguenti Dipartimenti:

A tutti i Dipartimenti è conferito il potere di intrattenere i rapporti contrattuali con i terzi attinenti alle proprie competenze e necessari per il raggiungimento degli obiettivi assegnati.

Di seguito, sono rappresentate, in via esemplificativa, le finalità cui ogni Dipartimento è deputato.

Il Dipartimento Business Development svolge una serie di attività e si suddivide in:

- ✓ **Sales Force**: si occupa dell'intero processo di vendita, posizionando i servizi UPS ed i vantaggi che il cliente può trarne dal punto di vista del servizio ed economico.
- ✓ **BD Operation**: supporta gli Account Executives e gli Area Sales Managers nella raccolta dati dell'attività di tutta la forza vendita (visite, clienti acquisiti, dati di fatturato, nuove opportunità, etc) al fine di effettuare analisi settimanali e/o mensili, che permettano di monitorare l'andamento delle performance dei venditori, promuovere iniziative a supporto della crescita del fatturato e preparare stime di fatturato futuro.
- ✓ **BD Office**: supporta gli Account Executives e gli Area Sales Managers nelle attività amministrative e, su richiesta, presta assistenza ai clienti su eventuali problemi emersi o su richieste particolari.
- ✓ **Customer Solution Group**: si occupa di prestare attività di consulenza ai clienti per il miglioramento della Supply Chain, offrendo soluzioni tecnologiche e suggerimenti sui processi produttivi.
- ✓ **BD Training**: si occupa della progettazione ed erogazione in aula di interventi formativi rivolti specificamente alla forza vendita.

Il Dipartimento Finance & Accounting è deputato a svolgere una serie di funzioni ed ha al suo interno diversi gruppi di lavoro:

- **ufficio paghe e contributi (payroll)**: si occupa della gestione presenze (ferie, malattie, permessi etc) e del pagamento degli stipendi.

- contabilità generale (general ledger): gestisce le riconciliazioni dei conti patrimoniali, il pooling e il rapporto con gli Istituti Bancari, le chiusure mensili e i relativi accantonamenti. Si occupa, inoltre della Dichiarazione IVA, della Redazione del Bilancio, della gestione dei beni ammortizzabili e del Controllo delle Note spese di tutto il personale dipendente.

Tutte le attività sopra elencate non sono gestite dal reparto GL locale, che si occupa principalmente "solo" dei principali adempimenti di scadenze fiscali. Nello specifico:

- riconciliazioni conti patrimoniali: gestite da società' esterna Accenture (India)
- Pooling e rapporto con banche: Tesoreria UPS di Londra (UK)
- Chiusure mensili e accantonamenti: Accenture (India)
- Dichiarazione Iva: società' Ernest Young - (India)
- Gestione beni ammortizzabili: Accenture (India)
- Controllo note spese: UPS GBS AP (India)

- contabilità fornitori (accounts payable): si occupa della gestione contabile delle fatture dei fornitori e del loro pagamento e della gestione contabile delle fatture intercompany. È responsabile degli acquisti e del pagamento danni ai clienti.

Tutta l'attività è gestita all'estero:

- fatture fornitori (incluso pagamento danni): UPS GBP Lodz (Polonia)
- fatture intercompany: Accenture (India)

- contabilità clienti (accounts receivable): gestisce da un punto di vista contabile gli incassi ricevuti tramite bonifico bancario e assegno a pagamento delle nostre fatture.

Il processo è svolto in UPS GBS AR Polonia e India.

- finance: è responsabile della preparazione del budget e del controllo di gestione oltreché di tutta l'attività di Reporting.

- cash on delivery (cod): si occupa della gestione contabile degli incassi ricevuti tramite le filiali e rimessa ai clienti delle somme dovute come Contrassegni. Gestisce, inoltre, i rimborsi per i pagamenti superiori all'importo dovuto e le comunicazioni ai clienti che necessitano di chiarimenti sulle loro posizioni contabili.

Il processo è svolto in UPS GBS COD e AR Polonia.

- recupero crediti (collection): si occupa del sollecito telefonico dei clienti regolari ed occasionali, relativamente alle fatture non pagate alla scadenza contrattuale; del controllo e della gestione del fornitore incaricato di recuperare gli importi insoluti a mezzo visite esattoriali ed infine della gestione delle pratiche legali curate da legale esterno.
- fatturazione (billing): si occupa del controllo, della preparazione e dell'audit dei documenti di spedizione. Gestisce inoltre i flussi informatici del sistema di fatturazione e la eventuale soluzione di discrepanze nello stesso al fine di consentire la corretta fatturazione di ogni spedizione effettuata.

Il Dipartimento Call Center risponde ad un numero unico per tutta Italia ed è diviso in 5 sottogruppi di lavoro a seconda della tipologia di chiamata gestita:

- ✓ Pick Up: per tariffe, tempi di transito e ordini di ritiro
- ✓ Tracking: per informazioni sullo stato delle spedizioni
- ✓ Universal: per informazioni di tipo generale e per problematiche composite.
- ✓ CRG (Customer Resolution group) che gestisce problematiche pacchi internazionali e apertura indagini e gestione pratiche Legali, PEC, ODR, GSR (area Amministrativa)
- ✓ Gruppo email, che gestisce richieste via e-mail
- ✓ Social Media, interagisce con clienti tramite canali social di UPS

All'interno del gruppo call center troviamo inoltre i gruppi Planner e Training.

Il Dipartimento Pca (Preferred Customer Associate) è l'interlocutore dedicato e specializzato all'assistenza di clienti selezionati.

Il Dipartimento Human Resources è deputato a gestire le seguenti attività:

- ✓ gestione del personale: racchiude dall'attività di ricerca e selezione del personale alla gestione e amministrazione quotidiana di tutto il personale dipendente (assunzioni, trasferimenti, cessazioni, variazioni contrattuali, ecc). Altre attività sono correlate alla gestione delle politiche retributive e dell'autoparco aziendale.
- ✓ Formazione/comunicazione interna: vale a dire tutte le attività formative, siano esse effettuate dall'interno che da società esterne e relative alla comunicazione interna.

- ✓ Legale: in quest'area rientrano la gestione del contenzioso legale, l'applicazione delle norme contrattuali.
- ✓ Benefits & Compensation: rientrano in quest'area le politiche di gestione retributiva e di benefit per i dipendenti.

Il Dipartimento Health and Safety (H&S) è deputato alla gestione dell'area Sicurezza sul Lavoro, valutando i rischi presenti in Azienda e individuando le misure da adottare, al fine di garantire la sicurezza e la salute dei lavoratori.

Il Dipartimento Labor si occupa della gestione delle relazioni sindacali, sia relativamente ai lavoratori diretti che agli indiretti (dipendenti di società terze, quali autisti, facchini..).

Il Dipartimento Security & Delivery è deputato a svolgere una serie di funzioni e per il tramite di:

A) Il **Delivery Information Dept** che a sua volta è diviso in 4 diversi sottogruppi:

- ✓ tracing: gestisce le richieste di informazione da parte dei clienti che non possono essere evase dal Call Center, ricercando i pacchi che non hanno informazioni a video.
- ✓ claims/reclami: gestiscono i rimborsi relativi alle spedizioni perse o danneggiate
- ✓ giacenze: si occupa di ottenere dai clienti e fornire alle filiali le informazioni che permettono lo sblocco della giacenza e la conclusione positiva della spedizione.
- ✓ overgood: si occupa della gestione e della verifica dei pacchi che all' interno del network risultano privi di riferimento del mittente/destinatario che consente il corretto instradamento della spedizione. Vengono inoltre gestiti i pacchi con scaduti termini di giacenza in filiale e gli abbandoni.

B) La **Security** che è il reparto che ha lo scopo di tutelare il patrimonio aziendale e le spedizioni affidate dai clienti per la movimentazione. L'attività si può riassumere in 3 fasi :

- ✓ Prevenzione di atti illeciti provenienti dall' interno o dall'esterno dell' organizzazione causati per danneggiare la società
- ✓ Viene effettuata con strumenti strutturali (tecnologie quali sistemi di allarme, sistemi di videosorveglianza e controllo accessi) o strumenti culturali (training , procedure, security awareness,auditing, sviluppo delle fonti, relazioni professionali con FF.OO.)
- ✓ Investigazione per accertare modalità e responsabilità degli atti illeciti che avviene tramite raccolta di dati oggettivi, interviste, accertamenti, sopralluoghi, analisi di report
- ✓ Prosecuzione per denunciare gli atti illeciti alle autorità giudiziarie e/o allontanare chi é stato riconosciuto come l'autore degli atti illeciti

L'Aviation security è il reparto che si occupa della conformità delle operazioni di esportazione del volume internazionale espresso via aerea, nell'ambito delle regolamentazioni vigenti per quanto riguarda la sicurezza aerea; garantisce pertanto la conformità degli obblighi di UPS, quale Agente Regolamentato che opera in autonomia, nell'ambito dell'inoltro sicuro delle merci che viaggiano su aeromobile.

Supervisiona l'attività degli addetti al controllo radiogeno appartenenti a società esterna in conformità agli standard UPS e dell'autorità aerea civile.

Il Dipartimento Marketing è deputato a svolgere una serie di attività e si compone sostanzialmente di 3 aree:

- ✓ L'Operational Marketing, che si compone dei due sotto gruppi 1) Revenue Management e 2) Planning. Il Revenue Managment é la funzione aziendale che ha come obiettivo la massimizzazione della profittabilità aziendale attraverso la gestione del fatturato e, più nello specifico, le scontistiche concesse ai singoli clienti. Il reparto Planning si occupa principalmente della preparazione del Business Plan e l'analisi dei dati a consuntivo. Il Business Plan é lo strumento attraverso il quale l'Azienda stabilisce i propri obiettivi di fatturato e volume per servizio, individuandone le strategie per il suo conseguimento.
- ✓ Il Customer Marketing si occupa del monitoraggio del mercato, i competitor e l'evoluzione delle preferenze dei clienti. L'obiettivo finale é l'identificazione di nuove tendenze affinché UPS possa proporre i servizi e la customer

experience più in linea con queste ultime, guadagnando quota di mercato. Questo obiettivo viene raggiunto attraverso l'elaborazione di iniziative e proposte atti alla penetrazione di determinati segmento di mercato, nonché lavorando direttamente sui singoli clienti in team con la forza vendita, trovando la proposta più idonea per le esigenze del cliente sotto esame.

- ✓ L'external communication: si occupa di verificare come l'azienda comunica all'esterno la propria immagine e il proprio marchio. Coordina le attività di advertising (realizzate da un'agenzia esterna), di direct marketing (mailing e newsletter), di digital marketing (social media, la gestione del profilo UPS principalmente Facebook e LinkedIn) e le public relations (rapporti con la stampa, organizzazione di eventi, convegni, ecc).

Il Dipartimento TSG fornisce un supporto tecnico per clienti interni ed esterni. Il supporto tecnico include, ma non è strettamente limitato, ai seguenti aspetti:

- ✓ Mantenimento in efficienza degli asset IT (pc, stampanti, etc)
- ✓ Rinnovo degli asset obsolete (PC, stampanti, device multifunzioni)
- ✓ Configurazione di sistemi
- ✓ Sviluppo e integrazione di sistemi di spedizione (come WorldShip, CampuShip) per la clientele
- ✓ Formazione di nuovi Access Points

Il Dipartimento Public Affairs ha la responsabilità di rappresentare, attraverso la comunicazione, l'azienda e la sua reputazione nell'ambito di contesti diversi da quelli strettamente connessi al mondo del trasporto, in particolare all'interno del contesto politico-legislativo. una delle finalità è quella di rappresentare adeguatamente la posizione di UPS, come importante realtà aziendale che opera sul territorio italiano e come tale soggetta a norme, leggi e responsabilità.

Il Dipartimento Industrial Engineering è deputato a svolgere un ruolo di consulenza interna all'azienda per lo sviluppo e l'implementazione di tutte le soluzioni che meglio soddisfano le esigenze dei clienti a tariffe competitive. Il Dipartimento è strutturato in 2 distinte sezioni:

- ✓ operations improvement section che si occupa dell'analisi organizzativa del lavoro, dell'analisi dei metodi, delle relative descrizioni e standardizzazioni, e della stesura di piani operativi.

- ✓ b&f/r.e./data management /sistems section che si occupa di training e supporto tecnologico dei sistemi, della gestione delle infrastrutture (Building & Facility e Real Estate), del controllo e dell'approvazione dei costi (REFCO / RFA), comprendendo la gestione operativa dei dati e delle informazioni ad essi collegate (Data Management) ed il relativo controllo secondo i parametri aziendali (Auditing e Reporting).

Il Dipartimento Building and Systems Engineering è responsabile della progettazione, costruzione e manutenzione di tutti i servizi UPS e delle attrezzature di smistamento. Plant Engineering è anche responsabile per lo sviluppo di tutela dell'ambiente, e le norme di sicurezza che garantiscono che UPS sia sempre conforme ai requisiti normativi. Progettazione, costruzione, manutenzione, ambiente, beni regolamentati e norme di sicurezza vengono definiti a livello Corporate e l'attuazione degli standard è effettuata a livello di Region e District. Le competenze principali del Plant Engineering sono l'ingegneria di processo, gestione della costruzione, il rispetto delle norme di sicurezza, protezione dei beni ed energia.

Il Dipartimento Transportation si compone delle seguenti funzioni:

- ✓ brokerage: è il dipartimento che prepara l'ingresso e l'uscita in Italia dei colli in arrivo e partenza che devono essere prima sdoganati e poi consegnati.
- ✓ Air: si occupa di tutte le operazioni di smistamento merci in arrivo negli aeroporti per le filiali collegate e viceversa di tutte le operazioni di consolidamento merci in partenza dall'Italia. Si occupa anche di tutte le operatività collegate agli aeromobili (gestione voli, carico e scarico aeromobili).
- ✓ Hub: all'interno degli Hubs, dove le spedizioni raccolte dalle filiali giungono attraverso i Feeder (camion), queste vengono smistate a seconda della località di destino, per essere poi ricaricate sui mezzi
- ✓ Feeders & Network planning: i Feeders, secondo uno schedulato, garantiscono il collegamento tra Hubs, Gateway e filiali mentre il Network planning si occupa della pianificazione del network (schedulato), e della sua ottimizzazione (creazione o eliminazione di nuove linee di traffico).

Il **Dipartimento Outside Service Provider Support Group (OSPSG)** si occupa della gestione di ogni rapporto tra la UPS e le società fornitrici di servizi operativi (società di trasporto che consegnano, ritirano e trasferiscono pacchi per nostro conto; società di facchinaggio che movimentano pacchi all'interno dei nostri magazzini;). Gestire, sotto ogni profilo, i rapporti con le società esterne, significa occuparsi degli aspetti amministrativi, legali, operativi, statistici ed informatici ad esse correlati.

Il **Dipartimento Procurement** é responsabile dell'attività di sourcing delle attività esternalizzate.

Le procedure sono quelle corporate, appositamente regionalizzate e la modalità di sourcing standard é il tender.

Il Procurement si occupa di relazionarsi con gli attuali partner OSP (esclusivamente nell'ambito delle attività di pick up e delivery) ed i potenziali OSP candidati.

Il Procurement effettua analisi delle attività da sottoporre al processo di sourcing.

Il Procurement tiene aggiornata la lista dei potenziali OSP, monitora costantemente il mercato ed é responsabile delle negoziazioni relative alle tariffe/compensi degli OSP. Il Procurement ha la responsabilità di definire I termini di pagamento per gli OSP.

Il **Dipartimento Access Point** si occupa di identificare e gestire I negozi terzi che accettano di collobarare con UPS per la spedizione e la ricezione dei pacchi, il reparto é suddiviso in coordinatori esterni (APSR) e operatrici interne (APSIR) che rispettivamente si occupano di :

- APSR : identificare I negozi da inserire nel Network in base alle caratteristiche richieste e provvedere alla loro formazione , inoltre si occupano di gestire parte delle problematiche operative; sono previste visite trimestrali ad ogni negozio per garantire il mantenimento e la qualità del Network
- APSIR : fornire agli Access Point assistenza sia amministrativa che operativa , assistenza che viene fornita sia telefonicamente che tramite email,inoltre supportano I coordinatori durante le varie fasi dell'implementazione dei nuovi negozi e eventuali cessazioni di collaborazione.

I Package Centers sono le filiali sparse sul territorio nazionale, le cui dimensioni possono variare a seconda del territorio e del volume gestito. Le filiali sono responsabili per lo smistamento e la consegna/ritiro puntuale dei pacchi dei nostri Clienti in un'area geografica designata.

Deve aggiungersi, infine, che alcune funzioni - tra cui la funzione Legal - sono centralizzate a livello di gruppo e forniscono un'assistenza *day to day* all'azienda.

Il Dipartimento Compliance che si occupa di garantire che le operazioni aziendali siano eseguite in conformità con le leggi, i regolamenti e le procedure pertinenti.

4.2.3 Gli organi collegiali interni

Nell'ambito della struttura organizzativa di UPS, assumono anche rilevanza i comitati interni sono funzionali alla messa a punto ed allo sviluppo di alcuni processi aziendali che consigliano la condivisione da parte di più soggetti. Mediante la costituzione dei comitati interni, difatti, la Società intende perseguire l'obiettivo di un significativo aumento della cultura del controllo in seno alla propria organizzazione, rappresentando detti comitati lo strumento ritenuto idoneo a garantire un'ulteriore e maggiormente efficiente applicazione del principio di segregazione delle funzioni.

In particolare, si segnalano:

Comitato BPT (Business Planning Team)

Si tratta di un comitato costituito nell'ambito della procedura deputata alla selezione dei fornitori. È costituito da tutte le funzioni interessate (Operativo, I. E, Dept., Security, OSP) e guidato dal Country Manager.

Si tratta di un comitato costituito dalle funzioni di HR, IE, F&A, BD, Marketing, Country Manager e la finalità è quella di applicare le strategie comunicate dal gruppo di coordinamento District Business Planning Team composto dalle stesse funzioni italiane a livello District.

Sue finalità sono inoltre quelle di favorire lo sviluppo strategico del business aziendale e il raggiungimento dei business goals, con un focus su revenue, profit, prodotti e servizi aziendali.

Comitato Staff

Composto dai responsabili dei Dipartimenti, si riunisce periodicamente per discutere delle principali tematiche che interessano l'azienda.

4.2.4. La Struttura Organizzativa in materia di Salute e Sicurezza sul Lavoro (*rinvio*)

Fermo restando l'approfondimento che sarà svolto nella Parte Speciale, deve intanto osservarsi che in materia di salute e sicurezza sul lavoro, la Società si è dotata di una struttura organizzativa conforme a quella prevista dalla normativa prevenzionistica vigente, nell'ottica di eliminare ovvero, laddove ciò non sia possibile, ridurre – e, quindi, gestire - i rischi lavorativi per i lavoratori.

Nell'ambito di tale struttura organizzativa, operano i soggetti di seguito indicati:

- 1) il datore di lavoro;
- 2) i dirigenti;
- 3) il responsabile servizio di prevenzione e protezione (di seguito, rispettivamente anche 'RSPP');
- 4) gli addetti al primo soccorso (di seguito, anche 'APS');
- 5) gli addetti alla prevenzione degli incendi (di seguito, anche 'API');
- 6) i rappresentanti dei lavoratori per la sicurezza (di seguito, anche 'RLS');
- 7) il medico competente;
- 8) i lavoratori;
- 9) i soggetti esterni all'azienda, ovvero: a) i soggetti cui è affidato un lavoro in virtù di contratto d'appalto o d'opera; b) i fornitori; c) i progettisti dei luoghi e dei posti di lavoro e degli impianti; d) gli installatori ed i montatori di impianti, attrezzature di lavoro o altri mezzi tecnici.

I compiti e le responsabilità dei soggetti sopra indicati in materia di SSL sono definiti formalmente in coerenza con lo schema organizzativo e funzionale della Società, con particolare riferimento alle figure specifiche operanti in tale ambito (i RSPP, gli APS, gli API, i RLS, il medico competente): a tale proposito, la Società esplicita, in sede di definizione dei compiti organizzativi e operativi dell'intero ente, anche quelli relativi alle attività di sicurezza di rispettiva competenza, nonché le responsabilità connesse all'esercizio delle attività stesse, con particolare riguardo ai compiti dei RSPP, del RLS, degli APS, degli API, dei RLS, del medico competente.

5.1. I principi generali

Così come richiesto dalla buona pratica aziendale e specificato anche nelle Linee Guida di Confindustria, nell'ultima versione del 2014, il Consiglio di Amministrazione di UPS è l'organo preposto a conferire ed approvare formalmente le deleghe ai singoli consiglieri; i poteri di firma poi sono assegnati in coerenza con le responsabilità organizzative e gestionali definite e, ove attribuito il relativo potere, con una puntuale indicazione delle soglie di approvazione delle spese.

Il livello di autonomia, il potere di rappresentanza ed i limiti di spesa assegnati ai vari titolari di deleghe e procure all'interno della Società risultano sempre individuati. Essi sono fissati in modo coerente con il ruolo o con il livello gerarchico del destinatario della delega o della procura nei limiti di quanto strettamente necessario all'espletamento dei compiti e delle mansioni da assegnare.

I poteri così conferiti vengono periodicamente aggiornati in funzione dei cambiamenti organizzativi che intervengono nella struttura della Società.

La Società ha, inoltre, istituito un flusso informativo, nei dell'OdV, al fine di garantire la tempestiva comunicazione dei cambiamenti organizzativi.

5.2. La struttura del sistema di deleghe e procure in UPS

Il sistema di deleghe e procure attualmente in vigore in UPS ripercorre il quadro che emerge dall'Organigramma aziendale, sovrapponendosi esattamente allo stesso ed integrandolo, per quanto eventualmente necessario al fine di conferire attribuzioni o compiti a soggetti che non rivestono ruoli apicali.

Il Consiglio di Amministrazione di UPS ha nominato un Amministratore Delegato con attribuzione di ampi poteri afferenti il coordinamento e la direzione dell'attività di gestione della Società, nonché il compimento diretto dei principali e più rilevanti atti sociali.

L'Amministratore Delegato, a sua volta, ha effettuato pari conferimenti ai responsabili di alcune funzioni e ciò in stretta relazione con le mansioni e l'attività

svolta da ciascuno di essi. Sono state, quindi, conferite le procure con importi differenziati in funzione del ruolo rivestito in seno all'organizzazione da esercitare nei limiti e nell'ambito delle competenze del Dipartimento di appartenenza e per le competenze e responsabilità specifiche assegnate a ciascun assegnatario.

Le procure sono anche analizzate dal Legal del gruppo e/o dai consulenti esterni.

Le linee generali a cui si attengono gli atti conferimento di poteri di firma sono:

- 1) indicazione del soggetto delegante e fonte del suo potere di delega o procura;
- 2) indicazione del soggetto delegato, con esplicito riferimento alla funzione ad esso attribuita ed il legame tra le deleghe e le procure conferite e la posizione organizzativa ricoperta dal soggetto delegato;
- 3) indicazione dell'oggetto, costituito dalla elencazione delle tipologie di attività e di atti per i quali la delega/procura viene conferita. Tali attività ed atti sono sempre funzionali e/o strettamente correlati alle competenze e funzioni del soggetto delegato;
- 4) ove attribuito, indicazione dei limiti di valore entro cui il delegato è legittimato ad esercitare il potere conferitogli. Tale limite di valore è determinato in funzione del ruolo e della posizione ricoperta dal delegato nell'ambito dell'organizzazione aziendale.

Le deleghe e le procure in UPS vengono raccolte ed organizzate secondo la struttura aziendale a cui corrispondono e sono sempre a disposizione delle varie funzioni dell'azienda, ovvero dei terzi legittimati ad accedervi (previa verifica della sussistenza di un effettivo interesse), presso la sede della Società.

Il sistema delle deleghe e dei poteri di firma viene aggiornato, in ragione delle modifiche intervenute nella struttura aziendale, in modo da risultare il più possibile coerente con l'organizzazione gerarchico-funzionale e le esigenze della Società.

6. PROCEDURE MANUALI ED INFORMATICHE

Nell'ambito del proprio sistema organizzativo, UPS si è impegnata a mettere a punto un complesso di procedure, sia manuali e sia informatiche, volto a

regolamentare lo svolgimento delle attività aziendali, nel rispetto dei principi indicati dalle Linee Guida di Confindustria.

In particolare, le procedure approntate dalla Società, sia manuali e sia informatiche, costituiscono le regole da seguire in seno ai processi aziendali interessati, prevedendo anche i controlli da espletare al fine di garantire la correttezza, l'efficacia e l'efficienza delle attività aziendali.

In questo contesto, pertanto, la Società assicura il rispetto dei seguenti principi:

- favorire il coinvolgimento di più soggetti, onde addivenire ad una adeguata separazione dei compiti mediante la contrapposizione delle funzioni;
- adottare le misure volte a garantire che ogni operazione, transazione, azione sia verificabile, documentata, coerente, congrua;
- prescrivere l'adozione di misure volte a documentare i controlli espletati rispetto alle operazioni e/o alle azioni effettuate.

Le procedure, oltre ad essere diffuse e pubblicizzate presso i servizi/funzioni interessati attraverso specifica comunicazione e formazione, vengono raccolte e poste a disposizione di tutti i soggetti aziendali sia a mezzo della pubblicazione sulla intranet aziendale e sia presso la sede della Società.

Per ciò che concerne le procedure in materia di gestione e prevenzione dei rischi in tema di SSL, un maggiore approfondimento sarà effettuato al par. 8 della Parte Speciale.

7. IL BUDGET ED IL CONTROLLO DI GESTIONE

Il sistema di controllo di gestione della Società prevede meccanismi di verifica della gestione delle risorse che devono garantire, oltre che la verificabilità e tracciabilità delle spese, l'efficienza e l'economicità delle attività aziendali, mirando ai seguenti obiettivi:

- definire in maniera chiara, sistematica e conoscibile tutte le risorse a disposizione delle funzioni aziendali nonché l'ambito in cui le stesse possono essere impiegate, attraverso la programmazione e definizione del *budget*;
- rilevare gli eventuali scostamenti rispetto a quanto predefinito in sede di *budget*, analizzarne le cause e riferire i risultati delle valutazioni ai livelli gerarchicamente responsabili al fine di predisporre i più opportuni interventi di adeguamento, attraverso la relativa consuntivazione.

7.1. Investimenti in materia di Salute e Sicurezza sul lavoro

La Società, fin dalla sua costituzione in Italia e anche in seguito, ha sempre dedicato una grande attenzione all'allocazione delle opportune risorse economiche per garantire l'assoluta sicurezza dei luoghi di lavoro.

Prendendo ad esempio anche solo l'ultimo quadriennio (2014-2018), la Società ha investito oltre 20.000.000,00 € per attività relative alla manutenzione sia ordinaria che straordinaria anche degli immobili nonché per le attività volte ad assicurare la corretta applicazione delle normative in tema di salute e sicurezza sul lavoro. Parte significativa delle risorse, inoltre, è destinata alla necessaria consulenza specialistica di primarie società di consulenza.

8. IL SISTEMA DI CONTROLLO SULLA SALUTE E SICUREZZA SUL LAVORO

8.1. La gestione operativa in materia di Salute e Sicurezza sul Lavoro

La gestione delle questioni connesse alla salute ed alla sicurezza sul lavoro è effettuata con l'obiettivo di provvedere in via sistematica:

- ✓ all'identificazione dei rischi ed alla loro valutazione;
- ✓ all'individuazione delle misure di prevenzione e di protezione adeguate rispetto ai rischi riscontrati, affinché questi ultimi siano eliminati ovvero, ove ciò non sia possibile, siano ridotti al minimo – e, quindi, gestiti - in relazione alle conoscenze acquisite in base al progresso tecnico;
- ✓ alla limitazione al minimo del numero di lavoratori esposti a rischi;
- ✓ alla definizione di adeguate misure di protezione collettiva e individuale, fermo restando che le prime devono avere priorità sulle seconde;
- ✓ al controllo sanitario dei lavoratori in funzione dei rischi specifici;

- ✓ alla programmazione della prevenzione, mirando ad un complesso che integri in modo coerente le condizioni tecniche e produttive dell'azienda con l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro, nonché alla successiva realizzazione degli interventi programmati;
- ✓ alla formazione, all'addestramento, alla comunicazione ed al coinvolgimento adeguati dei destinatari del Modello, nei limiti dei rispettivi ruoli, funzioni e responsabilità, nelle questioni connesse alla SSL;
- ✓ alla regolare manutenzione di ambienti, attrezzature, macchine e impianti, con particolare riguardo alla manutenzione dei dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti.

Le modalità operative per il concreto svolgimento delle attività ed il raggiungimento degli obiettivi sopra indicati sono definite nelle procedure aziendali, redatte in conformità alla normativa prevenzionistica vigente, le quali assicurano l'adeguata tracciabilità dei processi e delle attività svolte (si veda anche il par. 8 della Parte Speciale).

In ogni caso, il sistema predisposto dalla Società prevede la puntuale definizione dei compiti, dei doveri e delle responsabilità spettanti a ciascuna categoria di soggetti coinvolti nel settore della SSL, a partire dal datore di lavoro fino al singolo lavoratore.

In questo senso, sono stati considerati anche i seguenti profili:

- ✓ l'assunzione e la qualificazione del personale;
- ✓ l'organizzazione del lavoro e delle postazioni di lavoro;
- ✓ l'acquisizione dei beni e dei servizi impiegati dall'azienda e la comunicazione delle opportune informazioni a fornitori ed appaltatori;
- ✓ la manutenzione normale e straordinaria delle attrezzature, degli impianti, dei mezzi di prevenzione e dei dispositivi di protezione collettiva ed individuale;
- ✓ la qualificazione e la scelta dei fornitori e degli appaltatori;
- ✓ l'efficiente gestione delle emergenze;
- ✓ le modalità da seguire per affrontare le difformità riscontrate rispetto agli obiettivi fissati ed alle previsioni del sistema di controllo.

Sempre con riguardo alla SSL, è predisposto un sistema di flussi informativi che consente la circolazione delle informazioni all'interno dell'azienda, al fine sia di

favorire il coinvolgimento e la consapevolezza di tutti i destinatari del Modello, nei limiti dei rispettivi ruoli, funzioni e responsabilità, sia di assicurare la tempestiva ed adeguata evidenza di eventuali carenze o violazioni del Modello stesso, così come degli interventi necessari al suo aggiornamento.

Il sistema di gestione implementato dalla Società con riferimento alla SSL è conforme ai requisiti previsti dai più elevati standard di qualità riconosciuti a livello nazionale ed internazionale, inclusi i requisiti indicati dalle Linee Guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 così come suggerito dall'art. 30 del TU SSL.

Un ulteriore dettaglio sarà poi fornito al paragrafo 8 della Parte Speciale.

8.2. Il sistema di monitoraggio della sicurezza (rinvio)

La Società ha rivolto particolare attenzione alla esigenza di predisporre ed implementare, in materia di SSL, un efficace ed efficiente sistema di controllo.

Quest'ultimo, oltre a prevedere la registrazione delle verifiche svolte dalla Società, anche attraverso la redazione di appositi verbali, è incentrato su un sistema di monitoraggio della sicurezza che si sviluppa su un duplice livello.

Il primo livello di monitoraggio è svolto dalle funzioni che operano nell'ambito della struttura organizzativa. Il secondo livello di monitoraggio - come pure previsto dalle Linee Guida - è effettuato dall'Organismo di Vigilanza.

Il dettaglio sarà poi fornito al paragrafo 8 della Parte Speciale.

9. L'ORGANISMO DI VIGILANZA

9.1. La nomina, la composizione dell'Organismo di Vigilanza ed i suoi requisiti

Il Consiglio di Amministrazione di UPS ha provveduto alla nomina di un Organismo di Vigilanza, nel rispetto delle previsioni di cui alle Linee Guida di Confindustria.

Si tratta di un Organismo collegiale composto da 2 membri esterni ossia:

- un esperto in materia legale/penale con particolare focus alla responsabilità amministrativa da reato;
- un esperto in materia di salute e sicurezza sui luoghi di lavoro ed ambiente.

I componenti dell'OdV (con la specificazione del membro che ricopre il ruolo di Presidente) sono nominati dal Consiglio di Amministrazione che con la medesima delibera fissa il compenso spettante ai membri dell'OdV per l'incarico a ciascuno assegnato.

La nomina dell'OdV, i suoi compiti ed i suoi poteri, sono oggetto di tempestiva comunicazione alla Società.

L'OdV di UPS, in ossequio a quanto previsto dalle Linee Guida di Confindustria, risponde ai seguenti requisiti, che si riferiscono all'Organismo in quanto tale e caratterizzano la sua azione:

- autonomia e indipendenza: è previsto che l'OdV sia privo di compiti operativi, i quali potrebbero ledere l'obiettività di giudizio e non sia soggetto al potere gerarchico e disciplinare di alcun organo o funzione societari;
- professionalità: intesa come insieme di strumenti e tecniche necessarie allo svolgimento dell'attività assegnata;
- continuità di azione: l'OdV è provvisto di un adeguato budget e di adeguate risorse ed è dedicato esclusivamente all'attività di vigilanza in modo che sia garantita una efficace e costante attuazione del Modello;
- onorabilità ed assenza di conflitti di interessi: negli stessi termini previsti dalla Legge con riferimento ad amministratori e membri del Collegio Sindacale.

9.2 I casi di ineleggibilità e decadenza

I componenti dell'OdV sono scelti tra i soggetti, anche esterni all'Ente, qualificati ed esperti in ambito legale, di sistemi di controllo interno ed in materia di salute e sicurezza sui luoghi di lavoro.

Costituiscono motivi di ineleggibilità e/o decadenza del componente l'OdV:

- i) l'interdizione, l'inabilitazione, il fallimento o, comunque, la condanna penale, anche non passata in giudicato, per uno dei reati previsti dal Decreto o, comunque, ad una delle pene di cui all'art. 2 del D.M. 30 marzo 2000, n. 162, ovvero che importi l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità di esercitare uffici direttivi;

- ii) l'esistenza di relazioni di parentela, coniugio o affinità entro il quarto grado con i membri del Consiglio di Amministrazione di UPS, nonché con i medesimi membri degli altri Enti dello stesso Gruppo o con i soggetti esterni incaricati della revisione;
- iii) fatto salvo l'eventuale rapporto di lavoro subordinato, l'esistenza di rapporti di natura patrimoniale tra il componente e l'Ente o altri Enti dello stesso Gruppo, tali, per natura e valore economico, da compromettere l'indipendenza del componente stesso possono considerarsi le best practice, emanate dal Nazionale dei Dottori Commercialisti e degli Esperti Contabili per il Collegio Sindacale.

Qualora, nel corso dell'incarico, dovesse sopraggiungere una causa di decadenza, il componente è tenuto ad informare immediatamente il Consiglio di Amministrazione.

I requisiti di eleggibilità e/o le ipotesi di decadenza sono estesi anche alle risorse di cui l'OdV si avvale direttamente nell'espletamento delle proprie funzioni.

9.3. La durata dell'incarico e le cause di cessazione

L'incarico dell'OdV è conferito per la durata di tre anni e può essere rinnovato.

La cessazione dall'incarico dell'OdV, inteso come organo unitario, può avvenire per una delle seguenti cause:

- i) scadenza dell'incarico;
- ii) revoca dell'OdV da parte del Consiglio di Amministrazione;
- iii) rinuncia di tutti i componenti dell'OdV, formalizzata mediante apposita comunicazione scritta inviata al Consiglio di Amministrazione.

La revoca dell'OdV quale organo può avvenire solo per giusta causa, anche al fine di garantirne l'assoluta indipendenza.

Per giusta causa di revoca possono intendersi, in via non esaustiva:

- i) una grave negligenza nell'espletamento dei compiti connessi all'incarico;

- ii) il possibile coinvolgimento della Società in un procedimento, penale o civile, che sia connesso ad una omessa o insufficiente vigilanza.

La revoca per giusta causa è disposta con delibera del Consiglio di Amministrazione.

In caso di scadenza, revoca o rinuncia, il Consiglio di Amministrazione nomina senza indugio il nuovo OdV.

Al di fuori delle ipotesi riguardanti l'intero OdV, la cessazione dell'incarico di un singolo componente può avvenire:

- a seguito di revoca per giusta causa dell'incarico da parte del Consiglio di Amministrazione;
- a seguito di rinuncia all'incarico, formalizzata mediante apposita comunicazione scritta inviata al Consiglio di Amministrazione;
- qualora sopraggiunga una delle cause di decadenza di cui al successivo paragrafo.

Per giusta causa di revoca devono intendersi, oltre le ipotesi sopra previste per l'intero Organismo, a titolo esemplificativo, anche le seguenti ipotesi:

- a) il caso in cui il singolo componente sia coinvolto in un processo penale avente ad oggetto la commissione di un delitto;
- b) il caso in cui sia riscontrata la violazione degli obblighi di riservatezza previsti a carico dei membri dell'OdV;
- c) il caso di assenza ingiustificata per più di tre volte consecutive alle riunioni dell'OdV.

In ogni caso, la revoca è disposta con delibera del Consiglio di Amministrazione. In caso di cessazione di un singolo componente, per le cause sopra previste o per rinuncia del membro stesso, questi rimane in carica fino alla sua sostituzione, a cui provvede senza indugio il Consiglio di Amministrazione. Il membro nominato in sostituzione scade unitamente agli altri componenti dell'OdV.

9.4. Le risorse dell'Organismo di Vigilanza

Il Consiglio di Amministrazione assegna all'OdV le risorse umane e finanziarie ritenute opportune ai fini dello svolgimento dell'incarico assegnato. In particolare, l'Ente può avvalersi di risorse esterne esperte in materia di *internal auditing*, compliance, penale, salute e sicurezza sui luoghi di lavoro, ecc.

In ogni caso, ove necessario, il Consiglio di Amministrazione può assegnare ulteriori risorse all'Ente su indicazione dell'OdV, in numero adeguato rispetto alle dimensioni dell'Ente ed ai compiti spettanti all'OdV stesso.

Tutte le risorse assegnate, pur continuando a riportare al proprio referente gerarchico, riportano all'OdV per ciò che concerne le attività espletate per suo conto.

Con riguardo alle risorse finanziarie, l'OdV potrà disporre, per ogni esigenza necessaria al corretto svolgimento dei suoi compiti, del *budget* che l'Organo Amministrativo provvede ad assegnargli con cadenza annuale, su proposta dell'OdV stesso.

Qualora ne ravvisi l'opportunità, nel corso del proprio mandato, l'OdV può chiedere al Consiglio di Amministrazione, mediante comunicazione scritta motivata, l'assegnazione di ulteriori risorse umane e/o finanziarie.

In aggiunta alle risorse sopra indicate, l'OdV può avvalersi, sotto la propria diretta sorveglianza e responsabilità, dell'ausilio di tutte le strutture dell'Ente, così come di consulenti esterni; per questi ultimi, il compenso è corrisposto mediante l'utilizzo delle risorse finanziarie assegnate all'OdV.

9.5. I compiti e i poteri

Stante le funzioni precipuamente individuate dal Decreto in capo all'Organismo di Vigilanza, vale a dire di controllare il funzionamento e l'osservanza del Modello e curarne l'aggiornamento, spettano all'OdV i seguenti compiti:

- 1) di verifica e vigilanza sul Modello, ossia:

- verificare l'adeguatezza del Modello, ovvero la sua idoneità a prevenire il verificarsi di comportamenti illeciti, nonché ad evidenziarne l'eventuale realizzazione;
- verificare l'effettività del Modello, ovvero la rispondenza tra i comportamenti concreti e quelli formalmente previsti dal Modello stesso;
- a tali fini, monitorare l'attività dell'Ente effettuando verifiche periodiche e straordinarie (cd. "spot"), nonché i relativi follow-up;

2) di aggiornamento del Modello, ossia:

- curare l'aggiornamento del Modello, proponendo, se necessario, all'Organo Amministrativo o alle funzioni dell'Ente eventualmente competenti l'adeguamento dello stesso, al fine di migliorarne l'adeguatezza e l'efficacia, anche in considerazione di eventuali sopraggiunti interventi normativi e/o di variazioni della struttura organizzativa o dell'attività dell'Ente e/o di riscontrate significative violazioni del Modello;

3) di informazione e formazione sul Modello, ossia:

- monitorare le iniziative dirette a favorire la diffusione del Modello presso tutti i soggetti tenuti al rispetto delle relative previsioni (di seguito, anche, 'Destinatari');
- monitorare le iniziative, ivi inclusi i corsi e le comunicazioni, volte a favorire un'adeguata conoscenza del Modello da parte di tutti i Destinatari;
- riscontrare con la opportuna tempestività, anche mediante la predisposizione di appositi pareri, le richieste di chiarimento e/o di consulenza provenienti dalle funzioni o risorse ovvero dagli organi amministrativi e di controllo, qualora connesse e/o collegate al Modello;

4) di gestione dei flussi informativi da e verso l'OdV, ossia:

- assicurare il puntuale adempimento, da parte dei soggetti interessati, di tutte le attività di reporting inerenti il rispetto del Modello;
- esaminare e valutare tutte le informazioni e/o le segnalazioni ricevute e connesse al rispetto del Modello, ivi incluso per ciò che attiene le sospette violazioni dello stesso;

- informare gli organi competenti, nel proseguo specificati, in merito all'attività svolta, ai relativi risultati ed alle attività programmate;
- segnalare agli organi competenti, per gli opportuni provvedimenti, le eventuali violazioni del Modello ed i soggetti responsabili, proponendo la sanzione ritenuta più opportuna rispetto al caso concreto;
- in caso di controlli da parte di soggetti istituzionali, ivi inclusa la Pubblica Autorità, fornire il necessario supporto informativo agli organi ispettivi.

Nell'esecuzione dei compiti assegnatigli, l'OdV è sempre tenuto:

- a documentare puntualmente, anche mediante la compilazione e la tenuta di appositi registri, tutte le attività svolte, le iniziative ed i provvedimenti adottati, così come le informazioni e le segnalazioni ricevute, anche al fine di garantire la completa tracciabilità degli interventi intrapresi e delle indicazioni fornite alle funzioni dell'Ente interessate;
- a registrare e conservare tutta la documentazione formata, ricevuta o comunque raccolta nel corso del proprio incarico e rilevante ai fini del corretto svolgimento dell'incarico stesso.

Per l'espletamento dei compiti ad esso assegnati, all'OdV sono riconosciuti tutti i poteri necessari ad assicurare una puntuale ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello, nessuno escluso.

L'OdV, anche per il tramite delle risorse di cui dispone, ha facoltà, a titolo esemplificativo:

- di effettuare, anche a sorpresa, tutte le verifiche le ispezioni ritenute opportune ai fini del corretto espletamento dei propri compiti;
- di libero accesso presso tutte le funzioni, gli archivi ed i documenti dell'Ente, senza alcun consenso preventivo o necessità di autorizzazione, al fine di ottenere ogni informazione, dato o documento ritenuto necessario;
- di disporre, ove occorra, l'audizione delle risorse che possano fornire indicazioni o informazioni utili in merito allo svolgimento dell'attività dell'Ente o ad eventuali disfunzioni o violazioni del Modello;
- di avvalersi, sotto la sua diretta sorveglianza e responsabilità, dell'ausilio di tutte le strutture dell'Ente ovvero di consulenti esterni;

- di disporre, per ogni esigenza necessaria al corretto svolgimento dei suoi compiti, delle risorse finanziarie stanziare dal Consiglio di Amministrazione.

9.6. Il Regolamento dell'OdV

L'OdV, una volta nominato, redige un proprio regolamento interno volto a disciplinare gli aspetti e le modalità concreti dell'esercizio della propria azione.

In particolare, nell'ambito di tale regolamento devono essere disciplinati i seguenti profili:

- la tipologia delle attività di verifica e di vigilanza svolte;
- la tipologia delle attività connesse all'aggiornamento del Modello;
- l'attività legata all'adempimento dei compiti di informazione e formazione dei destinatari del Modello;
- la gestione dei flussi informativi da e verso l'OdV;
- il funzionamento e l'organizzazione interna dell'OdV (convocazione e decisioni dell'Organismo, verbalizzazione delle riunioni, ecc.).

Per quanto riguarda, in modo specifico, la calendarizzazione delle riunioni, il Regolamento dovrà prevedere che l'OdV si riunisca con cadenza almeno bimestrale e, comunque, ogni qualvolta lo richiedano le concrete esigenze connesse allo svolgimento delle attività proprie dell'OdV.

9.7. Il rapporto informativo da e verso l'Organismo di Vigilanza

L'OdV, deve essere tempestivamente informato da tutti i soggetti aziendali, nonché dai terzi tenuti all'osservanza delle previsioni del Modello, di qualsiasi notizia relativa all'esistenza di possibili violazioni dello stesso.

In ogni caso, devono essere obbligatoriamente e immediatamente trasmesse all'OdV le informazioni:

- I. che possono avere attinenza con violazioni, anche potenziali, del Modello, incluse, a titolo esemplificativo e non esaustivo:
 - a) eventuali ordini ricevuti dal superiore e ritenuti in contrasto con la legge, la normativa interna, o il Modello;
 - b) eventuali richieste od offerte di denaro, doni (eccedenti il valore modico) o di altre utilità provenienti da, o destinate a, pubblici ufficiali o incaricati di pubblico servizio e/o privati;

- c) eventuali scostamenti significativi dal budget o anomalie di spesa emersi dalle richieste di autorizzazione nella fase di consuntivazione del Controllo di Gestione;
- d) il budget annuale di spesa/investimento predisposto al fine di effettuare gli interventi migliorativi necessari e/o opportuni in ambito sicurezza sul lavoro;
- e) i provvedimenti e/o le notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità dai quali si evinca lo svolgimento di indagini che interessano, anche indirettamente, la Società, i dipendenti o i componenti degli organi sociali;
- f) le richieste di assistenza legale inoltrate dai dipendenti ai sensi del CCNL, in caso dell'avvio di un procedimento penale a carico degli stessi che abbia ad oggetto attività svolte nell'interesse di UPS;
- g) le notizie relative ai procedimenti disciplinari in corso e alle eventuali sanzioni irrogate ovvero la motivazione della loro archiviazione;
- h) le decisioni relative alla richiesta o alla domanda di rinnovo di licenze, certificazioni, autorizzazioni ecc.;
- i) in merito agli infortuni con prognosi maggiore o uguale a 40 giorni (o su infortuni che, anche se non gravi, si contraddistinguono per la loro ripetitività) nonché gli indici infortunistici su base annuale. L'OdV, in tali casi, potrà acquisire dal Datore di Lavoro, dall'RSPP e dai RLS:
 - a. le informazioni necessarie per verificare le cause dell'infortunio stesso;
 - b. le ragioni per le quali le misure di prevenzione e sicurezza non hanno, in tutto o in parte, funzionato;
 - c. le indicazioni circa le misure correttive che s'intendono adottare per evitare la ripetizione delle condizioni che hanno consentito l'infortunio;
 - d. i successivi riscontri circa l'effettiva adozione delle misure correttive.
- j) in merito agli aspetti sanitari, da parte del medico competente: a) indicazione delle situazioni anomale riscontrate nell'ambito delle visite periodiche o programmate (tali segnalazioni, nel rispetto delle norme sulla privacy, saranno riferite al tipo di mansione, alle sostanze utilizzate ed alla lavorazione che il medico competente ritiene possa

- avere incidenza sulla salute del lavoratore); b) programma di sorveglianza sanitaria;
- k) segnalazione tempestiva, da parte dei responsabili aziendali, di situazioni di pericolo o comunque di rischio che possano pregiudicare la salute o l'integrità fisica delle persone che operano in azienda o che possono comunque essere danneggiate a seguito di attività svolte dall'azienda;
 - l) trasmissione del verbale della Riunione annuale ex art. 35 del D. Lgs. 81/08 e del riesame della direzione relativamente al sistema di gestione della salute e sicurezza;
 - m) segnalazioni, non tempestivamente riscontrate dalle funzioni competenti, concernenti sia carenze o inadeguatezze dei luoghi, delle attrezzature di lavoro, ovvero dei dispositivi di protezione messi a disposizione della Società, sia ogni altra situazione di pericolo connesso alla salute ed alla sicurezza sul lavoro;
 - n) eventuali aggiornamenti del DVR o del DUVRI o di altri documenti rilevanti in tema SSL (piano emergenze, ecc.);
 - o) relazione scritta annuale da parte del RSPP contenente la descrizione della situazione delle unità locali per quanto riguarda l'igiene e sicurezza sul lavoro: stato del sistema di prevenzione e protezione implementato in azienda; effettuazione degli interventi formativi in materia di sicurezza, prevenzione ed igiene del lavoro, ovvero segnalazione della mancata effettuazione di quelli programmati, indicandone le ragioni; la prevenzione incendi e la tutela dell'ambiente;
 - p) relazioni scritte su base annuale da parte della funzione OSP SG Dept., nonché della funzione Security e della funzione Plant Engineering aventi ad oggetto l'andamento dell'esecuzione dei contratti di appalto, nonché eventuali criticità;
 - q) aggiornamenti sulla avvenuta esecuzione dei piani di comunicazione e formazione;
 - r) le informazioni relative alla sussistenza di un conflitto di interessi effettivo o potenziale con la Società.

II. relative all'attività della Società, che possono assumere rilevanza quanto all'espletamento da parte dell'OdV dei compiti ad esso assegnati, incluse, senza che ciò costituisca limitazione:

- a) le notizie relative ai cambiamenti organizzativi o delle procedure aziendali vigenti e gli aggiornamenti del sistema dei poteri e delle deleghe;
- b) le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
- c) eventuali criticità con riguardo alle gare, pubbliche o a rilevanza pubblica, a livello nazionale/locale cui la Società ha partecipato; nonché eventuali criticità rispetto alle commesse eventualmente ottenute a seguito di trattativa privata;
- d) il bilancio annuale, corredato della nota integrativa, nonché la situazione patrimoniale;
- e) le comunicazioni, da parte della Società di Revisione (ove nominata) o del Collegio Sindacale, relative ad ogni criticità emersa, anche se risolta;
- f) gli incarichi conferiti alla società di revisione diversi dall'incarico di revisione (ove nominata);
- g) informazioni sulle autorizzazioni ambientali in scadenza e copia delle autorizzazioni rinnovate relative ad aree di rischi ambientali;
- h) verbali conseguenti alle ispezioni svolte dagli organi di controllo;
- i) copia annuale del MUD;
- j) risultanze di tutti gli Audit Interni.

L'OdV, nel corso dell'attività di controllo, deve agire in modo da garantire che i soggetti coinvolti non siano oggetto di ritorsioni, discriminazioni o, comunque, penalizzazioni, assicurando, quindi, la riservatezza del soggetto che effettua la segnalazione, salvo la ricorrenza di eventuali obblighi di legge.

La Società, al fine di facilitare le segnalazioni all'OdV da parte dei soggetti che vengano a conoscenza di violazioni del Modello, anche potenziali, attiva gli opportuni canali di comunicazione dedicati e, precisamente, una apposita casella di posta elettronica odv.ups@pec.it. Le segnalazioni possono essere inoltrate

anche per iscritto, anche in forma anonima, all'indirizzo: Organismo di Vigilanza, c/o presso la sede della Società in Via Fantoli, 15 Milano 20138.

Ai sensi dell'art. 6 comma 2 ter del Decreto l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.

Inoltre, ai sensi dell'art. 6, comma 2 quater il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. In questi casi, è onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

Quanto all'attività di reporting dell'OdV agli organi societari, si rammenta che l'OdV relaziona per iscritto, ogni sei mesi, al Consiglio di Amministrazione sull'attività compiuta nel periodo e sull'esito della stessa, fornendo pure una anticipazione sulle linee generali di intervento per il periodo successivo.

L'attività di *reporting* avrà ad oggetto, in particolare:

- l'attività svolta dall'OdV;
- eventuali problematiche o criticità che si siano evidenziate nel corso dell'attività di vigilanza;
- le azioni correttive, necessarie o eventuali, da apportare al fine di assicurare l'efficacia e l'effettività del Modello, nonché lo stato di attuazione delle azioni correttive deliberate dal Consiglio di Amministrazione;
- l'accertamento di comportamenti in violazione del Modello;
- l'eventuale mancata o carente collaborazione da parte delle funzioni aziendali nell'espletamento dei propri compiti di verifica;

- qualsiasi informazione ritenuta utile ai fini dell'assunzione di determinazioni urgenti da parte degli organi deputati.

In ogni caso, l'OdV può rivolgersi all'Amministratore Delegato, ogni qualvolta lo ritenga opportuno ai fini dell'efficace ed efficiente adempimento dei compiti ad esso assegnati.

Gli incontri devono essere verbalizzati e le copie dei verbali devono essere conservate presso gli uffici dell'OdV.

10. IL CODICE DI CONDOTTA

Così come previsto dalle Linee Guida dalle maggiori Associazioni di categoria, il codice di Condotta è uno dei protocolli fondamentali per la costruzione di un valido Modello, ai sensi del Decreto, idoneo a prevenire i reati presupposto indicati dallo stesso Decreto.

Il gruppo UPS, di cui fa parte la Società, già da molti anni ha adottato un Codice di Condotta - che costituisce un vero e proprio punto di riferimento per tutti coloro che svolgono la propria attività per conto e nell'interesse delle società UPS in tutto il mondo. Esso contiene, tra l'altro, i principi etici generali e le norme comportamentali di riferimento cui tutti i destinatari devono uniformarsi.

La finalità del Codice di Condotta è, dunque, di garantire il più elevato standard di eticità possibile nello svolgimento dell'attività sociale. Al Codice di Condotta si affianca un altro documento denominato Policy Book la cui prima versione risale al 1929.

Allo scopo di garantire la piena *compliance* al TU SSL e al Decreto, i principi del Codice di Condotta sono integrati, limitatamente alla salute e sicurezza sul lavoro, dagli ulteriori principi e regole individuate nell'apposita Parte Speciale, al paragrafo 11.

Il Codice di Condotta e gli ulteriori principi etici riportati nella Parte Speciale sono conformi ai principi indicati dalle Linee Guida di Confindustria, e devono essere

tassativamente ottemperati dai seguenti soggetti (indicati, di seguito, cumulativamente come "Destinatari"):

- ✓ i componenti degli Organi Sociali;
- ✓ i dirigenti, i dipendenti, senza alcuna eccezione;
- ✓ tutti i soggetti che, pure esterni alla Società, operino direttamente o indirettamente per la stessa (ad es., collaboratori, consulenti, fornitori, partner commerciali, ecc.).

Pur rimandando ai documenti specifici per il dettaglio, di seguito vengono indicati alcuni dei valori e delle aree su cui incidono i principi fondamentali seguiti dalla Società nello svolgimento della propria attività e che devono essere rispettati da tutti coloro che per essa agiscono.

Il Codice di Condotta individua e regola una serie di principi etici che devono essere rispettati con riferimento:

- ai rapporti con la Pubblica Amministrazione;
- alla corretta scelta dei fornitori e dei consulenti;
- alla concorrenza;
- al rispetto delle risorse umane, alla gestione del personale e all'equità del trattamento;
- alla accuratezza nella gestione delle scritture contabili;
- al trattamento delle informazioni confidenziali;
- al conflitto di interessi;
- alla gestione del patrimonio della Società;
- alla privacy;
- alle relazioni con i clienti;
- all'utilizzo degli strumenti tecnologici;
- alle attività commerciali internazionali;
- alla tutela dei diritti di proprietà industriale e intellettuale;
- alla tutela dell'ambiente;
- ai diritti umani;
- alla tutela della salute e sicurezza sul lavoro.

Con riferimento a questa ultima tematica, come sopra indicato, in ossequio ai suggerimenti delle Linee Guida di Confindustria, sono poi dedicati una serie di ulteriori principi nella Parte Speciale del Modello.

11.1. L'elaborazione e l'adozione del Sistema Disciplinare

Ai sensi degli artt. 6 e 7 del Decreto, il Modello può ritenersi efficacemente attuato, ai fini dell'esclusione di responsabilità della Società, se prevede un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure ivi indicate.

UPS ha, quindi, adottato un sistema disciplinare (di seguito, anche 'Sistema Disciplinare') precipuamente volto a sanzionare la violazione dei principi, delle norme e delle misure previste nel Modello e nei relativi Protocolli, nel rispetto delle norme previste dalla contrattazione collettiva nazionale, nonché delle norme di legge o di regolamento vigenti.

Sulla scorta di tale Sistema Disciplinare, sono passibili di sanzione sia le violazioni del Modello e dei relativi Protocolli commesse dai soggetti posti in posizione "apicale" - in quanto titolari di funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, ovvero titolari del potere, anche solo di fatto, di gestione o di controllo della Società stessa - sia le violazioni perpetrate dai soggetti sottoposti all'altrui direzione o vigilanza o operanti in nome e/o per conto di UPS.

Nel rispetto di quanto previsto anche dalla Linee Guida di Confindustria, l'instaurazione di un procedimento disciplinare, così come l'applicazione delle relative sanzioni, prescindono dall'eventuale instaurazione e/o dall'esito di eventuali procedimenti penali aventi ad oggetto le medesime condotte rilevanti ai fini del Sistema Disciplinare.

11.2. La struttura del Sistema Disciplinare

Il Sistema Disciplinare unitamente al Modello di cui costituisce fra i principali protocolli è consegnato, anche per via telematica o su supporto informatico, ai soggetti in posizione apicale ed ai dipendenti.

11.2.1. I destinatari del Sistema Disciplinare

I Soggetti Apicali

Le norme ed i principi contenuti nel Modello e nei Protocolli ad esso connessi devono essere rispettati, in primo luogo, dai soggetti che rivestono, in seno all'organizzazione di UPS, una posizione cd. "apicale".

A mente dell'art. 5, I comma, lett. a) del Decreto, rientrano in questa categoria le persone "che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale", nonché i soggetti che "esercitano, anche di fatto, la gestione o il controllo" dell'ente.

Assume rilevanza, *in primis*, la posizione dei componenti degli organi di amministrazione e controllo della Società (di seguito, anche 'Amministratori' e 'Sindaci'), quale che sia il sistema prescelto tra quelli indicati dal legislatore (amministratore unico / consiglio di amministrazione).

In aggiunta, agli Amministratori ed ai Sindaci, assume rilevanza la posizione dei soggetti che operano per la società incaricata della revisione (di seguito, indicati anche solo come 'Revisoré'), cui UPS può demandare il compito di curare il controllo contabile. Pur costituendo soggetto esterno alla Società, il Revisore è equiparato, ai fini di quanto previsto nel Sistema Disciplinare, agli Amministratori ed ai Sindaci, anche in considerazione dell'attività svolta per la Società.

Infine, nel novero dei Soggetti Apicali, vanno ricompresi, alla stregua dell'art. 5 del Decreto, i soggetti dotati di autonomia finanziaria e funzionale, nonché - ove presenti - i preposti delle sedi secondarie. Tali soggetti possono essere legati alla Società sia da un rapporto di lavoro subordinato (si pensi al caso di taluni dirigenti dotati di particolare potere finanziario o di autonomia), sia da altri rapporti di natura privatistica (ad esempio, mandato, agenzia, preposizione institoria, ecc.).

I dipendenti

L'art. 7, IV comma, lett. b) del Decreto prescrive l'adozione di un idoneo Sistema Disciplinare che sanzioni le eventuali violazioni delle misure previste nel Modello poste in essere dai soggetti sottoposti alla direzione o alla vigilanza di un soggetto "apicale".

Assume rilevanza, a tale proposito, la posizione di tutti i dipendenti di UPS legati

alla Società da un rapporto di lavoro subordinato, indipendentemente dal contratto applicato, dalla qualifica e/o dall'inquadramento aziendale riconosciuti (ad es., dirigenti non "apicali", quadri, impiegati, operai, lavoratori a tempo determinato, lavoratori con contratto di inserimento, ecc.; di seguito, anche 'Dipendenti').

Nell'ambito di tale categoria, rientrano anche i Dipendenti cui sono assegnati, o che comunque svolgono, funzioni e/o compiti specifici in materia di salute e sicurezza sul lavoro (ad es., il Responsabile e gli Addetti al Servizio Prevenzione e Protezione, gli Addetti al Primo Soccorso, gli Addetti alla Protezione Incendi, i Rappresentanti dei Lavoratori per la Sicurezza, ecc.)

Gli altri soggetti tenuti al rispetto del Modello

Il presente Sistema Disciplinare ha, inoltre, la funzione di sanzionare le violazioni del Modello commesse da soggetti anche diversi da quelli sopra indicati.

Si tratta, in particolare, di tutti i soggetti (di seguito, collettivamente denominati anche 'Terzi Destinatari') che sono comunque tenuti al rispetto del Modello in virtù della funzione svolta in relazione alla struttura societaria ed organizzativa della Società, ad esempio in quanto funzionalmente soggetti alla direzione o vigilanza di un soggetto "apicale", ovvero in quanto operanti, direttamente o indirettamente, per UPS.

Nell'ambito di tale categoria, possono farsi rientrare:

- tutti coloro che intrattengono con UPS un rapporto di lavoro di natura non subordinata (ad es., gli appaltatori, subappaltatori, i collaboratori a progetto, i consulenti, i lavoratori somministrati, i collaboratori in virtù di contratto di servizi);
- i collaboratori a qualsiasi titolo;
- i procuratori, gli agenti e tutti coloro che agiscono in nome e/o per conto della Società;
- i soggetti cui sono assegnati, o che comunque svolgono, funzioni e compiti specifici in materia di salute e sicurezza sul lavoro;
- i contraenti ed i partner.

11.2.2. Le condotte rilevanti ai sensi dell'applicazione del Sistema

Disciplinare

Ai fini del presente Sistema Disciplinare, e nel rispetto delle previsioni di cui alla contrattazione collettiva (laddove applicabili), costituiscono violazioni del Modello tutte le condotte, commissive o omissive (anche colpose), che siano idonee a ledere l'efficacia dello stesso quale strumento di prevenzione del rischio di commissione dei reati rilevanti ai fini del Decreto.

Nel rispetto del principio costituzionale di legalità, nonché di quello di proporzionalità della sanzione, tenuto conto di tutti gli elementi e/o delle circostanze ad essa inerenti, si ritiene opportuno definire le possibili violazioni, graduate secondo un ordine crescente di gravità.

In particolare, per tutte le Parti Speciali (eccetto la Parte Speciale H) assumono rilevanza le seguenti condotte:

- 1) mancato rispetto del Modello, qualora si tratti di violazioni realizzate nell'ambito delle attività "sensibili" di cui alle aree "strumentali" identificate nel Documento di Sintesi del Modello (Parti Speciali A, C e O), e sempre che non ricorra una delle condizioni previste nei successivi nn. 3 e 4;
- 2) mancato rispetto del Modello, qualora si tratti di violazioni realizzate nell'ambito delle attività "sensibili" di cui alle aree "a rischio reato" identificate nel Documento di Sintesi del Modello (tutte le Parti Speciali eccetto la Parte Speciale H), e sempre che non ricorra una delle condizioni previste nei successivi nn. 3 e 4;
- 3) mancato rispetto del Modello, qualora si tratti di violazione idonea ad integrare il solo fatto (elemento oggettivo) di uno dei reati previsti nel Decreto;
- 4) mancato rispetto del Modello, qualora si tratti di violazione finalizzata alla commissione di uno dei reati previsti dal Decreto, o comunque sussista il pericolo che sia contestata la responsabilità della Società ai sensi del Decreto;
- 5) mancato rispetto della procedura di segnalazione prevista dal Modello con particolare riferimento alla violazione delle misure di tutela del segnalante previste dal Modello stesso nonché effettuazione con dolo o colpa grave segnalazioni che si rivelano infondate.

É opportuno definire, inoltre, le possibili violazioni concernenti il settore della salute e sicurezza sul lavoro (Parte Speciale H), anch'esse graduate secondo un ordine crescente di gravità:

- 6) mancato rispetto del Modello, qualora la violazione determini una situazione di concreto pericolo per l'integrità fisica di una o più persone, incluso l'autore della violazione, e sempre che non ricorra una delle condizioni previste nei successivi nn. 7, 8 e 9;
- 7) mancato rispetto del Modello, qualora la violazione determini una lesione all'integrità fisica di una o più persone, incluso l'autore della violazione, e sempre che non ricorra una delle condizioni previste nei successivi nn. 8 e 9;
- 8) mancato rispetto del Modello, qualora la violazione determini una lesione, qualificabile come "grave" ai sensi dell'art. 583, comma 1, cod. pen., all'integrità fisica di una o più persone, incluso l'autore della violazione, e sempre che non ricorra una delle condizioni previste nel successivo n. 9;
- 9) mancato rispetto del Modello, qualora la violazione determini una lesione, qualificabile come "gravissima" ai sensi dell'art. 583, comma 1, cod. pen., all'integrità fisica ovvero la morte di una o più persone, incluso l'autore della violazione.

11.2.3. Le sanzioni

Il Sistema Disciplinare prevede con riguardo ad ognuna delle condotte rilevanti le sanzioni astrattamente comminabili per ciascuna categoria di soggetti tenuti al rispetto del Modello.

In ogni caso, ai fini dell'applicazione delle sanzioni si deve tener conto dei principi di proporzionalità e di adeguatezza rispetto alla violazione contestata, nonché delle seguenti circostanze:

- a) la gravità della condotta o dell'evento che quest'ultima ha determinato;
- b) la tipologia della violazione;
- c) le circostanze nel cui ambito si è sviluppata la condotta;
- d) all'intensità del dolo o al grado della colpa.

Ai fini dell'eventuale aggravamento della sanzione, sono inoltre considerati i seguenti elementi:

- i) l'eventuale commissione di più violazioni nell'ambito della medesima condotta, nel qual caso l'aggravamento sarà operato rispetto alla sanzione prevista per la violazione più grave;
- ii) l'eventuale concorso di più soggetti nella commissione della violazione;
- iii) l'eventuale recidività del suo autore.

Le sanzioni nei confronti dei Soggetti Apicali

Qualora sia accertata la commissione di una delle violazioni rilevanti da parte di un Soggetto Apicale, ove tale soggetto non sia inquadrabile nei Dipendenti, saranno applicate le seguenti sanzioni:

- il richiamo scritto;
- la diffida al puntuale rispetto del Modello;
- la decurtazione degli emolumenti per un importo deliberato dal Consiglio di Amministrazione;
- la revoca dall'incarico.

In particolare:

- a) per le violazioni di cui ai nn. 1), e 6) del paragrafo 11.2.2., sarà applicata la sanzione del richiamo scritto ovvero quella della diffida al rispetto del Modello;
- b) per le violazioni di cui ai nn. 2) e 7) del paragrafo 11.2.2., sarà applicata la sanzione della diffida al rispetto delle previsioni del Modello ovvero quella della decurtazione degli emolumenti per l'ammontare deliberato dal Consiglio di Amministrazione;
- c) per le violazioni di cui ai nn. 3) e 8) del paragrafo 11.2.2., sarà applicata la sanzione della decurtazione degli emolumenti ovvero quella della revoca dall'incarico;
- d) per le violazioni di cui ai nn. 4) e 9) del paragrafo 11.2.2., sarà applicata la sanzione della revoca dall'incarico.

Con riferimento alla violazione di cui al n. 5 del paragrafo 11.2.2. ossia mancato rispetto della procedura di segnalazione prevista dal Modello con particolare riferimento alla violazione delle misure di tutela del segnalante previste dal Modello stesso nonché effettuazione con dolo o colpa grave di segnalazioni che si rivelano infondate, si applicheranno le sanzioni di cui sopra graduate a seconda della gravità della condotta.

Qualora la violazione sia contestata ad un Amministratore legato alla Società da un rapporto di lavoro subordinato, saranno applicate le sanzioni previste per i Dipendenti nel successivo paragrafo.

Le sanzioni nei confronti dei Dipendenti

Qualora sia accertata la commissione di una delle violazioni indicate nel paragrafo 11.2.2 da parte di un soggetto qualificabile come Dipendente, saranno applicate le sanzioni eventualmente rinvenibili nella contrattazione collettiva applicabile al caso concreto.

Al dipendente responsabile di più mancanze sono applicabili, secondo il principio di proporzionalità e gradualità, le seguenti sanzioni disciplinari:

- il rimprovero verbale;
- il rimprovero scritto;
- la multa fino a 3 (tre) ore di retribuzione;
- la sospensione da 1 a 10 giorni dal servizio e dalla retribuzione, ed in ogni caso nei limiti previsti dalla contrattazione collettiva applicabile al caso concreto;
- il licenziamento.

In particolare:

- a) per le violazioni di cui ai nn. 1) e 6) del paragrafo 11.2.2., sarà applicata la sanzione del rimprovero verbale ovvero quella del rimprovero scritto;
- b) per le violazioni di cui ai nn. 2) e 7) del paragrafo 11.2.2., sarà applicata la sanzione della multa ovvero quella della sospensione dal lavoro e dalla retribuzione;

- c) per le violazioni di cui ai nn. 3) e 8) del paragrafo 11.2.2., sarà applicata la sanzione della sospensione dal lavoro e dalla retribuzione ovvero quella del licenziamento;
- d) per le violazioni di cui ai nn. 4) e 9) del paragrafo 11.2.2., sarà applicata la sanzione del licenziamento.

Con riferimento alla violazione di cui al n. 5 del paragrafo 11.2.2. ossia mancato rispetto della procedura di segnalazione prevista dal Modello con particolare riferimento alla violazione delle misure di tutela del segnalante previste dal Modello stesso nonché effettuazione con dolo o colpa grave di segnalazioni che si rivelano infondate, si applicheranno le sanzioni di cui sopra graduate a seconda della gravità della condotta.

Le sanzioni nei confronti dei Terzi Destinatari

Qualora sia accertata la commissione di una delle violazioni indicate nel paragrafo 11.2.2. da parte di un Terzo Destinatario, saranno applicate le seguenti sanzioni:

- la diffida al puntuale rispetto del Modello, pena l'applicazione della penale di seguito indicata ovvero la sospensione o risoluzione del rapporto negoziale intercorrente con la Società;
- l'applicazione di una penale, convenzionalmente prevista, del 10% del corrispettivo pattuito in favore del Terzo Destinatario;
- la sospensione del rapporto contrattuale in essere e del pagamento del relativo corrispettivo;
- la risoluzione immediata del rapporto negoziale intercorrente con la Società.

Le clausole e le relative sanzioni possono variare in base alla tipologia del soggetto qualificabile come Terzo Destinatario (a seconda del caso che agisca in nome e per conto della Società o meno).

In particolare:

- a) per le violazioni di cui ai nn. 1), 2), 6) e 7) del paragrafo 11.2.2., sarà applicata la sanzione della diffida ovvero quella della penale convenzionale ovvero quella della sospensione o risoluzione, a seconda della gravità della violazione;

- b) per le violazioni di cui ai nn. 3) e 8) del paragrafo 11.2.2., sarà applicata la sanzione della penale convenzionale ovvero quella della sospensione o della risoluzione;
- c) per le violazioni di cui ai nn. 4) e 9) del paragrafo 11.2.2., sarà applicata la sanzione della risoluzione.

Con riferimento alla violazione di cui al n. 5 del paragrafo 11.2.2. ossia mancato rispetto della procedura di segnalazione prevista dal Modello con particolare riferimento alla violazione delle misure di tutela del segnalante previste dal Modello stesso nonché effettuazione con dolo o colpa grave di segnalazioni che si rivelano infondate, si applicheranno le sanzioni di cui sopra graduate a seconda della gravità della condotta.

Nel caso in cui le violazioni previste del paragrafo 11.2.2. siano commesse da lavoratori somministrati ovvero nell'ambito di contratti di appalto di opere o di servizi, le sanzioni verranno applicate, all'esito dell'accertamento positivo delle violazioni da parte del lavoratore, nei confronti del somministratore o dell'appaltatore.

Nell'ambito dei rapporti con i Terzi Destinatari, la Società inserisce, nelle lettere di incarico e/o negli accordi negoziali relativi, apposite clausole volte a prevedere, in caso di violazione del Modello, l'applicazione delle misure sopra indicate.

11.2.4. Il procedimento di irrogazione delle sanzioni

Il procedimento di irrogazione ha di regola inizio a seguito della ricezione, da parte degli organi aziendali di volta in volta competenti della comunicazione con cui l'OdV segnala l'avvenuta violazione del Modello. In ogni caso l'Organo Amministrativo o gli organi aziendali a ciò deputati possono comunque attivarsi autonomamente anche in assenza di segnalazione da parte dell'OdV.

Più precisamente, in tutti i casi in cui riceva una segnalazione (anche anonima) ovvero acquisisca, nel corso della propria attività di vigilanza e di verifica, gli elementi idonei a configurare il pericolo di una violazione del Modello, l'OdV espleta gli accertamenti ed i controlli rientranti nell'ambito della propria attività e ritenuti opportuni.

Esaurita l'attività di verifica e di controllo, l'OdV valuta, sulla base degli elementi in proprio possesso, se si è effettivamente verificata una violazione sanzionabile del Modello. In caso positivo, segnala la violazione agli organi aziendali competenti; in caso negativo, può trasmettere la segnalazione alle altre funzioni competenti ai fini della valutazione della eventuale rilevanza della condotta rispetto alle altre leggi o regolamenti applicabili.

Qualora riscontri la violazione del Modello l'OdV trasmette all'organo amministrativo una relazione contenente:

- la descrizione della condotta constatata;
- l'indicazione delle previsioni del Modello che risultano essere state violate;
- gli estremi del soggetto responsabile della violazione;
- gli eventuali documenti comprovanti la violazione e/o gli altri elementi di riscontro.

In tutti i casi deve essere disposta da parte dell'organo amministrativo l'audizione dell'interessato, l'acquisizione delle eventuali deduzioni da quest'ultimo formulate e l'espletamento degli eventuali ulteriori accertamenti ritenuti opportuni. Nell'ipotesi in cui l'interessato sia anche dipendente della Società devono essere rispettate tutte le procedure obbligatorie previste dallo Statuto dei Lavoratori nonché dal CCNL applicabile nella specie, senza alcuna limitazione.

12. COMUNICAZIONE E FORMAZIONE SUL MODELLO E SUI PROTOCOLLI

12.1. La comunicazione ed il coinvolgimento sul Modello e sui Protocolli connessi

Al fine di assicurare un corretto ed efficace funzionamento del Modello la Società si impegna ad implementare la divulgazione dello stesso, adottando le più opportune iniziative per promuoverne e diffonderne la conoscenza differenziando i contenuti a seconda dei Destinatari. In particolare, garantendo la comunicazione formale dello stesso a tutti i soggetti riferibili alla Società mediante consegna di copia integrale, nonché mediante idonei strumenti divulgativi e la affissione in luogo accessibile a tutti.

Per i Terzi Destinatari tenuti al rispetto del Modello, una sintesi dello stesso è messa a disposizione su richiesta.

Sotto tale ultimo aspetto, al fine di formalizzare l'impegno al rispetto dei principi del Modello nonché dei Protocolli ad esso connessi da parte di Terzi Destinatari, è previsto l'inserimento nel contratto di riferimento di una apposita clausola, ovvero, per i contratti già in essere, la sottoscrizione di una specifica pattuizione integrativa, in tal senso.

L'OdV promuove, anche mediante la predisposizione di appositi piani, approvati dal Consiglio di Amministrazione ed implementati dalla Società, e monitora tutte le ulteriori attività di informazione che dovesse ritenere necessarie o opportune.

La Società promuove la comunicazione ed il coinvolgimento adeguati dei destinatari del Modello, nei limiti dei rispettivi ruoli, funzioni e responsabilità, nelle questioni connesse alla SSL, con particolare riguardo ai seguenti profili:

- i rischi per la sicurezza e la salute connessi all'attività aziendale;
- le misure e le attività di prevenzione e protezione adottate;
- i rischi specifici cui ciascun lavoratore è esposto in relazione all'attività svolta;
- i pericoli connessi all'uso delle sostanze e dei preparati pericolosi;
- le procedure che riguardano il pronto soccorso, la lotta antincendio, l'evacuazione dei lavoratori;
- la nomina dei soggetti cui sono affidati specifici compiti in materia di SSL (ad esempio, RSPP, ASPP, APS, API, RLS, medico competente).

A tali fini, è anche definito, documentato, implementato, monitorato e periodicamente aggiornato un programma di informazione e coinvolgimento dei Destinatari del Modello in materia di SSL, con particolare riguardo ai lavoratori neo-assunti, per i quali è necessaria una particolare qualificazione.

Il coinvolgimento dei soggetti interessati è assicurato anche mediante la loro consultazione preventiva in occasione di apposite riunioni periodiche.

12.2. La formazione e l'addestramento sul Modello e sui Protocolli connessi

In aggiunta alle attività connesse alla Informazione dei Destinatari, l'OdV ha il compito di curarne la periodica e costante Formazione, ovvero di promuovere e monitorare l'implementazione, da parte della Società, delle iniziative volte a favorire una conoscenza ed una consapevolezza adeguate del Modello e dei Protocolli ad esso connessi, al fine di incrementare la cultura di eticità all'interno della Società.

In particolare, è previsto che i principi del Modello, ed in particolare quelli del Codice Etico che ne è parte, siano illustrati alle risorse aziendali attraverso apposite attività formative (ad es. corsi, seminari, questionari, ecc.), a cui è posto obbligo di partecipazione e le cui modalità di esecuzione sono pianificate dall'OdV mediante predisposizione di specifici Piani, approvati dal Consiglio di Amministrazione ed implementati dalla Società.

I corsi e le altre iniziative di formazione sui principi del Modello sono, peraltro, differenziati in base al ruolo ed alla responsabilità delle risorse interessate, ovvero mediante la previsione di una formazione più intensa e caratterizzata da un più elevato grado di approfondimento per i soggetti qualificabili come "apicali" alla stregua del Decreto, nonché per quelli operanti nelle aree qualificabili come "a rischio" ai sensi del Modello.

La Società promuove, inoltre, la formazione e l'addestramento dei Destinatari del Modello, nei limiti dei rispettivi ruoli, funzioni e responsabilità, nelle questioni connesse alla SSL, al fine di assicurare un'adeguata consapevolezza circa l'importanza sia della conformità delle azioni rispetto al Modello, sia delle possibili conseguenze connesse a violazioni dello stesso; in quest'ottica, particolare rilevanza è riconosciuta alla formazione ed all'addestramento dei soggetti che svolgono compiti in materia di SSL.

A tali fini, è definito, documentato, implementato, monitorato ed aggiornato, da parte della Società, un programma di formazione ed addestramento periodici dei Destinatari del Modello - con particolare riguardo ai lavoratori neo-assunti, per i quali è necessaria una particolare qualificazione - in materia di SSL, anche con riferimento alla sicurezza aziendale e ai differenti profili di rischio (ad esempio, squadra antincendio, pronto soccorso, preposti alla sicurezza, ecc.). In particolare, si prevede che la formazione e l'addestramento sono differenziati in base al posto

di lavoro e alle mansioni affidate ai lavoratori, nonché erogati anche in occasione dell'assunzione, del trasferimento o del cambiamento di mansioni o dell'introduzione di nuove attrezzature di lavoro, di nuove tecnologie, di nuove sostanze e preparati pericolosi.

13. AGGIORNAMENTO DEL MODELLO

L'OdV ha il compito di monitorare il necessario e continuo aggiornamento ed adeguamento del Modello (ivi incluso il Codice Etico), eventualmente suggerendo mediante comunicazione scritta all'organo amministrativo, o alle funzioni aziendali di volta in volta competenti, le correzioni e gli adeguamenti necessari o opportuni. Il Consiglio di Amministrazione è responsabile, unitamente alle funzioni aziendali eventualmente interessate, dell'aggiornamento del Modello e del suo adeguamento in conseguenza di un mutamento degli assetti organizzativi o dei processi operativi, di significative violazioni del Modello stesso, di integrazioni legislative.

ALLEGATO 1: I REATI PRESUPPOSTO

Si fornisce, di seguito, una sintetica indicazione delle categorie di reati rilevanti a mente del Decreto.

La prima tipologia di reati cui, a mente del Decreto, consegue la responsabilità amministrativa dell'Ente è quella dei **reati commessi nei confronti della Pubblica Amministrazione**, che vengono dettagliati agli artt. **24 e 25** del Decreto, ossia:

- truffa in danno dello Stato o di altro ente pubblico (art. 640, II comma, n. 1, cod. pen.);
- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis cod. pen.);
- frode informatica in danno dello Stato o di altro ente pubblico (art. 640 ter cod. pen.);
- corruzione per l'esercizio della funzione (artt. 318 e 321 cod. pen.);
- corruzione per un atto contrario ai doveri d'ufficio (artt. 319 e 321 cod. pen.);
- corruzione in atti giudiziari (artt. 319 ter e 321 cod. pen.);

- induzione indebita a dare o promettere utilità (art. 319 quater cod. pen.);
- istigazione alla corruzione (art. 322 cod. pen.);
- corruzione di persone incaricate di pubblico servizio (artt. 320 e 321 cod. pen.);
- peculato, concussione, corruzione, induzione indebita a dare o promettere utilità e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis cod. pen.);
- concussione (art. 317 cod. pen.);
- malversazione di erogazioni pubbliche (art. 316 bis cod. pen.);
- indebita percezione di erogazioni pubbliche (316 ter cod. pen.);
- traffico di influenze illecite (art. 346 bis cod. pen. come introdotto dalla L. 9 gennaio 2019, n. 3);
- frode nelle pubbliche forniture (art. 356 cod. pen.);
- frode ai danni del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale (art. 2 L. 898/1986);
- peculato (art. 314, comma 1, cod. pen.);
- peculato mediante profitto dell'errore altrui (art. 316 cod. pen.);
- abuso d'ufficio (art. 323 cod. pen.).

Con riferimento alle fattispecie di cui agli articoli 314, primo comma, 316 e 323 del codice penale, sopra indicate, si specifica che rilevano qualora il fatto offenda gli interessi finanziari dell'Unione europea.

L'art. **25 bis** del Decreto – introdotto dall'art. 6 della Legge 23 settembre 2001, n. 409, – richiama, poi, i **reati di falsità in monete, in carte di pubblico credito e in valori da bollo**, modificati poi dal D.lgs. n. 125 del 27 luglio 2016:

- falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 cod. pen.);
- alterazione di monete (art. 454 cod. pen.);
- spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 cod. pen.);
- spendita di monete falsificate ricevute in buona fede (art. 457 cod. pen.);
- falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art.

459 cod. pen.);

- contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 cod. pen.);
- fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 cod. pen.);
- uso di valori di bollo contraffatti o alterati (art. 464, commi 1 e 2, cod. pen.).

Un'ulteriore e importante tipologia di reati cui è ricollegata la responsabilità amministrativa dell'Ente è, inoltre, costituita dai **reati societari**, categoria disciplinata dall'art. **25 ter** del Decreto, disposizione introdotta dal D. Lgs. 11 aprile 2002, n. 61, che individua le seguenti fattispecie, così come modificate dalla Legge 28 dicembre 2005, n. 262, dalla Legge 6 novembre 2012 n. 190, dalla Legge 27 maggio 2015, n. 69 e dal D.lgs. n. 38 del 15 marzo 2017:

- false comunicazioni sociali (art. 2621 cod. civ. nella sua nuova formulazione disposta dalla Legge 27 maggio 2015, n. 69);
- false comunicazioni sociali delle società quotate (art. 2622 cod. civ., nella sua nuova formulazione disposta dalla Legge 27 maggio 2015, n. 69);
- falso in prospetto (art. 2623 cod. civ., abrogato dall'art. 34 della L. n. 262/2005, la quale ha tuttavia introdotto l'art. 173 bis del D.Lgs. 24 febbraio 1998, n. 58)⁵;
- falsità nelle relazioni o nelle comunicazioni della società di revisione (art. 2624 cod. civ.)⁶;

⁵ L'art. 2623 del c.c. (Falso in prospetto) è stato abrogato dalla l. 262/2005, che ha riprodotto la medesima previsione di reato tramite l'introduzione dell'art. 173-bis del D.Lgs. 24 febbraio 1998, n. 58 (di seguito anche T.U.F). Tale nuova disposizione incriminatrice, allo stato, non è testualmente annoverata fra i reati richiamati dal D.Lgs 231/2001. Parte della dottrina ritiene comunque che l'art. 173 bis TUF, seppure non richiamato dal D.lgs. 231/2001, sia rilevante per la responsabilità amministrativa degli enti, poiché deve ritenersi in continuità normativa con il precedente art. 2623 c.c. La giurisprudenza, invece, si è pronunciata in senso contrario, seppure sul diverso reato di cui all'art. 2624 c.c. (Falsità nelle relazioni o nelle comunicazioni della Società di Revisione) [vedi nota seguente], ritenendo quel reato non più fonte di responsabilità ex D.lgs. 231/2001 e facendo leva sul principio di legalità delle norme contenute nel Decreto. Vista la mancanza di una pronuncia specifica sull'art. 2623, analoga a quella intervenuta per l'art. 2624, in via cautelativa, si è deciso di considerare astrattamente il reato nel Modello.

⁶ Si segnala che il D. Lgs. 27 gennaio 2010 n. 39 (Attuazione della direttiva 2006/43/CE, relativa alle revisioni legali dei conti annuali e dei conti consolidati, che modifica le direttive 78/660CEE e 83/349/CEE e che abroga la direttiva 84/253/CEE), entrato in vigore il 7 aprile 2010, ha abrogato l'art. 2624 del codice civile - Falsità nelle relazioni o nelle comunicazioni delle società di revisione - reinserendo, peraltro, la medesima fattispecie all'interno dello stesso D.Lvo 39/2010 (art. 27), il quale però, non è richiamato dal D.Lgs 231/2001. Le Sezioni Unite della Corte di Cassazione, con la sentenza n. 34776/2011, hanno stabilito che la fattispecie di falsità in revisione già prevista dall'art. 2624 c.c. non può più essere considerata fonte della responsabilità da reato degli enti, atteso che il suddetto articolo è stato abrogato dal D.lgs. 39/2010. La Corte ha infatti evidenziato come l'intervento legislativo che ha riformato la materia della revisione contabile abbia voluto intenzionalmente sottrarre i reati dei revisori dall'ambito di operatività del d.lgs. 231/2001 e come,

- impedito controllo (art. 2625 cod. civ.);
- indebita restituzione dei conferimenti (art. 2626 cod. civ.);
- illegale ripartizione degli utili e delle riserve (art. 2627 cod. civ.);
- illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 cod. civ.);
- operazioni in pregiudizio dei creditori (art. 2629 cod. civ.);
- omessa comunicazione del conflitto di interessi (art. 2629 bis cod. civ.);
- formazione fittizia del capitale (art. 2632 cod. civ.);
- indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 cod. civ.);
- corruzione tra privati (art. 2635, comma III cod. civ.);
- istigazione alla corruzione tra privati (art. 2635 bis cod. civ.);
- illecita influenza sull'assemblea (art. 2636 cod. civ.);
- aggio (art. 2637 cod. civ., modificato dalla Legge 18 aprile 2005, n. 62);
- ostacolo all'esercizio delle funzioni delle Autorità pubbliche di vigilanza (art. 2638 cod. civ., modificato dalla L. n. 62/2005 e dalla L. n. 262/2005).

L'intervento riformatore non si è fermato e, con la Legge 14 gennaio 2003, n. 7, è stato introdotto l'art. **25 quater**, con cui si estende ulteriormente l'ambito di operatività della responsabilità amministrativa da reato **ai delitti aventi finalità di terrorismo e di eversione dell'ordine democratico** previsti dal codice penale e dalle leggi speciali.

Successivamente, la Legge 11 agosto 2003, n. 228, ha introdotto l'art. **25 quinquies**, poi modificato dalla L. n. 199/2016, a mente del quale l'Ente è responsabile per la commissione dei **delitti contro la personalità individuale**:

- riduzione o mantenimento in schiavitù (art. 600 cod. pen);
- tratta e commercio di schiavi (art. 601 cod. pen);
- alienazione e acquisto di schiavi (art. 602 cod. pen);
- prostituzione minorile (art. 600-bis commi 1 e 2 cod. pen);
- pornografia minorile (art. 600-ter cod. pen);
- detenzione di materiale pornografico (art. 600-quater cod. pen);

dunque, alla luce del principio di legalità che lo governa, non possa che concludersi per l'intervenuta sostanziale abolizione dell'illecito da falso in revisione.

- pornografia virtuale (art. 600-quater.1 cod. pen.);
- iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies cod. pen.);
- intermediazione illecita e sfruttamento del lavoro (art. 603 bis cod. pen.);
- adescamento di minori (art. 609 undecies cod. pen.).

La L. n. 62/2005, c.d. Legge Comunitaria, e la L. n. 262/2005, meglio conosciuta come Legge sul Risparmio, hanno ancora incrementato il novero delle fattispecie di reato rilevanti ai sensi del Decreto. È stato, infatti, introdotto **l'art. 25 sexies**, relativo ai **reati di abuso dei mercati** (c.d. *market abuse*):

- abuso di informazioni privilegiate (art. 184 del D.Lgs. n. 58/1998);
- manipolazione del mercato (art. 185 del D.Lgs. n. 58/1998).

Tali reati sono stati successivamente modificati dal D. Lgs. n. 107 del 2018 "*Norme di adeguamento della normativa nazionale alle disposizioni del regolamento (UE) n. 596/2014, relativo agli abusi di mercato*" che abroga la direttiva 2003/6/CE e le direttive 2003/124/UE, 2003/125/CE e 2004/72/CE.

La legge 9 gennaio 2006, n. 7, ha, inoltre, introdotto l'art. **25 quater** del Decreto, che prevede la responsabilità amministrativa da reato dell'Ente nell'ipotesi che sia integrata la fattispecie di **pratiche di mutilazione degli organi genitali femminili** (art. 583 bis cod. pen.).

In seguito, la Legge 16 marzo 2006, n. 146, che ha ratificato la Convenzione e i Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 e il 31 maggio 2001, ha previsto la responsabilità degli Enti per alcuni **reati aventi carattere transnazionale**.

La fattispecie criminosa si considera tale, quando, nella realizzazione della stessa, sia coinvolto un gruppo criminale organizzato e sia per essa prevista l'applicazione di una sanzione non inferiore nel massimo a 4 anni di reclusione, nonché, quanto alla territorialità, sia commessa in più di uno Stato; sia commessa in uno Stato, ma abbia effetti sostanziali in un altro Stato; sia commessa anche in un solo Stato, ma una parte sostanziale della sua preparazione o pianificazione o direzione e controllo avvenga in un altro Stato; sia commessa in uno Stato, ma in esso sia coinvolto un gruppo criminale organizzato protagonista di attività criminali in più di uno Stato.

I reati a tale fine rilevanti sono:

- associazione per delinquere (art. 416 cod. pen.);
- associazioni di tipo mafioso anche straniere (art. 416 bis cod. pen.);
- associazione a delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291 quater del DPR 23 gennaio 1973, n. 43);
- associazione finalizzata al traffico illecito di sostanze stupefacenti o

psicotrope (art. 74 del DPR 9 ottobre 1990, n. 309);

- traffico di migranti (art. 12, commi 3, 3 bis, 3 ter e 5, D. Lgs. 25 luglio 1998, n. 286);
- intralcio alla giustizia, nella forma di non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria e del favoreggiamento personale (artt. 377 bis e 378 cod. pen.).

Il Legislatore italiano ha, poi, novellato il Decreto mediante la Legge 3 agosto 2007, n. 123, e, in seguito, mediante il D. Lgs. 21 novembre 2007, n. 231.

Con la L. n. 123/2007, è stato introdotto l'art. **25 septies** del Decreto, poi sostituito dal D. Lgs. 9 aprile 2008, n. 81, che prevede la responsabilità degli Enti per i **reati di omicidio colposo e lesioni colpose gravi o gravissime**, commessi con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro:

- omicidio colposo (art. 589 cod. pen.), con violazione delle norme infortunistiche e sulla tutela dell'igiene e della salute sul lavoro;
- lesioni personali colpose (art. 590, comma 3 cod. pen.), con violazione delle norme infortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Il D.Lgs. n. 231/2007 ha introdotto l'art. **25 octies** del Decreto, a mente del quale l'Ente è responsabile per la commissione dei reati di **ricettazione** (art. 648 cod. pen.), **riciclaggio** (art. 648 bis cod. pen.) e **impiego di denaro, beni o utilità di provenienza illecita** (art. 648 ter cod. pen.).

Inoltre, con la Legge 15 dicembre 2014, n. 186 "*Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio*" ha introdotto la nuova fattispecie dell'**auto-riciclaggio** (art. 648 ter 1 c.p.) e, contestualmente, ha previsto un aumento delle sanzioni previste per il reato di riciclaggio e di impiego di denaro, beni o altra utilità di provenienza illecita.

La Legge 18 marzo 2008, n. 48 ha introdotto, infine, l'art. **24 bis** del Decreto, che estende la responsabilità degli Enti anche ad alcuni **reati c.d. informatici**:

- accesso abusivo ad un sistema informatico o telematico (art. 615 ter cod. pen.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater cod. pen.);
- installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies cod. pen.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 bis cod. pen.);

- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (Art. 635 ter cod. pen.);
- danneggiamento di sistemi informatici o telematici (art. 635 quater cod. pen.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies cod. pen.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 cod. pen.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies cod. pen.);
- violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105);
- documenti informatici (art. 491 bis cod. pen.)

La norma sopra citata (*"se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici"*) estende le disposizioni in tema di falso in atto pubblico alle falsità riguardanti un documento informatico; i reati richiamati sono i seguenti:

- falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 cod. pen.);
- falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 cod. pen.);
- falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 cod. pen.);
- falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 cod. pen.);
- falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative (art. 480 cod. pen.);
- falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 cod. pen.);
- falsità materiale commessa dal privato (art. 482 cod. pen.);
- falsità ideologica commessa dal privato in atto pubblico (art. 483 cod. pen.);
- falsità in registri e notificazioni (art. 484 cod. pen.);
- falsità in foglio firmato in bianco. Atto pubblico (art. 487 cod. pen.);
- altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni

- sulle falsità materiali (art. 488 cod. pen.);
- uso di atto falso (art. 489 cod. pen.);
- soppressione, distruzione e occultamento di atti veri (art. 490 cod. pen.);
- copie autentiche che tengono luogo degli originali mancanti (art. 492 cod. pen.);
- falsità commesse da pubblici impiegati incaricati di un servizio pubblico (art. 493 cod. pen.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies cod. pen.).

La Legge 15 luglio 2009, n. 94, recante disposizioni in materia di sicurezza pubblica, ha introdotto l'art. **24 ter** e, dunque, la responsabilità degli enti per la commissione dei **delitti di criminalità organizzata**⁷:

- associazione per delinquere (art. 416, co. 6 cod. pen.);
- associazioni di tipo mafioso anche straniere (art. 416 bis cod. pen.);
- scambio elettorale politico-mafioso (art. 416 ter cod. pen.);
- sequestro di persona a scopo di estorsione (art. 630 cod. pen.);
- tutti i delitti, se commessi avvalendosi delle condizioni indicate dall'art. 416 bis cod. pen per agevolare l'attività delle associazioni previste dalla stessa disposizione (i.e. assoggettamento ed omertà derivanti dall'esistenza di un vincolo associativo);
- associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74, D.P.R. 9.10.1990, n. 309);
- delitti di 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, co. 2, lett. a) n. 5 c.p.p.).

La Legge 23 luglio 2009, n. 99, recante disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia, ha ampliato le ipotesi di reato di falso previste dall'art. **25 bis** del Decreto, che prevede la responsabilità degli enti per i reati di **falsità in monete, in carte di pubblico credito, valori di bollo e in strumenti o segni di riconoscimento** ossia:

- falsificazione di monete, spendita e introduzione nello Stato previo concerto di monete falsificate (art. 453 cod. pen.);

⁷ I delitti di criminalità organizzata erano prima rilevanti, ai fini del Decreto, solo se aventi carattere transnazionale.

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

Il medesimo intervento legislativo ha introdotto l'art. **25 bis 1**, volto a prevedere la responsabilità degli enti per i reati contro l'industria e il commercio nonché l'art. **25 novies** volto a prevedere la responsabilità degli enti per i **delitti in materia di violazione del diritto d'autore**.

Quanto ai primi, assumono rilevanza i seguenti reati:

- turbata libertà dell'industria o del commercio (art. 513 cod. pen.);
- Illecita concorrenza con minaccia o violenza (art. 513 bis cod. pen.);
- frodi contro le industrie nazionali (art. 514 cod. pen.);
- frode nell'esercizio del commercio (art. 515 cod. pen.);
- vendita di sostanze alimentari non genuine come genuine (art. 516 cod. pen.);
- vendita di prodotti industriali con segni mendaci (art. 517 cod. pen.);
- fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517 ter cod. pen.);
- contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517 quater cod. pen.).

Con riferimento alla tutela del diritto di autore, devono considerarsi i seguenti reati previsti e puniti dagli artt. 171, primo comma, lettera a-bis), e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies della legge 22 aprile 1941, n. 633).

Inoltre, l'art. 4 della Legge 3 agosto 2009, n. 116 ha introdotto l'articolo **25 decies**, a mente del quale l'ente è ritenuto responsabile per la commissione del reato previsto dall'art. 377-bis del codice penale ossia **induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria**.

Successivamente il D.lgs. 121/2011 ha introdotto nel Decreto l'art. **25 undecies** che ha esteso la responsabilità amministrativa da reato degli enti ai c.d. **reati ambientali**, ossia a due contravvenzioni di recente introduzione nel codice penale (artt. 727-bis c.p. e 733-bis c.p.) nonché ad una serie di fattispecie di reato già previste dal c.d. Codice dell'Ambiente (D.lgs. 152/2006) e da altre normative speciali a tutela dell'ambiente (L n. 150/1992, L. n. 549/1993, D.lgs. n. 202/2007).

Inoltre, la **Legge 22 maggio 2015, n. 68 recante Disposizioni in materia di delitti contro l'ambiente** (GU n. 122 del 28-5-2015) in vigore dal 29/05/2015 ha introdotto nel codice penale il titolo VI - bis dedicato ai delitti contro l'ambiente. In particolare, ad integrazione delle fattispecie già previste e punite a titolo contravvenzionale dal Codice dell'ambiente (D. lgs. 152/2006) vengono introdotte nel codice penale diverse fattispecie di reato, tra cui i seguenti reati, rilevanti anche ai sensi del Decreto:

- art. 452 bis - Inquinamento ambientale;
- art. 452 quater - Disastro ambientale;
- art. 452-quinquies- Delitti colposi contro l'ambiente;
- Art. 452 sexies - Traffico e abbandono di materiale ad alta radioattività;
- Art. 452 octies- Circostanze aggravanti.

Il D. lgs. n. 21/2018 "*Disposizioni di attuazione del principio di delega della riserva di codice nella materia penale a norma dell'articolo 1, comma 85, lettera q), della legge 23 giugno 2017, n. 103*" ha abrogato l'art. 260 del D.lgs. 152/2016 introducendo una disposizione di analogo contenuto nel codice penale, l'art. 452 quaterdecies (*Attività organizzate per il traffico illecito di rifiuti*).

In attuazione della direttiva comunitaria 2009/52/CE è stato emanato il d.lgs. 109/2012 che, tra l'altro, ha sancito l'inserimento dell'articolo **25 duodecies** con la seguente previsione: **"Impiego di cittadini di paesi terzi il cui soggiorno è irregolare - in relazione alla commissione del delitto di cui all'articolo 22, comma 12-bis, del decreto legislativo 25 luglio 1998, n. 286 - ossia del datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno - si applica all'ente la sanzione pecuniaria da 100 a 200 quote, entro il limite di 150.000 euro"**.

Tale articolo è stato modificato dalla Legge n. 161/2017 di riforma del Codice Antimafia (D.lgs. 159/2011), che ha introdotto tre nuovi commi, che prevedono due nuovi reati presupposto connessi all'immigrazione clandestina di cui, rispettivamente, all'art. 12 commi 3, 3-bis, 3-ter, e all'art. 12, comma 5, del Testo Unico sull'Immigrazione (D.Lgs. 286/1998). In particolare:

- il comma 1-bis prevede l'applicazione all'ente della sanzione pecuniaria da 400 a 1000 quote per il reato di trasporto di stranieri irregolari nel territorio dello Stato di cui all'art. 12, commi 3, 3-bis e 3-ter del D. Lgs. 286/1998;
- il comma 1-ter prevede l'applicazione della sanzione pecuniaria da 100 a 200 quote in relazione alla commissione del reato di favoreggiamento della permanenza di stranieri irregolari nel territorio dello Stato di cui all'art. 12, comma 5 del D. Lgs. 286/1998;
- nei casi di condanna per i neo-introdotti reati presupposto di cui ai commi 1-bis e 1-ter del medesimo articolo, il comma 1-quater prevede l'applicazione delle sanzioni interdittive previste dall'art. 9, comma 2 del Decreto per una durata non inferiore ad un anno.

Con questo intervento normativo il Legislatore ha dunque ampliato il catalogo dei reati presupposto prevedendo la responsabilità dell'ente anche per i delitti relativi alle condotte di chi **dirige, organizza, finanzia, effettua il trasporto di stranieri in Italia o ne favorisce la permanenza al fine di trarre un ingiusto profitto dalla loro condizione di illegalità.**

Tale articolo è stato modificato dalla Legge n. 161/2017 di riforma del Codice Antimafia (D.lgs. 159/2011), che ha introdotto tre nuovi commi, che prevedono due nuovi reati presupposto connessi all'immigrazione clandestina di cui, rispettivamente, all'art. 12 commi 3, 3-bis, 3-ter, e all'art. 12, comma 5, del Testo Unico sull'Immigrazione (D.Lgs. 286/1998). In particolare:

- il comma 1-bis prevede l'applicazione all'ente della sanzione pecuniaria da 400 a 1000 quote per il reato di trasporto di stranieri irregolari nel territorio dello Stato di cui all'art. 12, commi 3, 3-bis e 3-ter del D. Lgs. 286/1998;
- il comma 1-ter prevede l'applicazione della sanzione pecuniaria da 100 a 200 quote in relazione alla commissione del reato di favoreggiamento della permanenza di stranieri irregolari nel territorio dello Stato di cui all'art. 12, comma 5 del D. Lgs. 286/1998;
- nei casi di condanna per i neo-introdotti reati presupposto di cui ai commi 1-bis e 1-ter del medesimo articolo, il comma 1-quater prevede l'applicazione delle sanzioni interdittive previste dall'art. 9, comma 2 del Decreto per una durata non inferiore ad un anno.

Con questo intervento normativo il Legislatore ha dunque ampliato il catalogo dei reati presupposto prevedendo la responsabilità dell'ente anche per i delitti relativi alle condotte di chi **dirige, organizza, finanzia, effettua il trasporto di stranieri in Italia o ne favorisce la permanenza al fine di trarre un ingiusto profitto dalla loro condizione di illegalità.**

La Legge 19 dicembre 2019, n. 157, che ha convertito con emendamenti il D.L. 26 ottobre 2019, n. 124, recante "*Disposizioni urgenti in materia fiscale e per esigenze indefettibili*", ha introdotto nel Decreto l'art. **25 quinquiesdecies**,

rubricato "Reati tributari", che prevede la punibilità dell'ente per le seguenti fattispecie:

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti ex art. articolo 2 del D.Lgs. 74/2000;
- dichiarazione fraudolenta mediante altri artifici ex art. 3 del D.Lgs. 74/2000;
- emissione di fatture o altri documenti per operazioni inesistenti ex art. 8 del D.Lgs. 74/2000;
- occultamento o distruzione di documenti contabili ex art. 10 del D.Lgs. 74/2000;
- sottrazione fraudolenta al pagamento di imposte ex art. 11 del D.Lgs. 74/2000.

L'art. 25 *quinquiesdecies* è stato, poi, modificato con D.Lgs. 14 luglio 2020, n. 75 (e, successivamente, con D.Lgs. 4 ottobre 2022, n. 156) che – recependo la Direttiva UE 2017/1371 relativa alla "lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale" (c.d. Direttiva PIF) ha introdotto il seguente comma 1-bis: "In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, quando sono commessi al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegue o possa conseguire un danno complessivo pari o superior a dieci milioni di euro, si applicano all'ente le seguenti sanzioni pecuniarie:

a) per il delitto di dichiarazione infedele previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote;

b) per il delitto di omessa dichiarazione previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote;

c) per il delitto di indebita compensazione previsto dall'articolo 10-quater, la sanzione pecuniaria fino a quattrocento quote."

Il Decreto Legislativo 14 luglio 2020, n. 75, ha introdotto l'art. **25 sexiesdecies** in materia di **contrabbando** prevedendo l'applicazione della sanzione pecuniaria fino a 200 quote (o 400 quote nel caso in cui i diritti di confine dovuti superino i 100.000 euro) in relazione alla commissione dei reati di contrabbando previsti dal decreto del Presidente della Repubblica 23 gennaio 1973, n. 43.

Il Decreto Legislativo 29 novembre 2021, n. 284, ha, poi, introdotto il nuovo art. **25 octies.1** rubricato "Delitti in materia di strumenti di pagamento diversi dai contanti" che estende la responsabilità delle persone giuridiche anche ai reati di indebito utilizzo e falsificazione di carte di credito e di pagamento (art. 493-ter c.p.), detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.) e frode informatica (art. 640-ter c.p.) quest'ultimo "nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale".

Infine, la Legge del 9 marzo 2022 n. 22 recante "*Disposizioni in materia di reati contro il patrimonio culturale*" ha inserito, nel Decreto 231 gli articoli **25 septiesdecies** rubricato "*Delitti contro il patrimonio culturale*" e **25 duodevicies** rubricato "*Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici*". Tali norme introducono la responsabilità amministrativa dell'ente per i seguenti reati presupposto:

- Furto di beni culturali (art. 518-bis c.p.)
- Appropriazione indebita di beni culturali (art. 518-ter c.p.)
- Ricettazione di beni culturali (art. 518-quater c.p.)
- Falsificazione in scrittura privata relativa a beni culturali (art. 518-octies c.p.)
- Violazioni in materia di alienazione di beni culturali (art. 518-novies c.p.)
- Importazione illecita di beni culturali (art. 518-decies c.p.)
- Uscita o esportazione illecite di beni culturali (art. 518-undecies c.p.)
- Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518-duodecies c.p.)
- Contraffazione di opere d'arte (art. 518-quaterdecies c.p.)
- Riciclaggio di beni culturali (art. 518-sexies c.p.)
- Devastazione e saccheggio di beni culturali e paesaggistici (art. 518-terdecies c.p.)

Per completezza, deve ricordarsi, inoltre, che l'art. 23 del Decreto punisce l'inosservanza delle **sanzioni interdittive**, che si realizza qualora all'Ente sia stata applicata, ai sensi del Decreto, una sanzione o una misura cautelare interdittiva e, nonostante ciò, lo stesso trasgredisca agli obblighi o ai divieti ad esse inerenti.