MODELLO ORGANIZZATIVO
EX D.LGS. 231/01

ADOPERA S.R.L.

Approvato con determinazione dell'Amministratore Unico n. 4 del 28/01/2019
Documento aggiornato con determina dell'Amministratore Unico n. 10 del 25/06/2019
Documento aggiornato con determina dell'Amministratore Unico n. 2 del 28/01/2020
Documento aggiornato con determina dell'Amministratore Unico n. 5 del 28/03/2023
Documento aggiornato con determina dell'Amministratore Unico n. 1 del 24/01/2024
Documento aggiornato con determina dell'Amministratore Unico n. 1 del 28/01/2026

SOMMARIO

1. IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO A CARICO DELLE PERSONE GIURIDICHE, SOCIETÀ ED ASSOCIAZIONI

1.1 Premessa

In data 8 giugno 2001, è stato emanato - in esecuzione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 - il Decreto Legislativo n. 231 (da qui in avanti, il "Decreto"), entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali a cui l'Italia ha già da tempo aderito, quali la *Convenzione di Bruxelles del 26 luglio 1995* sulla tutela degli interessi finanziari delle Comunità Europee, la *Convenzione* anch'essa firmata *a Bruxelles il 26 maggio 1997* sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri e la *Convenzione OCSE del 17 dicembre 1997* sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Il Decreto ha introdotto nell'ordinamento nazionale il concetto di responsabilità "amministrativa" delle persone giuridiche (riferibile sostanzialmente alla responsabilità penale). I diretti destinatari della disciplina in esame sono gli organismi con personalità giuridica, nonché le società ed associazioni prive di personalità giuridica (art.1 comma 2 D.lgs. 231/2001) con esclusione dello Stato, degli enti pubblici territoriali, di quelli non economici e aventi funzioni di rilievo costituzionale.

La responsabilità dell'ente può essere esclusa se esso ha adottato ed efficacemente attuato, prima della commissione dei reati, modelli di organizzazione, gestione e controllo idonei a prevenire i reati stessi e, più in generale, ha ottemperato alle disposizioni previste dal decreto in esame.

Ebbene, Adopera, nell'ambito della propria corporate governance, ha ritenuto di ottemperare alle prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di reati.

L'attuazione del Modello di organizzazione e gestione (d'ora in avanti "Modello" o MOG) risponde alla convinzione dell'azienda che ogni elemento utile alla correttezza e trasparenza gestionale sia meritevole di attenzione e possa contribuire positivamente all'immagine della società ed alla tutela degli interessi degli stakeholders aziendali (individui, istituzioni e consumatori). In questo senso

l'attuazione della norma può essere considerata la continuazione delle politiche aziendali che hanno portato all'introduzione del Codice di Comportamento.

La scelta di adozione del Modello si ritiene che possa costituire, insieme al Codice di Comportamento e agli ulteriori elementi della governance societaria uno strumento di sensibilizzazione per favorire la diffusione di comportamenti etici e socialmente responsabili da parte di tutti i soggetti che operano per conto dell'azienda.

Scopo del Modello è la predisposizione di un sistema strutturato ed organico di procedure e regole che devono essere rispettate al fine di ridurre il rischio di commissione dei reati contemplati nel Decreto, con l'obiettivo di costituire l'esimente ai fini della responsabilità amministrativa degli enti.

Il modello si propone, inoltre, le seguenti finalità:

- Determinare in tutti coloro che operano in nome e per conto dell'azienda la piena consapevolezza dei rischi che si produrrebbero in capo alla società, in caso di violazione delle disposizioni contenute nel presente documento e, più in generale, di tutte le disposizioni adottate dall'azienda stessa;

- Individuare le regole per prevenire comportamenti illeciti contrari agli interessi aziendali (anche quando apparentemente essa potrebbe trarne un vantaggio), poiché si tratta di comportamenti in contrasto con i principi etico-sociali della società oltre che con le disposizioni di legge;

- Consentire all'azienda, grazie ad un monitoraggio costante dei processi sensibili e quindi dei rischi di commissione di reato, di reagire tempestivamente al fine di prevenire e contrastare la commissione dei reati stessi.

1.2 I soggetti autori del reato

Secondo il Decreto, la Società è responsabile per i reati commessi, a suo vantaggio o nel suo interesse, da:

- **cd. "soggetti apicali"**, persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo della Società sessa;

- persone sottoposte alla direzione o alla vigilanza di uno dei soggetti in posizione apicale (**c.d. "soggetti sottoposti all'altrui direzione**").

La Società non risponde, per espressa previsione legislativa (art. 5 comma 2 del Decreto) se le persone indicate hanno agito nell'interesse esclusivo proprio o di terzi.

1.3 L'apparato sanzionatorio

Le sanzioni previste dal Decreto a carico della Società giudicata responsabile della commissione dei reati sopra menzionati sono:

1) **sanzione pecuniaria:**
   viene applicata per "quote", in un numero non inferiore a 100 e non superiore a 1000. L'importo di ciascuna quota è fissato dal Giudice da un minimo di € 258,00 ad un massimo di € 1549,00 sulla base delle condizioni economiche e patrimoniali della Società allo scopo di assicurare l'efficacia della sanzione;

2) **sanzioni interdittive:**
   sono applicabili anche quale misura cautelare ed hanno una durata non inferiore a tre mesi e non superiore a due anni.
   Esse possono consistere in:
   a) interdizione dall'esercizio dell'attività;
   b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
   c) divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
   d) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi;
   e) divieto di pubblicizzare beni o servizi;
   f) confisca (e sequestro preventivo in sede cautelare);
   g) pubblicazione della sentenza in caso di applicazione di una sanzione interdittiva.

In alcuni casi il giudice, in alternativa all'applicazione della sanzione che determina l'interruzione dell'attività, può disporre la prosecuzione dell'attività e la nomina di un commissario giudiziale (ad esempio quando la società svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività).

Nei casi previsti dall'art. 16 del Decreto si può arrivare anche all'interruzione definitiva dell'esercizio dell'attività.

L'art. 13 prevede che le sanzioni interdittive possano applicarsi in relazione ai casi espressamente previsti dalla legge (reati contro la pubblica amministrazione, alcuni reati contro la fede pubblica quali la falsità in monete, i delitti in materia di terrorismo e di eversione dell'ordine democratico, nonché i delitti contro la personalità individuale) e quando ricorre almeno una delle seguenti condizioni:

- la società ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in tale ultimo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
- in caso di reiterazione degli illeciti.

Nelle ipotesi di commissione, nelle forme del tentativo, dei delitti indicati nel Capo I del Decreto (artt. da 24 a 25-sexies), le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui la società impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26).

L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra società e soggetti che assumono di agire in suo nome e per suo conto.

1.4 L'interesse o il vantaggio per la Società

Ulteriore elemento costitutivo della responsabilità in questione è rappresentato dalla necessità che la condotta illecita ipotizzata sia stata posta in essere dai citati soggetti *"nell'interesse o a vantaggio della Società"* e non "nell'interesse esclusivo proprio o di terzi" (art. 5 comma 1 e 2).

Ne deriva che la responsabilità della società sorge non soltanto allorché il comportamento illecito abbia determinato un vantaggio (patrimoniale o meno) per la società, ma anche nell'ipotesi in cui, pur in assenza di tale concreto risultato, il fatto-reato trovi ragione nell'interesse della società.

Sul significato dei termini "interesse" e "vantaggio", la Relazione governativa che accompagna il Decreto attribuisce al primo una valenza "soggettiva", riferita cioè alla volontà dell'autore (persona fisica) materiale del reato (questi deve essersi attivato avendo come fine della sua azione la realizzazione di uno specifico

interesse della società), mentre al secondo una valenza di tipo "oggettivo" riferita quindi ai risultati effettivi della sua condotta (il riferimento è ai casi in cui l'autore del reato, pur non avendo direttamente di mira un interesse della società, realizza comunque un vantaggio in suo favore). Sempre la Relazione, infine, suggerisce che l'indagine sulla sussistenza del primo requisito (l'interesse) richiede una verifica *ex ante*, viceversa quella sul "vantaggio" che può essere tratto della società anche quando la persona fisica non abbia agito nel suo interesse, richiede sempre una verifica *ex post* dovendosi valutare solo il risultato della condotta criminosa.

L'art. 12 primo comma lett. a) stabilisce un'attenuazione della sanzione pecuniaria per il caso in cui *"l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e la società non ne ha ricavato vantaggio o ne ha ricevuto vantaggio minimo*".

Pertanto se il soggetto ha agito perseguendo sia l'interesse proprio che quello della società, la stessa sarà passibile di sanzione. Ove risulti prevalente l'interesse dell'agente rispetto a quello della società, sarà possibile un'attenuazione della sanzione stessa a condizione, però, che la società non abbia tratto vantaggio o abbia tratto vantaggio minimo dalla commissione dell'illecito; nel caso in cui, infine, si accerti che il soggetto ha perseguito esclusivamente un interesse personale o di terzi, la società non sarà responsabile affatto a prescindere dal vantaggio eventualmente acquisito.

1.5 L'esonero della responsabilità

Per beneficiare dell'esimente da responsabilità le società devono elaborare un modello di organizzazione, gestione e controllo tale da rispondere alle esigenze delle realtà aziendale di riferimento.

In tal senso l'art. 6 del decreto prevede che la società non risponde se prova che:

1) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quelli verificatisi;
2) il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei modelli nonché di curare il loro aggiornamento è stato affidato ad un organismo interno dotato di autonomi poteri di iniziativa e controllo;
3) le persone fisiche hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
4) non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lettera b).

Il Decreto delinea il contenuto dei modelli di organizzazione e di gestione prevedendo che gli stessi devono rispondere, in relazione all'estensione dei poteri delegati ed al rischio di commissione dei reati, alle seguenti esigenze:

1) individuare le attività nel cui ambito possono essere commessi i Reati;
2) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai reati da prevenire;
3) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
4) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e sull'osservanza del Modello organizzativo;
5) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello organizzativo.

Nel caso di un reato commesso dai soggetti sottoposti all'altrui direzione, la Società non risponde se dimostra che alla commissione del reato non ha contribuito l'inosservanza degli obblighi di direzione o vigilanza. In ogni caso la responsabilità è esclusa se la Società, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello di organizzazione, gestione e controllo idoneo a prevenire i reati della specie di quello verificatosi.

2. IL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO DI ADOPERA PATRIMONIO E INVESETIMENTI CASALECCHIO DI RENO SRL

Adopera Patrimonio e Investimenti Casalecchio di Reno S.r.l. (di seguito anche Adopera), è un'azienda di Servizi Pubblici Locali a capitale interamente pubblico, partecipata al 98,70% dal Comune di Casalecchio di Reno, allo 0,65% DAL Comune di Zola Predosa e allo 0,65% dal Comune di Monte San Pietro.

Nasce nel 2007 come Azienda Speciale Multiservizi e, ad oggi, è iscritta all'Albo Nazionale dei Gestori Ambientali iscrizione nr. BO/10230.

In particolare, Adopera ha per oggetto la gestione di servizi pubblici e la manutenzione del patrimonio del Comune di Casalecchio di Reno perseguendo finalità di mantenimento, incremento e miglioramento della qualità delle infrastrutture e dei servizi su tutto il territorio comunale.

In ragione della peculiarità della sua attività produttiva e dell'utenza a cui la stessa è rivolta, tale società ha inteso adottare un Modello Organizzativo così come previsto ex D.lgs. 231/01, limitatamente ad alcuni reati presupposto non tutti quelli

previsti dal D.lgs. 231/01 (sono esclusi per es. reati tributari, reati societari, ecc. astrattamente configurabili ma ritenuti comunque gestiti con solide procedure e prassi aziendali).

La scelta di limitare le fattispecie criminose di cui al presente MOG ai fini del D.lgs. 231/01, è frutto di una valutazione di carattere statistico e di opportunità giuridica da parte dell'Amministratore Unico, che ha ritenuto tale approccio il mezzo più efficace e realistico finalizzato alla tutela della società stessa.

L'adozione del Modello così come sopra specificato è finalizzata da un lato a determinare piena consapevolezza presso i soci, amministratori, dipendenti e collaboratori di Adopera delle disposizioni contenute nel Decreto e dall'altro istituire un complesso organico di principi e procedure idonei a gestire un sistema di controllo interno al fine di prevenire la commissione dei reati ivi previsti.

Il MOG adottato da Adopera:

1) identifica e valuta i rischi aziendali in relazione ai reati ritenuti applicabili alla realtà aziendale;
2) individua un sistema di controllo preventivo;
3) adotta un Codice di Comportamento e il relativo sistema sanzionatorio;
4) prevede l'istituzione di un organismo di vigilanza permanente.

Il Piano triennale anticorruzione ex D.lgs. 190/12 deve ritenersi parte integrante del presente MOG.

2.1 Destinatari del Modello

Sono destinatari del MOG (di seguito i "Destinatari") l'Amministratore Unico di Adopera, i soggetti coinvolti nelle funzioni di Organismo di Vigilanza, i dipendenti, i consulenti esterni, i partner commerciali e i fornitori.
Più in generale il Modello è destinato a tutti coloro che esercitano, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo nella società ed i soggetti sottoposti alla direzione o vigilanza di costoro, quali i dipendenti, i collaboratori, i consulenti, gli agenti, i procuratori e - in via generale - a tutti i terzi che agiscono per conto della società nell'ambito delle attività ritenute anche potenzialmente a rischio di commissione di uno dei reati previsti dal Decreto.
Il rispetto del Modello è garantito mediante la previsione di un apposito sistema sanzionatorio ed anche attraverso l'adozione di clausole contrattuali che obbligano i soggetti esterni che operano per conto della società (collaboratori, consulenti, partner, clienti o fornitori) al rispetto delle previsioni del modello.

2.2 Struttura del MODELLO

Il Presente MOG è costituito da:

- Parte generale
- Parti speciali
- Allegati

3. IL PROCESSO DI REALIZZAZIONE DEL MODELLO

Le caratteristiche essenziali del metodo seguito per la costruzione del MOG corrispondono ad un tipico processo di gestione e valutazione dei rischi (Risk Management e Risk Assessment).

In questo contesto il MOG deve prevenire e gestire efficacemente i rischi identificati riconducendoli ad un livello di rischio definito "accettabile", che può essere identificato in un *«sistema di prevenzione tale da non poter essere aggirato se non* ***fraudolentemente****»*, in linea con la disposizione normativa che prevede quale criterio oggettivo di attribuzione della responsabilità l'elusione fraudolenta del modello di organizzazione.

Di conseguenza, la soglia di rischio deve essere tale da escludere che il soggetto operante in nome e per conto dell'azienda sia all'oscuro delle direttive aziendali e che il reato possa essere commesso a causa di un mero errore di valutazione delle direttive medesime.

3.1 Le fasi di costruzione del Modello

La costruzione del MOG adottato da Adopera è stata scandita dalle seguenti fasi:

1) FASE DIAGNOSTICA

La presente fase ha portato alla realizzazione delle seguenti attività:

- Organizzazione, pianificazione, comunicazione e avvio del Progetto;
- Raccolta documentazione ed informazioni preliminari;
- Interviste e surveys ai soggetti apicali ed ai loro sottoposti adibiti a mansioni sensibili.

2) RISK ASSESSMENT

La presente fase ha portato alla realizzazione delle seguenti attività:

- Identificazione e analisi delle aree a rischio;
- Identificazione degli specifici processi sensibili ai reati Decreto 231 previsti nel MOG ed emersi dall'analisi di dettaglio;

- Valutazione dei rischi attraverso la mappatura dei processi sensibili in termini di reati a cui ciascun processo risulta esposto, potenziali modalità attuative, funzioni organizzative coinvolte;
- Gap Analysis e definizione dei protocolli e/o procedure necessarie per ritenere il rischio accettabile.

3) REALIZZAZIONE DEL MOG

La presente fase ha portato alla realizzazione delle seguenti attività:

- Predisposizione del Codice di Comportamento;
- Realizzazione della parte generale del MOG;
- Realizzazione delle parti speciali del MOG;

Nelle parti speciali del Modello vengono specificamente analizzate le singole fattispecie di reato che la direzione ha inteso analizzare, le aree sensibili aziendali, le funzioni responsabili, i protocolli e le norme di comportamento per rendere il rischio di commissione dei reati presupposto accettabile anche attraverso una matrice di rischio P x D.

3.a LA VALUTAZIONE DEL RISCHIO

In particolare per la "Valutazione del Rischio di Infrazione e commissione del reato" è stata presa in considerazione da un lato la gravità degli effetti che tali reati presupposto possono provocare Gravità (Impatto/Danno) G, dall'altro la Probabilità P che il reato possa essere commesso.

Al fattore "Gravità (Impatto/Danno) G" è stato assegnato un valore crescente da 1 a 4, in base alla maggiore o minore "sensibilità" del processo/attività in esame, alla frequenza di esecuzione e alle considerazioni emerse rispetto alle responsabilità coinvolte anche attraverso specifiche interviste con le stesse. All'interno di tale fattore, sono contenute anche valutazioni generali in merito alla tipologia e alla gravità delle sanzioni (sanzioni pecuniarie e sanzioni interdittive) nelle quali la società può incorrere.
Tutto ciò precisando che Adopera mira a presidiare l'accadimento di qualsiasi fatto illecito contemplato nel D.Lgs 231/2001 per prevenire ogni tipologia di ricaduta in termini di immagine o di danno economico finanziario.

Il fattore "Probabilità P" sempre con valore assegnato da 1 a 4 è stato invece valorizzato in base alla presenza degli elementi individuati quali: linee guida di principio/indirizzo, prassi aziendali, autorizzazioni, ecc…), diretti a mitigare i rischi connessi alla concretizzazione dei reati. La conseguenza è che la scala individuata è inversa rispetto al fattore gravità/impatto cioè il giudizio di minore probabilità con

presidio/procedura efficace è pari a 1 mentre quello di presidio/procedura meno efficace (alta probabilità) è uguale a 4.

La classificazione del rischio è quindi il risultato della moltiplicazione tra i fattori "Gravità (Impatto/Danno) G" e Probabilità P.
Si può andare quindi da un potenziale Rischio Minimo 1 (dove entrambi i fattori sono valorizzati con 1) ad un Massimo Rischio avvalorato con 16 (dove entrambi i fattori sono stati stimati con valore pari a 4).

La classificazione finale del rischio è quindi il risultato della moltiplicazione tra i fattori:

R = G x (P- C) R = Gravità (Impatto/Danno) 1 X (Probabilità)

G = Gravità (Impatto/Danno)

Rappresenta la conseguenza materiale dell'evento

P = Probabilità

Rappresenta la probabilità che il fatto si verifichi

Le probabilità che il management deve assegnare al fatto che l'evento si verifichi:

Livello del Rischio

Si può iniziare/passare quindi da un potenziale Rischio Trascurabile 1 (dove entrambi i fattori sono valorizzati con 1) ad un Rischio Alto valutato con 16 (dove entrambi i fattori sono stati stimati con valore pari a 4) (Tav. 4).

Matrice per la classificazione del Rischio

G (Gravità) Impatto/Danno	Probabilità P			
	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

I valori individuati con colore verde (da 1 a 2) indicano un rischio trascurabile, quelli evidenziati in giallo (3 e 4) rischio basso, quelli in arancio rischio medio (6 e 8) e quelli con colore rosso (9, 12 e 16) rischio alto.

Classificazione del Rischio

Livello di Rischio	Definizione del Rischio rilevato	Danno – Impatto	Sigla2
1 - 2	**Trascurabile - Improbabile**	**Poco dannoso**	T
3 – 4	**Basso – Poco probabile**	**Moderatamente dannoso**	B
6 – 8	**Medio – Probabile**	**Dannoso**	M
9 – 12 – 16	Alto – Effettivo – Reale	Molto dannoso	A

La classificazione in fasce di gravità sopra riportata (Rischio: Trascurabile, Basso, Medio, Alto) consente di individuare congruentemente le priorità di attuazione delle azioni stesse e quindi le aree e i processi nei quali è necessario intervenire per mitigare/eliminare il rischio.

Possono essere consigliate delle azioni di miglioramento anche nel caso di rischi valutati come trascurabili, nella direzione di un miglioramento complessivo dell'intero sistema.

Valutazione finale del Rischio inteso come Rischio Residuo

Alla fine di tutto il processo e all'atto della "Mappatura" del rischio di commissione dei reati, analizzando ogni reato contemplato dal decreto si dovrà distinguere:

1) Reati che non hanno possibilità di essere commessi nel contesto aziendale;
2) Reati per cui esiste la possibilità di essere commessi.

A questo punto per quelli per cui esiste la possibilità di essere commessi si valuta il Rischio Finale di commissione che dovrà risultare accettabile sulla base delle procedure/protocolli presenti nella realtà aziendale.

STIMA DELL' AREA RISCHIO

Contestualmente alla determinazione dell'esposizione del Reato o Illecito si valuta:

- qual è la probabilità che dal pericolo, al quale il settore è esposto possa derivare un illecito o la commissione di un reato;

- qual è l'entità del possibile danno se tale probabilità si materializza.

La stima viene effettuata utilizzando le informazioni acquisite nella fase di

"Valutazione dell'esposizione" e utilizzando la scala semi-quantitativa descritta qui di seguito:

Scala delle probabilità che avvenga un danno In Riferimento all' Evento (Reato) vagliato.

	Probabilità	Definizione
1	Trascurabile Improbabile Irrilevante	- Non sono noti episodi già verificati, e/o - L'evento si può verificare solo per una concatenazione di eventi improbabili e tra loro indipendenti, e/o - Il verificarsi dell'evento susciterebbe incredulità in azienda e/o - rischi a livello di assenza di probabilità (Improbabile – Trascurabile – Irrilevante) e perciò accettabili anche in assenza di azioni correttive e/o - la mancanza rilevata può provocare un danno per la concomitanza di più eventi poco probabili e indipendenti, e/o - non sono noti eventi o episodi già verificatisi.
2	Basso Poco probabile Tollerabile	- Sono noti rari episodi già verificati, e/o - l'evento può verificarsi solo in circostanze particolari, e/o - il verificarsi dell'evento susciterebbe sorpresa in azienda, e/o - rischi con probabilità trascurabile (Poco Probabile - Tollerabile – Basso) e/o - il pericolo può provocare un danno solo in circostanze sfortunate, e/o

3	Medio Probabile Moderato	- E' noto qualche episodio in cui il pericolo ha causato danno, e/o - il pericolo può trasformarsi in danno anche se non in modo automatico, e/o - il verificarsi dell'evento susciterebbe scarsa sorpresa in azienda, e/o - rischi con probabilità di esposizione media (Probabile - Moderato – Medio) che l'impresa deve gestire e governare, e/o - il pericolo può provocare un danno anche se in modo automatico o diretto, e/o - è noto qualche episodio in cui la mancanza ha fatto seguire un danno.
4	Alto Effettivo Reale	Rischio effettivo (esistente, concreto, reale) che la società deve eliminare o neutralizzare - Sono noti episodi in cui la commissione ha causato danno, e/o - il pericolo esiste e può trasformarsi in danno con una correlazione diretta, e/o - il verificarsi dell'evento non susciterebbe sorpresa/incredulità in azienda, e/o - rischi con elevato livello di probabilità di impatto che rappresentano un rischio NON accettabile (Molto Probabile – Intollerabile - Alto) che l'impresa deve assolutamente eliminare, e/o - esiste una correlazione diretta tra il pericolo ed il verificarsi del danno ipotizzato e/o - si sono già verificati danni per la stessa mancanza rilevata nella stessa azienda o in aziende simili.

Scala dell'entità del Danno

	Gravità (Danno/Impatto)	Definizione
1	Lieve	Danno con effetti rapidamente reversibili.

		Comportamento continuato con effetti rapidamente reversibili. 1) Se l'evento si verifica che danno può provocare alla società? 2) Se l'evento si verifica quanto può compromettere l'attività della società? 3) Che conseguenze temporali può avere?
2	Significativo	Danno con effetti significativi reversibili a medio termine. Danno con effetti durevoli ma reversibili. 1) Se l'evento si verifica che danno può provocare alla società? 2) Se l'evento si verifica quanto può compromettere l'attività della società? 3) Che conseguenze temporali può avere?
3	Grave	- Danno/Impatto che può provocare mancato funzionamento della società e/o - Danno con effetti significativi irreversibili, e/o - Danno con effetti irreversibili o parzialmente irreversibili. 1) Se l'evento si verifica che danno può provocare alla società? 2) Se l'evento si verifica quanto può compromettere l'attività della società? 3) Che conseguenze temporali può avere?
4	Gravissimo	- Danno/ Impatto che può compromettere il mantenimento della società, che può produrre pregiudizio alla sicurezza ed incolumità delle persone o impatti ambientali negativi, o comunque che non soddisfa i requisiti di legge / normativi cogenti, e/o - Danno con effetti molto gravi irreversibili o conseguenze letali e fatali per la società e/o - Esposizione cronica con effetti letali o totalmente invalidanti. 1) Se l'evento si verifica che danno può provocare alla società? 2) Se l'evento si verifica quanto può compromettere l'attività della società? 3) Che conseguenze temporali può avere?

Per gli specifici reati presupposto analizzati, pertanto, il rischio è stato calcolato sulla base delle valutazioni sopra descritte anche a fronte di colloqui con il personale coinvolto nei lavori di redazione del presente MOG per poi valutare ed individuare i protocolli e le procedure necessarie al fine di ritenere il rischio accettabile.

4. COMPONENTI DEL MODELLO

Le componenti del Modello adottato da Adopera si possono riassumere nella seguente struttura:

MODELLO DI GOVERNO DELL'ENTE

CODICE ETICO

SISTEMA DISCIPLINARA

ORGANISMO DI VIGILANZA

COMUNICAZIONE E FORMAZIONE (WHISTLEBLOWING)

5. IL MODELLO DI GOVERNO AZIENDALE

Al fine di perseguire un efficiente ed efficace governo della Società per il raggiungimento degli obiettivi prefissati è necessario organizzare l'azienda secondo un modello di governo che assicuri un valido sistema di controllo interno e di compliance, contemplando un sistema organizzativo, un sistema dei poteri e delle deleghe ed un sistema dei processi aziendali.

5.1 Il sistema organizzativo

Adopera ha formalizzato il proprio sistema organizzativo il quale definisce:

- L'organigramma della Società;
- Le linee di dipendenza gerarchica;
- Le funzioni e le relative responsabilità, con l'indicazione di eventuali deleghe o procure conferite.

Il Manuale viene aggiornato ad ogni modifica organizzativa permanente ed è diffuso a tutti i dipendenti.

5.2 Il sistema dei poteri

Il Sistema dei Poteri di Adopera è strutturato in modo da definire i seguenti 3 livelli:

- **Poteri "esterni"** (deleghe o procure): sono poteri conferiti a determinate funzioni aziendali per compiere determinate attività in nome e per conto della Società nei confronti di terzi, quali ad esempio firmare un contratto di assunzione di personale o di acquisto di beni o servizi, aprire un conto corrente ecc.;
- **Poteri "interni**": sono autorizzazioni ad efficacia interna in forza delle quali le funzioni aziendali esercitano un potere o un controllo nell'ambito di un determinato processo, ad esempio l'autorizzazione di una richiesta di acquisto, la verifica e conferma della ricezione di un bene o servizio richiesto, l'autorizzazione ad un pagamento ecc.;
- **Procure speciali**: sono le deleghe o procure conferite per l'esercizio di un singolo atto.

Tutti i poteri conferiti devono rispettare il principio della separazione delle funzioni, devono essere redatti in forma scritta e riportati negli specifici mansionari aziendali.

5.3 Il sistema dei processi

Un processo aziendale è un insieme di fasi, ciascuna costituita da una serie di attività, svolte in sequenza e/o in parallelo, che partendo da un dato input iniziale permettono di raggiungere un determinato output finale.

Nell'ambito più generale dei processi aziendali, Adopera ha individuato quelli cosiddetti "sensibili" in ordine alla potenziale commissione dei reati previsti dal D.Lgs. 231/2001 e per i quali ha definito dei "Protocolli" di controllo, ossia un insieme di principi, meccanismi organizzativi, operativi e di comportamento, funzionali alla gestione del rischio-reato, nel senso che la loro corretta applicazione – anche in combinazione con altre norme di condotta – è tale da prevenire la commissione dei reati contemplati dal Decreto.

I processi aziendali, e in particolare quelli sensibili:

- sono definiti nel rispetto di principi e norme di comportamento adottate dalla Società (correttezza, trasparenza, onestà, collaborazione, integrità,…)
- prevedono meccanismi interni di controllo;

- sono caratterizzati per quanto possibile dal principio di segregazione delle funzioni nello svolgimento del processo;
- sono coerenti rispetto alle responsabilità organizzative assegnate, ai poteri interni ed esterni, al Codice di Comportamento ed alla normativa vigente;
- sono tracciabili e verificabili al fine di dimostrare l'applicazione e il rispetto dei punti precedenti;
- sono aggiornati all'evolvere del contesto organizzativo, di business e normativo;
- sono oggetto di controllo dell'attività in quanto ritenuta sensibile ai reati ex Decreto 231;
- sono formalizzati all'interno di documenti e/o procedure aziendali che ne disciplinano modalità operative, responsabilità e protocollo di prevenzione; tali documenti sono diffusi a tutte le funzioni aziendali che partecipano al relativo processo.

5.3.1. Rapporto tra Modello e Piano di prevenzione della corruzione ex L. 190/2012

La legge 6 novembre 2012, n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" (c.d. "Legge Anticorruzione") – pubblicata in G.U. n. 265 del 13/11/2012 e entrata in vigore il 28/11/2012 – è finalizzata ad avversare i fenomeni corruttivi e l'illegalità nella pubblica amministrazione.
L'intervento legislativo si muove nella direzione di rafforzare l'efficacia e l'effettività delle misure di contrasto al fenomeno corruttivo puntando ad uniformare l'ordinamento giuridico italiano agli strumenti sovranazionali di contrasto alla corruzione già ratificati dal nostro Paese, in particolare, la Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione, adottata dall'Assemblea generale dell'O.N.U. il 31 ottobre 2003 con risoluzione n. 58/4, firmata dallo Stato italiano il 9 dicembre 2003, e ratificata con legge 3 agosto 2009, n. 116. La L. 190/12 interviene sia sul piano repressivo, che preventivo, riformulando i principali reati corruttivi previsti dal Codice Penale, inasprendo le pene e introducendone di nuovi.
La L. 190/12 avvia anche alcune norme di carattere attuativo: D. Lgs 33/13 (trasparenza) e D. Lgs 39/2013 (inconferibilità e incompatibilità di incarichi). A livello nazionale il sistema di prevenzione e contrasto della corruzione nella pubblica amministrazione si articola nelle strategie individuate nel Piano Nazionale Anticorruzione (d'ora in poi "P.N.A."), predisposto dal Dipartimento della funzione pubblica secondo linee di indirizzo adottate dal Comitato interministeriale. Il P.N.A. è poi approvato dalla Commissione indipendente per la Valutazione, l'Integrità e la Trasparenza (C.I.V.I.T.).

Il 17 settembre 2013 la C.I.V.I.T., ora A.N.A.C. – Autorità Nazionale Anti corruzione, ha approvato la proposta di Piano Nazionale Anticorruzione ("P.N.A.") elaborata dal Dipartimento della funzione pubblica in base alla legge n. 190 del 2012. Il paragrafo 1.3. del P.N.A. ("Destinatari") stabilisce espressamente che i propri contenuti sono rivolti anche agli enti pubblici economici (ivi comprese l'Agenzia del Demanio e le Autorità Portuali), agli enti di diritto privato in controllo pubblico, alle società partecipate e a quelle da esse controllate ai sensi dell'art. 2359 c.c. per le parti in cui tali soggetti sono espressamente indicati come destinatari.
Il P.N.A., quindi, specifica (par. 3.1.1.) che al fine di dare attuazione alle norme contenute nella L. 190/12 gli enti pubblici economici e gli enti di diritto privato in controllo pubblico, di livello nazionale o regionale/locale "sono tenuti ad introdurre e ad implementare adeguate misure organizzative e gestionali".
Al fine degli adempimenti sopraccitati, "per evitare inutili ridondanze qualora questi enti adottino già modelli di organizzazione e gestione del rischio sulla base del d.lgs. n. 231 del 2001 nella propria azione di prevenzione della corruzione possono fare perno su essi, ma estendendone l'ambito di applicazione non solo ai reati contro la pubblica amministrazione previsti dal d.lgs. n. 231 del 2001 ma anche a tutti quelli considerati nella legge n. 190 del 2012, dal lato attivo e passivo, anche in relazione al tipo di attività svolto dall'ente (società strumentali/società di interesse generale). Tali parti dei modelli di organizzazione e gestione, integrate ai sensi della legge n. 190 del 2012 e denominate Piani di prevenzione della corruzione, debbono essere trasmessi alle amministrazioni pubbliche vigilanti ed essere pubblicati sul sito istituzionale."
Si evidenzia che con propria Determinazione n. 8 del 17 giugno 2015 l'A.N.A.C. ha emesso le "Linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici" che "integrano e sostituiscono, laddove non compatibili, i contenuti del P.N.A. in materia di misure di prevenzione della corruzione e di trasparenza che devono essere adottate dagli enti pubblici economici, dagli enti di diritto privato in controllo pubblico e dalle società a partecipazione pubblica."
In attuazione del quadro normativo ed attuativo sopra delineato, la Società, pertanto, ha:
predisposto il Piano di Prevenzione della Corruzione; previsto specifici protocolli e procedure al fine di ridurre il rischio di commissione dei reati presupposto introdotti dalla L. 190/12, secondo le metodologie di realizzazione dei Modelli organizzativi stabilite dal D.lgs. n. 231/01 e dalle "Linee Guida" di riferimento, assicurando nel contempo lo svolgimento delle proprie attività in conformità alla disciplina sulla "Trasparenza"; previsto, nel Piano di Prevenzione della Corruzione, appositi meccanismi di accountability (flussi informativi) che consentano ai cittadini di avere

notizie; trasmesso alla Autorità Pubblica vigilante il Piano di Prevenzione della Corruzione; adottato adeguati meccanismi di pubblicità del Piano; nominato il Responsabile per l'attuazione dei propri Piani di Prevenzione della Corruzione definendone compiti e responsabilità.
Alla luce ti tutto quanto sopra detto, la Società ha adottato il Piano, da ritenersi parte integrante del proprio Modello di organizzazione e controllo ai sensi del D. Lgs 231/01 (d'ora in poi "Modello 231") estendendo l'ambito di applicazione del MOG non solo ai reati contro la pubblica amministrazione previsti dal Decreto ma anche a tutti quei reati considerati nella Legge n.190 del 2012, dal lato attivo e passivo, in relazione al tipo di attività svolta.

5.3.2 I principi preventivi generali

Il MOG adottato da Adopera individua dei principi generali di riferimento al fine di prevenire la commissione dei reati ex Decreto 231.
Oltre ad un primo livello di presidi di controllo costituito dal sistema organizzativo e dei poteri, dal Codice di Comportamento, dal Sistema Disciplinare e dall'Organismo di Vigilanza, si aggiunge un secondo livello costituito da principi preventivi generali tali da rispettare le seguenti caratteristiche:

1) **Separazione delle attività** – deve esistere, per quanto possibile, separazione tra chi esegue, chi controlla e chi autorizza il Processo Sensibile e, analogamente, tra chi richiede (ed utilizza) risorse o prestazioni, chi soddisfa la richiesta e chi effettua il pagamento a fronte della richiesta soddisfatta;
2) **Norme** – devono esistere disposizioni aziendali idonee a fornire almeno principi di riferimento generali per la regolamentazione del Processo Sensibile (ivi compreso l'eventuale rimando al contenuto di normative in vigore);
3) **Poteri di firma e poteri autorizzativi** – devono esistere regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi da esercitare verso terzi esterni all'azienda e/o internamente all'azienda;
4) **Tracciabilità** – devono essere predisposti meccanismi idonei a tracciare il contenuto delle attività sensibili ed identificare i soggetti coinvolti;
5) **Procedure** – Il Processo Sensibile deve trovare regolamentazione a livello di modalità tecnico-operative in una o più procedure formalizzate;
6) **Reporting** – Il Processo Sensibile deve essere supportato da adeguata reportistica che includa indicatori di anomalie ritenuti efficaci per la prevenzione e/o identificazione dei reati. Tale reportistica deve essere sistematicamente trasmessa all'Organismo di Vigilanza, secondo le modalità con esso concordate.

Segue infine un ulteriore livello costituito da protocolli specifici applicabili a singoli processi o attività, in aggiunta alle misure preventive generali.

6. IL CODICE DI COMPORTAMENTO (Regolamento interno)

E' un documento adottato da Adopera in cui sono individuati i principi generali e le regole comportamentali cui viene riconosciuto valore etico positivo; allo stato il documento cui fa riferimento l'Organizzazione è il Regolamento Interno anno 2014.

Esso ha lo scopo di indirizzare eticamente l'agire della azienda e le sue disposizioni sono conseguentemente vincolanti per i comportamenti di tutti gli amministratori dell'impresa, dei suoi dirigenti, dipendenti, consulenti e di chiunque vi instauri, a qualsiasi titolo, un rapporto di collaborazione.

7. IL SISTEMA DISCIPLINARE

Il sistema disciplinare aziendale si riferisce a quanto stabilito nel CCNL dei Igiene Ambientale Federambiente ed al CCNL settore edilizia.

Al fine di soddisfare il requisito richiesto dal d.lgs. 231/01 pertanto, tali disposizioni vengono integrate anche con la previsione di sanzioni applicabili in caso di violazione delle regole e dei principi stabiliti nell'ambito del MOG, con particolare riferimento alle norme contenute nel Codice di condotta dei pubblici dipendenti ex DPR 62/13 valido anche come codice di comportamento, nel Sistema dei Poteri, nelle norme di comportamento generali e protocolli preventivi specifici previsti nelle parti speciali del MOG, alle norme e disposizioni sulla salute e sicurezza sul lavoro e negli obblighi di comunicazione all'Organismo di Vigilanza.

Sono state inoltre introdotte specifiche sanzioni per l'inosservanza delle disposizioni del MOG da parte dei membri dell'Amministratore Unico e dei fornitori, collaboratori esterni che agiscono in nome e per conto della Società, prevedendo specifiche clausole contrattuali.

Al fine, inoltre, di conformarsi alle modifiche apportate al D.lgs. 231/2001 dal D.lgs. 24/23 in materia di whistleblowing, il sistema disciplinare adottato da Adopera trova, altresì, applicazione anche nei confronti di chi, con riferimento alle segnalazioni descritte al seguente paragrafo 9.4:

- viola le misure di tutela predisposte dalla Società a favore del segnalante;
- effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

Tali previsioni sono state introdotte allo scopo di garantire maggiore tutela al segnalante e, al contempo, dissuadere eventuali segnalazioni pretestuose e infondate, non rispondenti alle finalità del Modello Organizzativo.

7.1 Le sanzioni per i dipendenti

L'osservanza, da parte dei dipendenti (inclusi i dirigenti) della Società, delle disposizioni contenute nel Codice di condotta valido anche come Codice di Comportamento, nel MOG, nei protocolli aziendali e nelle procedure previste dal MOG ovvero dal medesimo richiamate, costituisce parte fondamentale delle loro obbligazioni contrattuali ai sensi e per gli effetti dell'articolo 2104 del Codice Civile.

La violazione di dette disposizioni, pertanto, concreterà un inadempimento delle obbligazioni derivanti dal rapporto di lavoro da parte del dipendente e comporterà la comminazione di sanzioni e/o misure di carattere disciplinare, nel rispetto del principio di gradualità e di proporzionalità, nonché delle procedure prescritte dalle norme applicabili come di seguito indicato, con ogni conseguenza di legge, anche in ordine alla conservazione del rapporto di lavoro e all'obbligo di risarcire i danni eventualmente cagionati.

Il Sistema Disciplinare è applicato in caso di mancato rispetto delle procedure interne, dei principi e delle *policies* (ivi compresi gli ordini impartiti dall'azienda sia in forma scritta che verbale) previsti o richiamati nel presente MOG e nel Codice di Comportamento, cioè nel caso in cui vengano posti in essere determinati comportamenti sanzionabili (impregiudicate le conseguenze anche disciplinari eventualmente derivanti dalle violazioni di altri obblighi previsti dalla legge e/o dal Contratto Collettivo Nazionale applicabile).

In base a quanto previsto dal CCNL Igiene Ambientale Federambiente e dal CCNL settore Edilizia, le mancanze del lavoratore dipendente (non figura apicale) possono dar luogo all'adozione, a seconda della loro gravità e recidività, di uno dei seguenti provvedimenti disciplinari:

a) richiamo verbale;
b) ammonizione scritta;
c) multa fino all'importo di 4 ore di paga;
d) sospensione dal lavoro fino a 10 giorni.
e) licenziamento con preavviso e TFR;
f) licenziamento senza preavviso e con TFR.

I provvedimenti di cui sopra non sollevano inoltre il lavoratore dalle eventuali responsabilità nelle quali egli sia incorso.

Tali sanzioni vengono irrogate al dipendente non solo in caso di violazione concreta dei principi di comportamento e/o delle prescrizioni del MOG, del Codice di Comportamento e/o delle procedure interne previste dal presente MOG ed in caso di condotte non conformi alle prescrizioni dello stesso, ma altresì in caso di illeciti disciplinari tentati, ossia di comportamenti od omissioni diretti in modo non equivoco a disattendere le regole comportamentali dettate dal presente MOG.

Per quanto riguarda i criteri di correlazione tra le mancanze dei lavoratori ed i provvedimenti disciplinari, viene stabilito che:

1) per la violazione delle norme di comportamento stabilite dal Codice di Comportamento e dal MOG saranno adottati i provvedimenti dell'ammonizione verbale o scritta, nei casi di prima mancanza, purché la violazione non configuri un reato. Il rimprovero verbale verrà applicato per le mancanze di minor rilievo;
2) il provvedimento della multa verrà adottato nei casi di maggiore gravità, anche in relazione alle mansioni applicate, o in caso di recidiva, mentre la sospensione verrà comminata qualora il lavoratore sia già stato punito con la multa nei 6 mesi precedenti.
3) Incorre nel provvedimento di licenziamento il lavoratore che provochi all'Azienda grave nocumento morale e/o materiale o che compia, in connessione con lo svolgimento del rapporto di lavoro, azioni che costituiscono reato a termine di legge.

Ove si faccia riferimento alla "gravità" delle violazioni del MOG essa sarà definita in relazione alle seguenti circostanze:

- il livello di responsabilità ed autonomia dell'autore della violazione;
- l'eventuale esistenza di precedenti situazioni di violazione a carico dello stesso;
- la presenza e l'intensità dell'elemento intenzionale;
- in relazione alle condotte colpose, la presenza ed il grado della negligenza, imperizia, imprudenza nell'inosservanza della regola cautelare;
- la prevedibilità delle conseguenze della condotta;
- la gravità del comportamento, con ciò intendendosi il livello di rischio e le conseguenze a cui la Società può ragionevolmente ritenersi esposta, ai sensi e per gli effetti del MOG, a seguito della condotta censurata;
- i tempi, i modi e le ulteriori circostanze nelle quali la violazione ha avuto luogo.

In materia di sicurezza e salute dei lavoratori, poiché il dipendente è vincolato altresì al rispetto dei principali obblighi previsti dall'articolo 20 del Decreto 81 del 2008, in caso di loro violazione, vengono applicate le suddette sanzioni, graduate anche in base al rischio di applicazione delle misure del Decreto che tale condotta ha provocato.
In caso di violazione, **da parte delle figure apicali** della Società, delle disposizioni, dei principi di comportamento e delle procedure contenute nel MOG o Codice di Comportamento, ovvero di adozione di un comportamento non conforme alle disposizioni del MOG e qualificabile come "sanzionabile", nei confronti dei responsabili saranno adottate le seguenti sanzioni:

a) Ammonizione scritta;
b) Licenziamento.

A titolo esemplificativo, la figura apicale incorrerà nel provvedimento del/della:

- **Ammonizione scritta**, in caso di violazione non grave di una o più regole procedurali o comportamentali previste nel MOG, l'osservanza delle quali costituisce condizione necessaria per il mantenimento del rapporto fiduciario con la Società, tenuto particolarmente conto delle responsabilità affidate alla figura apicale;
- **Licenziamento con preavviso**, ai sensi dell'art. 2118 del Codice Civile e delle norme del CCNL Federambiente e del CCNL settore Edilizia, in caso di grave violazione di una o più prescrizioni del MOG (ossia delle regole procedurali o comportamentali ivi incluse), o di reiterazione di una o più violazioni di cui al punto che precede, tale da configurare – a seguito delle opportune e necessarie verifiche da parte della Società – un notevole inadempimento da ascriversi a colpa o dolo della figura apicale;
- **Licenziamento senza preavviso,** ai sensi dell'art. 2119 del Codice Civile e delle norme del CCNL Federambiente e del CCNL settore Edilizia, laddove la violazione di una o più prescrizioni del MOG (ossia delle regole procedurali o comportamentali ivi incluse) sia di gravità tale da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione anche provvisoria del rapporto di lavoro.

La sanzione concretamente da applicarsi sarà determinata in base alle circostanze sopra indicate con riferimento alla generalità dei dipendenti.

In ogni caso, per i lavoratori aventi la qualifica di figura apicale costituisce grave violazione delle prescrizioni del Modello:

- L'inosservanza dell'obbligo di direzione o vigilanza sui lavoratori subordinati circa la corretta ed effettiva applicazione del MOG;
- L'inosservanza dell'obbligo di vigilanza sugli altri destinatari del MOG che, sebbene non legati alla Società da un rapporto di lavoro subordinato, siano comunque soggetti alle prescrizioni del Modello stesso (es. appaltatori, fornitori, consulenti, etc.).

Fermo restando quanto sopra, la Società si riserva sin d'ora il diritto di agire nei confronti della figura apicale che sia stato oggetto delle misure sopra indicate per il ristoro dei danni subiti e/o di quelli che la Società sia tenuta a risarcire a terzi.

7.2 Le sanzioni per gli amministratori

Nei confronti dell'Amministratore Unico che abbia violato una o più regole di condotta stabilite dal Codice di Comportamento e/o dal MOG viene comminata una sanzione graduabile dal richiamo scritto alla revoca dalla carica e/o delle deleghe, in considerazione dell'intenzionalità e gravità del comportamento posto in essere (valutabile in relazione anche al livello di rischio cui la Società risulti esposta) e delle particolari circostanze in cui il suddetto comportamento si sia manifestato.

In particolare, nei confronti degli Amministratori potranno essere adottate le seguenti misure disciplinari:

- **Richiamo scritto** con intimazione a conformarsi alle disposizioni del MOG, che potrà essere irrogato in caso di lieve inosservanza dei principi e delle regole di comportamento contenute nel presente MOG, nel Codice di Comportamento, o nelle procedure aziendali;
- nei casi più gravi di violazioni integranti un inadempimento delle prescrizioni e/o delle procedure e/o delle norme interne contenute nel presente MOG, anche solo potenzialmente suscettibili di configurare un reato e/o un illecito amministrativo e/o una condotta consapevolmente in contrasto con le suddette prescrizioni, si potrà procedere, in considerazione dell'intenzionalità e gravità del comportamento posto in essere (valutabile in relazione anche al livello di rischio cui la Società risulta esposte) e delle particolari circostanze in cui il suddetto comportamento si sia manifestato, rispettivamente, all'applicazione delle seguenti misure:

  i) **revoca totale o parziale delle deleghe** eventualmente conferite e
  (ii) **revoca del mandato** con effetto immediato.

E' fatto salvo in ogni caso il diritto della Società al risarcimento dei danni subiti.

7.3 Sanzioni per Organo di Controllo di Adopera

In caso di violazione delle disposizioni contenute nel MOG e nel Codice di Comportamento da parte di uno o più membri del Revisore Unico, l'Amministratore Unico e/o l'Organismo di Vigilanza dovrà informare, senza ritardo e per iscritto, l'intero e verranno presi tutti gli opportuni provvedimenti consentiti dalla vigente normativa, compresa la revoca dell'incarico conferito ai soggetti.

Nei casi ritenuti di maggiore gravità, l'Amministratore Unico, sentito il Revisore Unico, convocherà l'Assemblea per gli opportuni provvedimenti.

Nell'ipotesi in cui sia stato disposto il rinvio a giudizio di uno o più dei Sindaci, presunti autori del reato da cui deriva la responsabilità amministrativa della Società, l'Amministratore Unico o il Revisore Unico dovrà procedere alla convocazione dell'Assemblea dei Soci per deliberare in merito alla eventuale revoca del mandato o di eventuali e differenti scelte, comunque adeguatamente motivate.

Analoga procedura troverà applicazione anche per eventuali successive fasi processuali.

In ogni caso, è fatta salva la facoltà della Società di esercitare azioni di responsabilità e risarcitorie.

7.4 Sanzioni per fornitori e collaboratori esterni che agiscono in nome e per conto di Adopera

Allo scopo di garantire l'effettività del MOG, anche nei confronti dei fornitori e collaboratori esterni che agiscono in nome e per conto di Adopera, è prevista una clausola da inserire nel contratto di riferimento del fornitore che stabilisce l'obbligo con relativa sanzione, di attenersi alle regole del Codice di Comportamento e del MOG (clausola risolutiva espressa).

In caso di violazione da parte di collaboratori, fornitori o partner commerciali delle disposizioni del Modello (o del Codice di Comportamento), pertanto, l'Amministratore Unico, sentito se del caso l'Organismo di Vigilanza, valuterà se porre termine alla relazione contrattuale in essere e comminerà l'eventuale sanzione prevista dal contratto stesso.

Il contratto con collaboratori, fornitori e partner dovrà essere immediatamente risolto dalla Società nel caso in cui essi si rendano responsabili della violazione delle prescrizioni e/o delle procedure e/o delle norme interne contenute o richiamate nel presente MOG o nel Codice di Comportamento, anche solo

potenzialmente suscettibili di configurare un reato e/o un illecito amministrativo e/o una condotta consapevolmente in contrasto con le suddette prescrizioni, se così previsto dallo stesso contratto.

Per quanto riguarda i lavoratori legati alla società da rapporti di lavoro di natura diversa dal lavoro subordinato (collaboratori e, in generale, soggetti esterni) le misure applicabili e le procedure disciplinari avvengono nel rispetto della legge e delle condizioni contrattuali.

7.5 Applicazione delle sanzioni e organo competente

L'adozione dei provvedimenti disciplinari nei confronti dei dipendenti della Società dovrà essere effettuata nel rispetto di quanto stabilito dall'art. 7 della Legge 20/05/1970 n. 300 (Statuto dei Lavoratori), per quanto riguarda la contestazione dell'illecito e per l'irrogazione della relativa sanzione, previsioni che si intendono in questa sede integralmente richiamate. In particolare:

- non verrà adottato alcun provvedimento disciplinare senza che l'addebito sia stato preventivamente contestato al lavoratore e senza averlo sentito a sua difesa;
- i provvedimenti disciplinari più gravi del rimprovero verbale non verranno applicati prima che siano trascorsi cinque giorni dalla contestazione per iscritto del fatto che vi ha dato causa, nel corso dei quali il lavoratore potrà presentare le proprie giustificazioni, eventualmente con l'assistenza di un rappresentante sindacale;
- qualora il provvedimento disciplinare non venga adottato nei sei giorni successivi alla presentazione di tali giustificazioni, queste si intenderanno accolte;
- la comminazione di ogni provvedimento disciplinare più grave del richiamo verbale verrà comunicata mediante provvedimento scritto motivato;
- non si terrà conto, ai fini della recidiva, dei provvedimenti disciplinari decorsi due anni dalla loro comminazione.

L'applicazione del sistema delle sanzioni in ordine alla violazione del Codice di Comportamento o del MOG è autonoma rispetto allo svolgimento e all'esito del procedimento penale eventualmente avviato presso l'Autorità giudiziaria competente in ragione della violazione stessa.
Le presunte violazioni del Codice di Comportamento e del Modello devono essere tempestivamente segnalate all'Organismo di Vigilanza, il quale potrà effettuare verifiche e controlli in piena autonomia ed eventualmente inoltrare

all'Amministratore Unico una propria relazione in ordine all'adozione dei provvedimenti ritenuti idonei.

L'organo competente a deliberare in merito all'irrogazione di sanzioni per la violazione del Codice di Comportamento e del MOG è l'Amministratore Unico o, nei casi in cui sia coinvolto l'Amministratore stesso, l'Assemblea dei Soci.

7.6 Il ruolo di sorveglianza dell'ODV

Il sistema disciplinare qui contemplato è soggetto a costante verifica da parte dell'Organismo di Vigilanza.

In particolare, l'Organismo di Vigilanza verifica che la Società abbia provveduto ad assicurare adeguata informazione in merito all'esistenza del Sistema Disciplinare ed alle conseguenze che possono derivare dalla violazione dei principi e delle norme di comportamento previste o richiamate dal Modello e dal Codice di Comportamento, in favore dei lavoratori e di tutti i soggetti destinatari dello stesso.

Inoltre, l'Organismo di Vigilanza provvede a riferire tempestivamente agli organi di vertice della Società le eventuali segnalazioni ricevute in merito a possibili violazioni del Modello o del Codice di Comportamento, nonché a richiedere alle funzioni aziendali preposte e delegate alla gestione dei procedimenti disciplinari e all'irrogazione delle sanzioni, informazioni, dati e/o notizie utili a vigilare sulla corretta applicazione del Sistema Disciplinare.

Infine, l'Organismo di Vigilanza, pur non disponendo di poteri disciplinari o sanzionatori diretti, deve essere informato in merito ai procedimenti disciplinari svolti ed alle eventuali sanzioni irrogate, ovvero ai provvedimenti motivati di archiviazione di procedimenti disciplinari a carico del personale aziendale, adottati dalla Società.

8. L'ORGANISMO DI VIGILANZA

8.1 Individuazione

Al fine di garantire alla Società l'esimente dalla responsabilità amministrativa in conformità a quanto previsto dall'art. 6 del Decreto 231, è necessaria l'individuazione e la costituzione da parte della Società di un Organismo di Vigilanza fornito dell'autorità e dei poteri necessari per vigilare, in assoluta autonomia, sul funzionamento e sull'osservanza del Modello, nonché di curarne il relativo aggiornamento, proponendone le modifiche o integrazioni ritenute opportune al Consiglio di Amministrazione della Società.

I componenti dell'Organismo di Vigilanza della Società (di seguito anche "**OdV**") sono scelti tra soggetti in possesso dei requisiti di autonomia, indipendenza e professionalità richiesti dal Decreto 231 per svolgere tale ruolo.

Il Decreto 231 non fornisce indicazioni alcuna circa la composizione dell'OdV; pertanto, la scelta tra una sua composizione mono-soggettiva o plurisoggettiva e l'individuazione dei suoi componenti - interni o esterni all'ente - devono tenere conto - come suggerito dalle Linee Guida di Confindustria e come confermato dalla giurisprudenza in materia - delle finalità perseguite dalla legge in uno con la tipologia di società nella quale l'OdV andrà ad operare, dovendo esso assicurare il profilo di effettività dei controlli in relazione alla dimensione e alla complessità organizzativa dell'ente.
In base a tali indicazioni, l'OdV deve possedere le seguenti principali caratteristiche:

a) Autonomia ed indipendenza

I requisiti di autonomia ed indipendenza che l'OdV deve necessariamente possedere, affinché la Società possa andare esente da responsabilità, si riferiscono in particolare alla funzionalità dello stesso OdV. La posizione dell'OdV nell'ambito delle Società dovrà cioè assicurare l'autonomia dell'iniziativa di controllo da ogni interferenza o condizionamento proveniente dalla Società e dai suoi organi dirigenti.
Tali requisiti sono assicurati tramite la collocazione dell'OdV in una posizione di vertice in seno all'organizzazione aziendale, senza attribuzione, formale o anche solo in via di fatto, di alcun ruolo esecutivo che possa renderlo partecipe di decisioni ed attività operative della Società, che altrimenti lo priverebbero della necessaria obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello.

I requisiti di autonomia e indipendenza oltre che a riferirsi all'OdV nel suo complesso debbono anche riferirsi ai suoi componenti singolarmente considerati: in caso di OdV a composizione plurisoggettiva, nei quali alcuni componenti siano esterni e altri interni, non essendo esigibile dai componenti di provenienza interna una totale indipendenza dalle Società, il grado di indipendenza dell'OdV dovrà essere valutato nella sua globalità.

Al fine di garantire l'effettiva sussistenza dei requisiti sopra descritti, è opportuno che i membri dell'OdV posseggano alcuni requisiti soggettivi formali che garantiscano ulteriormente la loro autonomia e indipendenza (ad esempio onorabilità, assenza di conflitti di interesse con gli organi sociali e con il vertice aziendale etc.).

b) Professionalità

I componenti l'OdV debbono possedere, così come specificato anche in talune pronunce giurisprudenziali, apposite competenze tecniche, onde poter provvedere efficacemente all'espletamento dei propri compiti ispettivi e di controllo. Trattasi di tecniche di tipo specialistico, proprie di chi svolge attività ispettiva, consulenziale e giuridica.
Con riferimento all'attività ispettiva e di analisi del sistema di controllo, è opportuno che i membri dell'OdV abbiano esperienza, ad esempio, nelle tecniche di analisi e valutazione dei rischi, nelle misure per il loro contenimento, nel *flow-charting* di procedure e processi per l'individuazione dei punti di debolezza, nelle tecniche di intervista e di elaborazione dei questionari. Tali tecniche possono essere utilizzate sia per adottare – all'atto del disegno del Modello Organizzativo e delle successive modifiche – le misure più idonee a ragionevolmente prevenire la commissione dei reati, sia per verificare che i comportamenti tenuti dalle persone che operano nelle Società rispettino effettivamente i comportamenti codificati, sia - eventualmente - per accertare come si sia potuto verificare un determinato reato e chi lo abbia commesso.

Con riferimento alle competenze giuridiche, si rileva che la disciplina di cui al Decreto 231 è sostanzialmente giuridico-penale e lo scopo del sistema di controllo previsto dal decreto è quello di prevenire la realizzazione di reati. E' dunque essenziale la conoscenza della struttura e delle modalità realizzative dei reati e del sistema giuridico e procedurale.

Si ricorda in ogni caso che l'OdV, al fine di adempiere ai propri compiti, può utilizzare, oltre alle competenze specifiche dei singoli membri, anche risorse aziendali interne o consulenti esterni.

c) Continuità di azione

Al fine di garantire l'efficace e costante attuazione del Modello, l'OdV deve garantire continuità nell'esercizio delle sue funzioni, che non deve essere intesa come "presenza continua", ma come effettività e frequenza del controllo.

La definizione degli aspetti attinenti alla continuità d'azione dell'OdV, quali la calendarizzazione dell'attività, la verbalizzazione delle riunioni e la disciplina dei flussi informativi dalle strutture aziendali all'OdV, è rimessa allo stesso Organismo, il quale, nell'esercizio della propria facoltà di autoregolamentazione, dovrà disciplinare il proprio funzionamento interno. A tal proposito è opportuno che l'OdV

stesso formuli un regolamento delle proprie attività (determinazione delle cadenze temporali dei controlli, individuazione dei criteri e delle procedure di analisi, etc.).

Tutto ciò considerato, in ottemperanza a quanto previsto all'art. 6 lettera b) del Decreto 231, è istituito presso un organo con funzioni di vigilanza e controllo (di seguito Organismo di Vigilanza – OdV) in ordine al funzionamento, all'efficacia, all'adeguatezza ed all'osservanza del Modello.

Nell'esercizio delle sue funzioni, l'OdV deve uniformarsi a principi di autonomia ed indipendenza.
A garanzia del principio di terzietà ed indipendenza, l'OdV è collocato in posizione gerarchica di vertice della Società. Esso deve riportare direttamente all'Amministratore Unico.

8.2 Composizione, Nomina e Durata

L'Organismo di Vigilanza di Adopera può essere o Collegiale o Monocratico; attualmente risulta essere monocratico con incarico affidato all'Avv. Alessandro Vasi.

I componenti dell'OdV rimangono in carica per tre anni e sono rieleggibili.

I componenti dell'Organismo di Vigilanza, nell'esercitare le proprie funzioni, devono mantenere i necessari requisiti di autonomia e indipendenza richiesti dal Decreto 231: essi devono, pertanto, comunicare immediatamente all'Amministratore Unico e allo stesso Organismo di Vigilanza l'insorgere di eventuali situazioni che non consentano di conservare il rispetto di tali requisiti.
I membri dell'Organismo di Vigilanza designati restano in carica per tutta la durata del mandato ricevuto.

Non possono essere eletti alla carica di componenti dell'Organismo di Vigilanza e, se eletti, decadono automaticamente dall'ufficio:

1. coloro che si trovano nelle condizioni previste dall'articolo 2382 del Codice Civile (interdizione, inabilitazione, fallimento, condanna ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici ovvero l'incapacità ad esercitare uffici direttivi);
2. il coniuge, i parenti e gli affini entro il quarto grado degli amministratori non-indipendenti della Società; il coniuge, i parenti e gli affini entro il quarto grado degli amministratori non-indipendenti delle società da questa controllate, delle società che la controllano e di quelle sottoposte a comune controllo;

3. coloro che sono stati condannati con sentenza ancorché non definitiva (ivi compresa quella pronunciata ex art. 444 c.p.p.):
    - alla reclusione per un tempo non inferiore a un anno: i) per uno dei delitti previsti dal RD n. 267/1942; ii) per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, dei mercati e dei valori mobiliari e di strumenti di pagamento; iii) per un delitto contro la pubblica amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica o in materia tributaria;
    - alla reclusione per un tempo non inferiore a due anni per qualunque delitto non colposo;
    - per uno o più reati tra quelli previsti e richiamati dal Decreto, a prescindere dal tipo di condanna inflitta;
    - per un reato che importi la condanna ad una pena da cui derivi l'interdizione, anche temporanea, dai pubblici uffici ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.
4. coloro che hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate le sanzioni previste dall'art. 9 del Decreto;
5. coloro nei cui confronti sia stata applicata una delle misure di prevenzione previste dall'art. 3 della legge 19 marzo 1990, n. 55 e sue successive modifiche.

Fatte salve le ipotesi di decadenza automatica, i componenti dell'OdV non possono essere revocati dall'Amministratore Unico se non per giusta causa, sentito il parere del Revisore Unico.

Rappresentano ipotesi di giusta causa di revoca:

- una sentenza di condanna della Società ai sensi del Decreto, o una sentenza di patteggiamento, ove risulti dagli atti l'"omessa o insufficiente vigilanza" da parte dell'OdV secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;
- il mancato riserbo relativamente alle informazioni di cui vengano a conoscenza nell'espletamento dell'incarico;
- la mancata partecipazione a più di tre riunioni dell'OdV consecutive senza giustificato motivo.

Nei casi di ODV Collegiale, in caso di dimissioni o di decadenza automatica di un componente dell'OdV, quest'ultimo ne darà comunicazione tempestiva all'Amministratore Unico, che prenderà senza indugio le decisioni del caso.

Nei casi di OdV Collegiale, tale organo si intende decaduto se vengono a mancare, per dimissioni o altre cause, la maggioranza dei componenti. In tal caso, l'Amministratore Unico provvede a nominare di nuovo tutti i componenti dell'OdV.

Ove sussistano gravi ragioni di convenienza, l'Amministratore Unico procederà a disporre sentito il parere del Revisore Unico e, ove non coinvolti, degli altri membri dell'OdV, la sospensione dalle funzioni di uno o tutti i membri dell'OdV, provvedendo tempestivamente alla nomina di un nuovo membro o dell'intero Organismo *ad interim*.

8.3 Compiti dell'Organismo di Vigilanza

L'OdV ha i seguenti compiti:

Attività di verifica e vigilanza

1) verificare periodicamente le attività poste in essere nell'ambito dei processi sensibili individuati dal Modello;
2) effettuare verifiche periodiche volte all'accertamento di quanto previsto dal MOG ed in particolare che le procedure e i controlli in esso contemplati siano posti in essere e documentati in modo conforme e che i principi del Codice di Comportamento siano rispettati;
3) vigilare sulla corretta applicazione del Sistema Disciplinare da parte delle funzioni aziendali allo stesso preposte;
4) verificare l'adeguatezza, l'efficacia e l'effettiva capacità del Modello di prevenire la commissione degli illeciti previsti dal Decreto.

Aggiornamento del Modello

5) valutare il mantenimento nel tempo della solidità e funzionalità del Modello, provvedendo affinché la Società curi l'aggiornamento del Modello 231; a tal proposito si specifica che il presente MOG non è altro che una fotografia dello stato attuale di Adopera che deve essere mantenuto "vivo" dall'OdV attraverso specifiche raccomandazioni al fine di potere ritenere tale MOG sempre attuale;
6) attività di follow-up, ossia verifica dell'attuazione e dell'effettiva funzionalità delle soluzioni proposte.

Reporting da e verso l'OdV

7) attuare, in conformità al Modello, un efficace flusso informativo nei confronti degli organi sociali competenti in merito all'efficacia e all'osservanza del

Modello, in particolare, predisporre periodicamente un rapporto da presentare all'Amministratore Unico, che evidenzi le problematiche riscontrate e individui le azioni correttive da intraprendere;

8) esaminare e valutare tutte le informazioni e/o le segnalazioni ricevute in relazione al Modello, ivi incluso per ciò che attiene le eventuali violazioni dello stesso;
9) in caso di controlli da parte di soggetti istituzionali, ivi inclusa la Pubblica Autorità, fornire il necessario supporto informativo agli organi ispettivi.

Informazione e formazione

10) promuovere iniziative per la formazione dei destinatari del Codice di Comportamento e del MOG, per la loro comunicazione e diffusione;
11) monitorare le iniziative, ivi inclusi i corsi e le comunicazioni, volte a favorire un'adeguata conoscenza del Modello da parte di tutti i Destinatari;
12) valutare e rispondere alle richieste di chiarimento provenienti dalle funzioni aziendali ovvero dagli organi amministrativi e di controllo, qualora connesse e/o collegate al Modello.

Nell'ambito delle attività sopra enunciate, l'OdV provvederà ai seguenti adempimenti:

- promuovere la diffusione e la verifica nel contesto aziendale della conoscenza e della comprensione dei principi delineati nel Modello;
- raccogliere, elaborare, conservare e aggiornare ogni informazione rilevante ai fini della verifica dell'osservanza del Modello;
- verificare e controllare periodicamente le aree e le attività a rischio individuate, effettuando, qualora lo ritenga necessario ai fini dell'espletamento delle proprie funzioni, anche controlli non preventivamente programmati (c.d. "controlli a sorpresa");
- monitorare e verificare il rispetto, da parte della Società, della normativa in tema di norme antinfortunistiche e sulla tutela dell'igiene e della sicurezza sul lavoro;
- verificare e controllare la regolare tenuta ed efficacia di tutta la documentazione inerente le attività/operazioni individuate nel Modello;
- verificare periodicamente le procure e le deleghe interne in vigore, raccomandando le necessarie modifiche nel caso in cui le stesse non siano più coerenti con le responsabilità organizzative e gestionali;
- istituire specifici canali informativi "dedicati", diretti a facilitare il flusso di segnalazioni ed informazioni verso l'Organismo;
- valutare periodicamente l'adeguatezza del Modello rispetto alle disposizioni ed ai principi regolatori del Decreto e le corrispondenti esigenze di aggiornamento;

- valutare periodicamente l'adeguatezza del flusso informativo e adottare le eventuali misure correttive.

Tutte le comunicazioni devono essere fatte per iscritto.

È fatto obbligo di informazione, in capo a qualunque funzione aziendale, dipendente e/o componente degli organi sociali, a fronte di richieste da parte dell'OdV o al verificarsi di eventi o circostanze rilevanti ai fini nello svolgimento delle attività di competenza dell'OdV.

Ai fini dello svolgimento degli adempimenti ad esso affidati, all'OdV sono attribuiti i poteri e le facoltà qui di seguito indicati:

- emanare disposizioni ed ordini di servizio intesi a regolare l'attività dell'Organismo nonché il flusso informativo da e verso lo stesso;
- accedere ad ogni e qualsiasi documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'OdV, ivi inclusi i libri societari di cui all'art. 2421 del cod. civ.;
- richiedere la collaborazione, anche in via continuativa, di strutture interne o ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello;
- disporre che i soggetti destinatari della richiesta forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso da parte delle strutture organizzative aziendali;
- condurre le indagini interne necessarie per l'accertamento di presunte violazioni delle prescrizioni del presente Modello;
- richiedere alle funzioni aziendali preposte e delegate alla gestione dei procedimenti disciplinari e all'irrogazione delle sanzioni informazioni, dati e/o notizie utili a vigilare sulla corretta applicazione del sistema disciplinare;
- richiedere, attraverso i canali e le persone appropriate, la riunione del Consiglio di Amministrazione per affrontare questioni urgenti;
- partecipare alle riunioni del Consiglio di Amministrazione;
- accedere alla documentazione elaborata dal Revisore Unico;
- richiedere ai responsabili di funzione di partecipare, senza potere deliberante, alle sedute dell'Organismo di Vigilanza.

Considerate le funzioni dell'Organismo di Vigilanza ed i contenuti professionali specifici da esse richieste, nello svolgimento dell'attività di vigilanza e controllo, l'Organismo di Vigilanza può essere supportato da uno staff dedicato (utilizzato,

anche a tempo parziale, per tali compiti specifici), oltre ad avvalersi del supporto delle altre funzioni interne alla Società che, di volta in volta, si rendessero necessarie per un'efficace attuazione del Modello.

L'Organismo di Vigilanza, qualora lo ritenga opportuno e/o nei casi in cui si richiedano a questa funzione attività che necessitino di specializzazioni professionali non presenti al suo interno, né all'interno della Società stessa, avrà la facoltà di avvalersi delle specifiche capacità professionali di consulenti esterni ai quali delegare predefiniti ambiti di indagine e le operazioni tecniche necessarie per lo svolgimento della funzione di controllo. I consulenti dovranno, in ogni caso, sempre riferire i risultati del loro operato all'Organismo di Vigilanza.

8.4 Autonomia operativa e finanziaria

L'OdV, anche demandando strutture interne, ha libero accesso presso tutte le funzioni aziendali senza necessità di ottenere ogni volta alcun consenso, al fine di ottenere, ricevere o raccogliere informazioni o dati utili per lo svolgimento delle proprie attività.

In sede di definizione del budget aziendale, l'Amministratore Unico deve approvare una dotazione iniziale di risorse finanziarie, proposta dall'OdV stesso, della quale l'OdV dovrà disporre per ogni esigenza necessaria al corretto svolgimento dei compiti cui è tenuto (consulenze specialistiche, trasferte, ecc) e di cui dovrà presentare rendiconto dettagliato.

8.5 Retribuzione dei componenti dell'ODV

L'Amministratore Unico riconosce emolumenti all'ODV decisi con apposita determina del medesimo organo.

9. COMUNICAZIONE FORMAZIONE E FLUSSI INFORMATIVI

9.1 Comunicazione dell'Organismo di Vigilanza verso gli Organi Societari

L'ODV riferisce in merito all'attuazione del Modello, all'emersione di eventuali aspetti critici e comunica l'esito delle attività svolte nell'esercizio dei compiti assegnati all'Amministratore Unico.

Sono previsti i seguenti flussi informativi:

1) su base semestrale, all'Amministratore Unico e al Revisore Unico, ai quali dovrà essere trasmessa una relazione scritta che evidenzi:
   - Quanto emerso dall'attività svolta dall'ODV nell'arco dell'anno nell'adempimento dei propri compiti;
   - il piano delle attività che intende svolgere nell'anno successivo;
   - eventuali modifiche normative in materia di responsabilità amministrativa degli enti;
   - il rendiconto relativo alle modalità di impiego delle risorse finanziarie costituenti il budget in dotazione all'ODV.

2) Immediatamente all'Amministratore Unico e/o al Responsabile antiriciclaggio ed anticorruzione in merito a:

- Gravi violazioni al Modello individuate durante lo svolgimento delle verifiche;
- eventuali problematiche significative scaturite dall'attività;
- carenze organizzative o procedurali idonee a determinare il concreto pericolo di commissione di reati rilevanti ai fini del Decreto;
- l'esistenza di modifiche normative particolarmente rilevanti ai fini dell'attuazione ed efficacia del Modello;
- ogni altra informazione rilevante al fine del corretto svolgimento delle funzioni proprie dell'OdV stesso, nonché al fine del corretto adempimento delle disposizioni di cui al Decreto.

Si prevede, inoltre che in caso di violazione del Modello commessa da parte dell'Amministratore, l'Organismo di Vigilanza procede agli accertamenti necessari e assume i provvedimenti opportuni.
In ogni caso Adopera Srl è dotata di specifica procedura denominata "Sistema reporting flussi".

Infine, l'OdV potrà chiedere di essere sentito dall'Amministratore Unico, dal Responsabile Anticorruzione, e dal responsabile Antiriciclaggio ogniqualvolta ritenga opportuno interloquire con detto organo; in ogni caso almeno una volta all'anno incontra l'RPCT di Adopera per ogni opportuna collaborazione e/o scambio informativo circa le rispettive verifiche. D'altra parte, l'OdV potrà essere convocato in ogni momento dall'Amministratore Unico, dall'RPCT e dagli altri organi societari per riferire su particolari eventi o situazioni inerenti al funzionamento ed al rispetto del Modello.

9.2 Comunicazione dell'ODV verso le funzioni di Adopera

L'ODV – a seconda delle circostanze - può inoltre:

- comunicare per iscritto i risultati dei propri accertamenti ai responsabili dei processi oggetto dei controlli. In tal caso, sarà necessario che l'ODV ottenga dai responsabili dei medesimi processi un piano delle azioni con relativa tempistica in ordine alle attività da migliorare, nonché le specifiche delle modifiche che saranno attuate;

- segnalare alle funzioni competenti per iscritto eventuali comportamenti / azioni non in linea con il MOG e con le procedure aziendali relative, al fine di acquisire tutte le informazioni da inviare alle funzioni competenti per valutare e applicare le sanzioni disciplinari.

Tali segnalazioni devono essere comunicate il prima possibile dall'ODV all'Amministratore Unico affinché assicurino il supporto delle strutture aziendali idonee nelle attività di accertamento e di attuazione delle misure correttive.

9.3 Obblighi di informazione nei confronti dell'ODV

Al fine di agevolare le attività di verifica e monitoraggio svolte dall'ODV il presidente del consiglio di amministrazione, l'amministratore delegato ed i responsabili di funzione individuati in seno all'organizzazione aziendale quali referenti dell'ODV, nell'ambito delle attività di loro competenza, sono tenuti a fornire, sempre e tempestivamente, all'Organismo di Vigilanza le informazioni che lo stesso ODV richieda nell'esercizio della propria attività, nonché ad inviare all'attenzione dello stesso, con la periodicità prevista nella procedura "sistema reporting flussi informativi 231" divulgata alle funzioni aziendali coinvolte, le informazioni, i documenti ed i dati relativi al periodo di riferimento considerato.

A titolo esemplificativo e non esaustivo, devono essere trasmesse all'ODV:

1) le notizie relative ai procedimenti disciplinari azionati in relazione a presunte violazioni del Modello ed alle eventuali azioni disciplinari intraprese, comprese le archiviazioni di tali procedimenti, con le relative motivazioni;
2) da parte delle funzioni aziendali, ciascuna per il proprio ambito di competenza, tutte le informazioni circa eventuali cambiamenti che possono influenzare l'adeguatezza e l'efficacia del Modello;
3) notizie relative ai cambiamenti organizzativi;
4) aggiornamenti del sistema delle deleghe;
5) report e altri protocolli di controllo posti in essere dalle funzioni responsabili dei processi aziendali;
6) report relativi alle consulenze e servizi professionali;
7) report relativi alle sponsorizzazioni, liberalità e omaggi;
8) report di attività aventi come interlocutore enti pubblici;

9) richieste di finanziamenti pubblici;
10) anomalie riscontrate dalle funzioni stesse;
11) provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per reati compiuti nell'esercizio dell'attività aziendale;
12) richieste di assistenza legale inoltrate da Amministratori, Dirigenti e/o dai dipendenti, nei confronti dei quali la Magistratura proceda per reati compiuti nell'esercizio dell'attività aziendale;
13) relazioni interne dalle quali emergano eventuali responsabilità per reati compiuti nell'esercizio dell'attività aziendale.

I flussi informativi di cui sopra devono essere effettuati in forma scritta al seguente indirizzo di posta elettronica:

ODV@ADOPERASRL.IT

La casella di posta elettronica dell'Organismo di Vigilanza è accessibile solamente da parte dei suoi componenti. A tal riguardo l'ODV è tenuto all'obbligo della riservatezza in relazione alle informazioni che dovesse ricevere nel corso della sua attività.

Adopera, titolare del trattamento dei dati personali ai sensi del Regolamento Europeo 2016/979 ("GDPR") e del D.Lg. 196/2003, tratterà i dati personali acquisiti mediante i flussi informativi per finalità connesse al rispetto degli obblighi derivanti dal Decreto 231/01 e dal Modello Organizzativo. I dati potranno essere trattati sia in forma cartacea che mediante l'utilizzo di strumenti elettronici. L'interessato potrà esercitare i diritti di cui al Capo III del GDPR rivolgendosi al titolare del trattamento.

L'inadempimento dell'obbligo di informazione nei confronti dell'ODV deve essere considerato come specifico illecito disciplinare. Pertanto, i responsabili di funzione che non adempiano correttamente all'obbligo di informativa nei confronti dell'Organismo di Vigilanza nei termini e nei modi qui delineati possono essere soggetti all'applicazione di sanzioni disciplinari.

9.4 Segnalazione di comportamenti illegittimi ai sensi del D.lgs. 24/23 7 in materia di "whistleblowing"

Il D. Lgs. 10 marzo 2023, n. 24 recepisce nel nostro ordinamento la Direttiva (UE) 2019/1937, riguardante la protezione delle persone che segnalano violazioni di

disposizioni normative nazionali o dell'Unione europea, c.d. Direttiva Whistleblowing, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato. La nuova normativa stabilisce che è legittimo e doveroso segnalare le violazioni di norme europee e nazionali civili, penali e amministrative, procedure e regolamenti aziendali, codici etici, contenute nei Modelli Organizzativi ex D.Lgs. n. 231/2001.

La nuova disciplina, inoltre, estende le misure di protezione, oltre ai segnalanti, anche ai c.d. "facilitatori" (coloro che prestano assistenza al lavoratore nel processo di segnalazione), ai colleghi che hanno una relazione di parentela (entro il 4° grado) ovvero un rapporto corrente e abituale con il segnalante, nonché agli eventuali Enti di proprietà o per cui lavora il segnalante ovvero che operano nel medesimo contesto lavorativo.

Lo scopo della norma è rafforzare le tutela della riservatezza dell'identità del segnalante, per incentivare le segnalazioni e per contrastare l'illegalità nelle aziende pubbliche e private, anche al fine di costruire una cultura della legalità. Il legislatore, a garanzia dei canali di segnalazione interna e della loro corretta applicazione, ha istituito un canale di segnalazione esterna, la cui gestione è demandata all' Autorità Nazionale Anti Corruzione (ANAC), ente preposto, altresì, ad irrogare sanzioni amministrative pecuniarie alle organizzazioni in caso di omessa predisposizione dei canali di segnalazione interna o di procedure per l'effettuazione e la gestione delle segnalazioni.

La normativa si applica alle imprese che hanno impiegato nell'ultimo anno la media di almeno 50 lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato, o aventi un Modello di Organizzazione e Gestione implementato; i possibili segnalatori sono i dipendenti, i collaboratori dell'ente – in qualsiasi forma – i partner e i fornitori.

ADOPERA si è dotata di un canale interno attraverso l'implementazione di una piattaforma informatica seguendo le linee guida ANAC del 16 luglio 2023 adottando e divulgando specifica procedura parte integrante del presente MOG ed individuando come soggetto ricevente la segnalazione l'RPCT che, pertanto, svolge anche la funzione whistleblowing.

Si fa presente che Adopera ha implementato specifiche procedure relative alle necessarie informative all'UFI in materia di antiriciclaggio previste in piano triennale anticorruzione.

9.5 Raccolta e conservazione delle informazioni

Ogni informazione, segnalazione, reportistica previsti nel Modello sono conservati dall'ODV in un apposito archivio informatico e/o cartaceo.

9.6 Formazione

Adopera si impegna a dare ampia divulgazione dei principi contenuti nel MOG del Codice di comportamento e del sistema sanzionatorio/disciplinare, affinché:

- ogni componente del Modello che abbia un impatto sull'operatività di ciascun amministratore o dipendente, sia da questi conosciuta;
- il singolo sia adeguatamente formato in modo tale che sia in condizioni di applicare correttamente le componenti del Modello rilevanti per la sua posizione.

I principi e i contenuti del Modello sono divulgati mediante corsi di formazione a cui è posto l'obbligo di partecipazione. La struttura dei corsi di formazione è definita dall'Organismo di Vigilanza in coordinamento con le funzioni aziendali competenti.

Il MOG e il codice di Comportamento sono a disposizione di ogni dipendente per un eventuale consultazione.

REATI CONTRO LA PA E IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE

1. Rapporti con la Pubblica Amministrazione

Ai fini della presente trattazione con l'espressione "Pubblica Amministrazione" (P.A.) si intende quel complesso di autorità, organi e agenti cui l'ordinamento affida la cura degli interessi pubblici che vengono individuati

- nelle istituzioni pubbliche nazionali; comunitarie e internazionali intese come strutture organizzative aventi il compito di perseguire con strumenti giuridici gli interessi della collettività; tale funzione pubblica qualifica l'attività svolta anche dai membri della Commissione della Comunità europea, del Parlamento europeo, della Corte di Giustizia e della Corte dei Conti della Comunità europea;

- nei pubblici ufficiali che a prescindere da un rapporto di dipendenza dallo Stato o da altro Ente Pubblico esercitano una funzione pubblica legislativa, giudiziaria o amministrativa;

- negli incaricati di pubbliche funzioni o di pubblico servizio che svolgono un'attività riconosciuta come funzionale ad uno specifico interesse pubblico,

caratterizzata quanto al contenuto, dalla mancanza dei poteri autorizzativi e certificativi propri della pubblica funzione, con la quale è solo in rapporto di accessorietà o complementarietà.

Qualora nello svolgimento della propria attività, dovessero sorgere problematiche interpretative sulla qualifica (pubblica o privata) dell'interlocutore, ciascuno dei Destinatari dovrà rivolgersi all'OdV per gli opportuni chiarimenti.

Segue ai successivi paragrafi un elenco esemplificativo di quei soggetti qualificati come "soggetti attivi" nei reati rilevanti ai fini del D.lgs. 231/2001, ovvero di quei soggetti la cui qualifica è necessaria ad integrare fattispecie criminose nello stesso previste.

2. Enti della pubblica amministrazione

Agli effetti della legge penale, viene comunemente considerato come "Ente della pubblica amministrazione" qualsiasi persona giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi.

Sebbene non esista nel codice penale una definizione di pubblica amministrazione, in base a quanto stabilito nella Relazione Ministeriale al codice stesso ed in relazione ai reati in esso previsti, sono ritenuti appartenere alla pubblica amministrazione quegli enti che svolgano "tutte le attività dello Stato e degli altri enti pubblici".

Nel tentativo di formulare una preliminare classificazione di soggetti giuridici appartenenti a tale categoria è possibile richiamare, da ultimo, l'art. 1 comma 2 D.lgs. 165/2001 in tema di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, il quale definisce come amministrazioni pubbliche tutte le amministrazioni dello Stato.

Non tutte le persone fisiche che agiscono nella sfera ed in relazione ai suddetti enti sono soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie criminose ex D.lgs. 231/2001. In particolare le figure che assumono rilevanza a tal fine sono soltanto quelle dei "Pubblici Ufficiali" e degli "Incaricati di Pubblico Servizio".

3. Pubblici Ufficiali

Ai sensi dell'art. 357 primo comma c.p. è considerato pubblico ufficiale "agli effetti della legge penale" colui il quale esercita "una pubblica funzione legislativa, giudiziaria o amministrativa".

Il secondo comma si preoccupa poi di definire la nozione di "pubblica funzione amministrativa". Non si è compiuta invece un'analoga attività definitoria per precisare la nozione di "funzione legislativa" e "funzione giudiziaria" in quanto la individuazione dei soggetti che rispettivamente le esercitano non ha di solito dato luogo a particolari problemi o difficoltà.

Pertanto, il secondo comma dell'articolo in esame precisa che, agli effetti della legge penale "è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi".

In altre parole, è definita pubblica la funzione amministrativa disciplinata da "norme di diritto pubblico", ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Il secondo comma dell'art. 357 c.p. traduce poi in termini normativi alcuni dei principali criteri di massima individuati dalla giurisprudenza e dalla dottrina per differenziare la nozione di "pubblica funzione" da quella di "servizio pubblico".

I caratteri distintivi della prima figura possono essere sintetizzati come segue:

- Pubblico Ufficiale: colui che esercita una pubblica funzione legislativa, giudiziaria o amministrativa.
- Pubblica funzione amministrativa: è disciplinata da norme di diritto pubblico e da atti autoritativi ed è caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi.

4. Incaricati di pubblico servizio

La definizione della categoria di "soggetti incaricati di pubblico servizio" non è allo stato concorde in dottrina così come in giurisprudenza. Volendo meglio puntualizzare tale categoria di "soggetti incaricati di un pubblico servizio", è necessario far riferimento alla definizione fornita dal codice penale e alle interpretazioni emerse a seguito dell'applicazione pratica. In particolare, l'art. 358 c.p. recita che *"sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio"*.

Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima

e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale.

Il "servizio", affinché possa definirsi pubblico, deve essere disciplinato - così come la "pubblica funzione" – da norme di diritto pubblico tuttavia senza poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

La legge inoltre precisa che non può mai costituire "servizio pubblico" lo svolgimento di "semplici mansioni di ordine" né la "prestazione di opera meramente materiale".

La giurisprudenza ha individuato una serie di "indici rivelatori" del carattere pubblicistico dell'ente, per i quali è emblematica la casistica in tema di società per azioni a partecipazione pubblica. In particolare, si fa riferimento ai seguenti indici:

a) la sottoposizione ad un'attività di controllo e di indirizzo a fini sociali, nonché ad un potere di nomina e revoca degli amministratori da parte dello Stato o di altri enti pubblici;
b) la presenza di una convenzione e/o concessione con la pubblica amministrazione;
c) l'apporto finanziario da parte dello Stato;
d) la presenza dell'interesse pubblico in seno all'attività economica.

Sulla base di quando sopra riportato, l'elemento discriminante per indicare se un soggetto rivesta o meno la qualità di "incaricato di un pubblico servizio" è rappresentato, non dalla natura giuridica assunta o detenuta dall'ente, ma dalle funzioni affidate al soggetto le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale.

I caratteri peculiari della figura dell'incaricato di pubblico servizio sono sintetizzabili come segue:

- Incaricati di Pubblico Servizio: coloro che, a qualunque titolo, prestano un pubblico servizio;
- Pubblico servizio: un'attività disciplinata da norme diritto pubblico e caratterizzata dalla mancanza di poteri di natura deliberativa, autorizzativa e certificativa (tipici della Pubblica funzione amministrativa).

Non può mai costituire Pubblico Servizio lo svolgimento di semplici mansioni di ordine né la prestazione di opera meramente materiale.

5. Reati correlati ad erogazioni dello Stato o di altri enti pubblici, richiamati dall'articolo 24 del D.Lgs. 231/2001.

Il Decreto per questi reati prevede le seguenti sanzioni:

Sanzione pecuniaria:
a) fino a 500 quote;
b) da 200 a 600 quote nel caso in cui l'Ente abbia conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità;

Sanzioni interdittive:
a) divieto di contrarre con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio;
b) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
c) divieto di pubblicizzare beni o servizi

5.1 Malversazione a danno dello Stato (art. 316 bis c.p.)

Chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni.
Questo reato presuppone che l'Ente abbia precedentemente conseguito in modo regolare dallo Stato o da altro ente pubblico o dalle Comunità Europee, contributi sovvenzioni o finanziamenti che abbiano una finalità pubblica predefinita (ed espressa nel provvedimento di concessione). Tutte queste erogazioni sono contraddistinte dall'essere concesse a condizioni più favorevoli di quelle di mercato, fino all'assoluta gratuità. In particolare, i contributi sono dei concorsi in spese per attività e iniziative e possono essere in conto capitale (erogazioni a fondo perduto che vengono assegnati a chi si trova in determinate situazioni), e/o in conto interessi (lo Stato o l'Ente pubblico si accolla una parte o la totalità degli interessi dovuti per operazioni di credito). Le sovvenzioni sono attribuzioni pecuniarie a fondo perduto a carattere periodico o una tantum. I finanziamenti sono atti negoziali, con i quali vengono erogate ad un soggetto, a condizioni di favore, somme che devono essere restituite a medio e/o a lungo termine con pagamento degli interessi, in parte o totalmente, ad opera dello Stato o di altro Ente pubblico.

Per l'integrazione del reato è sufficiente che anche solo una parte di quanto conseguito sia stato impiegato per scopi diversi da quelli previsti, non rilevando in alcun modo che l'attività programmata sia stata comunque svolta. Risultano altresì irrilevanti le finalità che l'autore del reato abbia voluto perseguire, poiché l'elemento soggettivo richiesto ad integrare la fattispecie è costituito dalla volontà di sottrarre risorse destinate ad uno scopo prefissato.

Questa fattispecie ha subito alcune modifiche a seguito dell'emanazione del decreto-legge n. 13/2022, recante «Misure urgenti per il contrasto alle frodi e per la sicurezza nei luoghi di lavoro in materia edilizia, nonché sull'elettricità prodotta da impianti da fonti rinnovabili» (c.d. decreto frodi), pubblicato in Gazzetta Ufficiale il giorno 25 febbraio 2022.

In particolare, nella rubrica le parole «a danno dello Stato» sono sostituite dalle seguenti: «di erogazioni pubbliche»; ed è stato esteso l'ambito di applicazione della fattispecie penale a mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, destinati a una o più finalità.

A titolo esemplificativo e non esaustivo, si indicano una o più modalità di realizzazione per tale reato in ADOPERA.:

a seguito dell'ottenimento non fraudolento di una contribuzione pubblica (nazionale o comunitaria) erogata in favore della Società per fini connessi allo svolgimento della propria attività (ad esempio, per la realizzazione e/o l ammodernamento delle infrastrutture), la funzione aziendale preposta alla concreta gestione della suddetta contribuzione (i.e. funzioni competenti in materia di amministrazione, finanza, finanziamenti pubblici) e/o le strutture interessate a fruire dei suddetti finanziamenti omettono, di destinare, anche solo in parte, le somme percepite alle predette finalità.

5.2 Indebita percezione di erogazioni a danno dello Stato (art. 316 ter c.p.)

Salvo che il fatto costituisca il reato previsto dall' articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni. La pena è della reclusione da uno a quattro anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso della sua qualità o dei suoi poteri. La pena è della reclusione da sei mesi a quattro anni se il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000 Quando la somma indebitamente percepita è pari o inferiore a 3.999,96 si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da 5.164,57 a 25.822. Tale sanzione non può comunque superare il triplo del beneficio conseguito.

Questa fattispecie accanto a quella analoga, ma più grave, prevista dall'art. 640 bis c.p. (v. oltre) costituisce uno strumento per colpire le frodi commesse nella fase propedeutica alla concessione delle erogazioni pubbliche.

Lo schema di questo reato prevede che il contributo sia percepito a seguito dell'utilizzo oppure della presentazione di dichiarazioni o di documenti falsi oppure a causa dell'omissione di informazioni dovute.

Rispetto all'ipotesi prevista dall'art. 640 bis c.p. (truffa aggravata per il conseguimento di erogazioni pubbliche) "l'indebita percezione di erogazioni" è svincolata, per la sua consumazione, sia dall'induzione in errore dell'ente erogatore sia dalla causazione di un evento dannoso al medesimo.

Tale fattispecie, accanto a quella analoga, più grave, prevista dall' art. 640 bis c.p. (v. oltre), costituisce uno strumento diretto a colpire le frodi commesse nella fase propedeutica alla concessione delle erogazioni pubbliche.
Essa, nello specifico, si realizza nei casi in cui si ottengano, senza averne il diritto, contributi, finanziamenti, mutui agevolati o altre diverse erogazioni da parte dello Stato, di altri Enti pubblici o dell'UE a seguito dell'utilizzo o della presentazione di dichiarazioni o di documenti falsi, ovvero a causa dell'omissione di informazioni dovute.

Rispetto all' ipotesi prevista dall' art. 640 bis c.p. (truffa aggravata per il conseguimento di erogazioni pubbliche), l'indebita percezione di erogazioni è svincolata, per la sua consumazione, sia dall' induzione in errore dell'Ente erogatore sia dalla causazione di un evento dannoso al medesimo.

Il D.Lgs. 75/2020 ha introdotto un inasprimento di pena (reclusione da sei mesi a quattro anni) qualora il fatto offenda gli interessi finanziari dell'Unione Europea e il danno o il profitto siano superiori ad euro 100.000. Come la fattispecie che precede, anche la norma in oggetto ha subito alcune modifiche a seguito dell'emanazione del decreto-legge n. 13/2022, recante «Misure urgenti per il contrasto alle frodi e per la sicurezza nei luoghi di lavoro in materia edilizia, nonché sull'elettricità prodotta da impianti da fonti rinnovabili» (c.d. decreto frodi), pubblicato in Gazzetta Ufficiale il giorno 25 febbraio 2022.

In particolare, la rubrica è stata sostituita in "Indebita percezione di erogazioni pubbliche" mentre sono state ricomprese nell'ambito della fattispecie anche le "sovvenzioni" (inserite dopo la parola "contributi").

A titolo esemplificativo e non esaustivo, si indicano una o più modalità di realizzazione per tale reato in ADOPERA:

Il personale predispone dichiarazioni fiscali o modelli di versamento incompleti o non veritieri al fine di ottenere un beneficio per la Società, p.e. il pagamento di contributi/imposte inferiori rispetto a quanto effettivamente dovuto.

5.3 Truffa commessa a danno dello Stato o di altro ente pubblico (art. 640 comma 2 n. 1 c.p.)

Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno è punito con la reclusione da sei mesi a tre anni e con la multa da € 51 a € 1.032.

La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro:

1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico (…)

Lo schema di questo reato è quello tradizionale della truffa (induzione in errore del soggetto attraverso una difforme rappresentazione della realtà, con ottenimento di un indebito beneficio e danno altrui) e si caratterizza per il soggetto raggirato: lo Stato o un altro ente pubblico.

Nella fattispecie in esame la truffa si configura come reato istantaneo e di danno, che si perfeziona non con l'azione diretta al profitto ma con la realizzazione di un danno di carattere patrimoniale.

L'attività attraverso cui si concreta il reato di truffa consiste in qualunque comportamento che tragga in errore lo Stato e l'ente pubblico che deve effettuare l'atto di disposizione patrimoniale e può consistere nella produzione di documenti contenenti informazioni o attestazioni false, dissimulanti o che comunque rappresentino la realtà in modo distorto. Il reato viene commesso anche sottacendo informazioni che – se conosciute dal soggetto erogante – avrebbero determinato in senso negativo la sua volontà negoziale.

A titolo esemplificativo e non esaustivo, si indicano una o più modalità di realizzazione per tale reato in ADOPERA: Trasmissione ad un Ente pubblico di documentazione non veritiera o alterata, anche in relazione alla richiesta di informazioni o chiarimenti, al fine di ottenere autorizzazioni o agevolazioni tariffarie.

5.4 Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.)

La pena è della reclusione da uno a sei anni e si procede d'ufficio se il fatto di cui all'art. 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.

Questa fattispecie può ormai qualificarsi come circostanza aggravante della truffa contemplata dall'art. 640 c.p. e si contraddistingue per l'oggetto specifico dell'attività illecita: erogazioni a fondo perduto, cessioni di credito a condizioni vantaggiose per impieghi determinati, mutui agevolati.

La condotta di cui all'art. 640 bis c.p. possiede un "quid pluris" rispetto alla tipicità descritta nell'art. 316 ter c.p. e si realizza allorquando i comportamenti falsi o reticenti, per le concrete modalità realizzative, per il contesto in cui avvengono, e per le circostanze che li accompagnano, sono connotati da una particolare carica di artificiosità e di inganno nei confronti dell'ente erogatore in modo da vanificare o rendere meno agevole l'attività di controllo delle autorità preposte.

La fattispecie si considera compiuta nel momento e nel luogo in cui l'agente consegue la materiale disponibilità dell'erogazione.

L'attività fraudolenta deve sfociare in una serie di eventi: l'induzione di altri in errore, il compimento di un atto di disposizione patrimoniale da parte dell'ingannato, il conseguimento di un ingiusto profitto da parte dell'agente o di un terzo con altrui danno.

Il reato in oggetto, a seguito delle recenti pronunce delle Sezioni Unite della Suprema Corte, può ormai qualificarsi quale circostanza aggravante della truffa contemplata dall'art. 640 c.p., dalla quale si contraddistingue per l'oggetto specifico dell'attività illecita: contributi, finanziamenti, mutui agevolati o altre erogazioni di carattere pubblico.

La condotta di cui all'art. 640 bis c.p. possiede un quid pluris rispetto alla tipicità descritta nell' art. 316 ter c.p.

Il reato, infatti, si realizza allorquando i comportamenti falsi o reticenti, per le concrete modalità realizzative, per il contesto in cui avvengono, nonché per le circostanze che li accompagnano, sono connotati da una particolare carica di artificiosità e di inganno nei confronti dell'Ente erogatore. La fattispecie si considera compiuta nel momento e nel luogo in cui l'agente consegue la materiale disponibilità dell'erogazione.

L'attività fraudolenta deve sfociare in una serie di eventi: l'induzione di altri in errore, il compimento di un atto di disposizione patrimoniale da parte dell'ingannato, il conseguimento di un ingiusto profitto da parte dell'agente o di un terzo con altrui danno.

La norma ha subito alcune modifiche a seguito dell'emanazione del decreto-legge n. 13/2022, recante «Misure urgenti per il contrasto alle frodi e per la sicurezza nei luoghi di lavoro in materia edilizia, nonché sull'elettricità prodotta da impianti da fonti rinnovabili» (c.d. decreto frodi), pubblicato in Gazzetta Ufficiale il giorno 25 febbraio 2022.

In particolare, sono state ricomprese nell'ambito della fattispecie anche le "sovvenzioni" (inserite dopo la parola "contributi").

A titolo esemplificativo e non esaustivo, si indicano una o più modalità di realizzazione per tale reato in ADOPERA:

Il personale, al fine di ottenere un ingiusto profitto per la Società, produce alla PA documenti falsi attestanti l'esistenza di condizioni essenziali per partecipare ad una gara, per ottenere licenze, autorizzazioni, concessioni etc.

5.5 Frode nelle pubbliche forniture (art. 356)

Chiunque commette frode(1)nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo precedente, è punito con la reclusione da uno a cinque anni e con la multa non inferiore a euro 1.032.
La pena è aumentata nei casi preveduti dal primo capoverso dell'articolo precedente.

Quest'ultima figura delittuosa, disciplinata all'art. 356 del Codice penale italiano, può essere commessa da un privato che abbia in essere un rapporto contrattuale con la Pubblica Amministrazione (per questo motivo, si suole parlare di reato proprio).

La norma incriminatrice punisce la commissione di frode nella esecuzione di contratti di fornitura o nell'adempimento degli obblighi contrattuali scaturenti da obbligazioni negoziali conclusi con lo Stato, con altro ente pubblico, ovvero con un'impresa esercente servizi pubblici o di pubblica necessità.

5.6 FRODE INFORMATICA (art. 640 TER)

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno è punito con la reclusione da sei mesi a tre anni e con la multa da 51 a 1.032.

La pena è della reclusione da uno a cinque anni e della multa da 309 a 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'art. 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.
La pena è della reclusione da due a sei anni e della multa da 600 a 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno da uno o più soggetti.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma e terzo comma o taluna delle circostanze previste dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età, e numero 7".

-sanzione pecuniaria: fino a 500 quote; tuttavia, se l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità, si applica la sanzione pecuniaria da 200 a 600 quote; -sanzioni interdittive: divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.

Il reato in oggetto prevede l'ipotesi in cui, mediante l'alterazione di un sistema informatico o telematico, ovvero mediante la manipolazione dei dati in esso contenuti, si ottenga un ingiusto profitto e un corrispondente danno allo Stato o ad altro Ente Pubblico.

L'attività fraudolenta dell'agente investe non la persona, di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la sua manipolazione.

A titolo esemplificativo e non esaustivo, si indicano una o più modalità di realizzazione per tale reato in ADOPERA: Il personale al fine di procurare un ingiusto profitto alla Società, altera o manipola il funzionamento di un sistema informatico o telematico, arrecando in tal modo un danno allo Stato o altro Ente pubblico.

6. Reati configurabili nei rapporti con la P.A. o con incaricati di Pubblico servizio, richiamati dall'articolo 25 del D.Lgs. 231/2001.

Le sanzioni previste dal Decreto per questa categoria di reati sono:

Sanzione pecuniaria;
a) fino a 200 quote (nei casi di cui agli artt. 318, 321 e 322 commi 1 e 3 c.p.);
b) da 200 a 600 quote (nei casi di cui agli artt. 319, 319 ter comma 1, 321 e 322 commi 2 e 4 c.p.);
c) da 300 a 800 quote (nei casi di cui agli artt. 317, 319 aggravato, 319 ter comma 2 e 321 c.p.);

Sanzioni interdittive:
Sono escluse solo per i casi di cui agli artt. 318, 321 e 322 commi 1 e 3.

Negli altri casi esse avranno durata non inferiore a 1 anno e sono:

a) interdizione dall'esercizio dell'attività;
b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c) divieto di contrarre con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio;
d) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
e) divieto di pubblicizzare beni o servizi.

Tuttavia, se prima della sentenza di primo grado l'ente si è efficacemente adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l'individuazione dei responsabili ovvero per il sequestro delle somme o altre utilità trasferite e ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi, le sanzioni interdittive hanno la durata stabilita dall'articolo 13, comma 2 del D.lgs. 231/2001 (durata non inferiore a 3 mesi e non superiore a 2 anni).

6.1 Concussione (art. 317 c.p.)

Il Pubblico Ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei a dodici anni.

Sanzioni applicabili all'ente:
-sanzione pecuniaria: da 300 a 800 quote;
-sanzioni interdittive: interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi. A seguito delle modifiche apportate della legge 9 gennaio 2019, n. 3 le sanzioni interdittive di cui all'art. 9 c. 2 sono applicate per una durata non inferiore a quattro e non superiore a sette anni, se il reato è stato commesso dai soggetti di cui all'art. 5 c. 1 lett. a) – ovverosia, da coloro i quali rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano di fatto le gestione e il controllo dell'ente – e per una durata non inferiore a due e non superiore a quattro anni, se il reato è stato commesso da soggetti di cui all'art. 5 c. 1 lett. b) – ovverosia, da coloro i quali sono sottoposti alla direzione o alla vigilanza dei soggetti di cui alla precedente lettera a).Tuttavia, la novella del 2019 ha introdotto altresì il comma 5 bis, il quale dispone che le sanzioni interdittive vengono inflitte nella comune durata prevista dall'art. 13 c. 2 (termine non inferiore a tre mesi né superiore ai due anni) nel caso in cui, prima della sentenza di primo grado, l'ente si sia efficacemente adoperato:

a) b) c) per evitare che l'attività delittuosa venga portata a conseguenze ulteriori; per assicurare la prova dei reati; per l'individuazione dei responsabili; d) per assicurare il sequestro delle somme o altre utilità trasferite;

ovvero

e) abbia eliminato le carenze organizzative che hanno reso possibile la verificazione del reato mediante l'adozione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi.

Tale fattispecie di reato si differenzia dalla corruzione in quanto non si è in presenza di un accordo tra il privato e il Pubblico Ufficiale bensì quest'ultimo, abusando dei propri poteri o della propria qualità, costringe il privato a procurare a sé o ad altri denaro o altra utilità. In altri termini, il Pubblico Ufficiale determina uno stato di soggezione della volontà della persona offesa mediante l'abuso della sua qualità (indipendentemente dalle sue competenze specifiche ma strumentalizzando la sua posizione di preminenza) o dei suoi poteri (condotte che rappresentano manifestazioni delle sue potestà funzionali per scopi diversi da

quello di cui è stato investito). Soggetti passivi di questo reato sono, al contempo, la Pubblica Amministrazione e il privato concusso.

A titolo esemplificativo e non esaustivo, si indicano una o più modalità di realizzazione per tale reato in ADOPERA: Il personale della Società, che nelle sue mansioni di pubblico ufficiale, approfittando di tale qualifica, richieda a soggetti terzi prestazioni non dovute a vantaggio o nell'interesse della azienda.

6.2 Corruzione per un atto d'ufficio (art. 318 c.p.)

Il pubblico ufficiale, che, per compiere un atto del suo ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa, è punito con la reclusione da sei mesi a otto anni.

Il reato in esame può essere commesso, oltre che dal pubblico ufficiale, anche dall'incaricato di un pubblico servizio "qualora rivesta la qualità di pubblico impiegato" (art. 320 c.p.).

Rispetto alla concussione, la corruzione sia propria (art. 319 c.p.) che impropria (art. 318 c.p.) si caratterizza per l'accordo illecito raggiunto tra i diversi soggetti.

Questa fattispecie si caratterizza per il rapporto paritetico che intercorre tra il soggetto pubblico e il privato corruttore. Nell'ipotesi ora esaminata (corruzione impropria), il pubblico ufficiale o l'incaricato di un pubblico servizio si accorda con il privato per compiere un atto comunque del suo ufficio. Tale deve intendersi qualunque atto che costituisca concreto esercizio di poteri inerenti all'ufficio di appartenenza del funzionario.

La differenza tra questa ipotesi di corruzione (impropria) e quella successiva "per atto contrario ai doveri d'ufficio" di cui all'art. 319 c.p. (propria) si ravvisa nel fatto che - nel primo caso - a seguito dell'accordo con il privatosi realizza da parte del pubblico ufficiale una violazione del principio di correttezza e di imparzialità, senza tuttavia che la parzialità si trasferisca nell'atto. Nel secondo caso, la parzialità colpisce l'atto che non realizza la finalità pubblica ad esso sottesa e viene compiuto ad uso privato.

Secondo la giurisprudenza più recente, la mancata individuazione dell'atto dell'ufficio che il pubblico ufficiale ha compiuto, non fa venir meno il delitto in esame ove, comunque, venga accertato che la consegna del denaro venne effettuata in ragione delle funzioni esercitate dal pubblico ufficiale e per retribuirne i favori.

E' prevista la sanzione pecuniaria fino a 200 quote.

A titolo esemplificativo e non esaustivo, si indicano una o più modalità di realizzazione per tale reato in ADOPERA:
il personale offre regalie a Pubblici Ufficiali ovvero a Incaricati di Pubblico Servizio al fine di condizionarne in senso favorevole l'operato, ad esempio in occasione di un procedimento volto alla verifica dell'ottemperanza alle prescrizioni imposte o di un accertamento ispettivo, effettuati da parte degli enti preposti (es. ASL, INAIL, ecc.).

6.3 Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)

Il pubblico ufficiale, che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da sei a dieci anni.
Il privato corruttore nella corruzione "propria" si assicura con la promessa o la dazione indebita un atto del pubblico ufficiale che contrasta con i doveri del suo ufficio.

Per stabilire se un atto sia contrario o meno ai doveri d'ufficio occorre avere riguardo non soltanto all'atto in sé per verificarne la legittimità o l'illegittimità, ma anche alla sua conformità a tutti i doveri d'ufficio o di servizio che possono venire in considerazione, con il risultato che un atto può essere in sè stesso non illegittimo e ciò nondimeno essere contrario ai doveri d'ufficio. La verifica deve essere fatta non in relazione a singoli atti, ma tenendo presente l'insieme del servizio reso al privato.

A titolo esemplificativo e non esaustivo, si indicano una o più modalità di realizzazione per tale reato in ADOPERA:
il personale della Società offre denaro ad un esponente di un organismo di certificazione di natura pubblica che, agendo in violazione degli obblighi inerenti al proprio ufficio, in sede di rilascio o rinnovo della certificazione, ovvero in sede di verifica, attesta falsamente il rispetto delle norme di riferimento.

6.4 Corruzione in atti giudiziari (art. 319 ter c.p.)

Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da sei a dodici anni.

Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da quattro a dodici anni; se deriva l'ingiusta

condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da sei a venti anni.

Tale ipotesi di reato si configura nel caso in cui l'Ente sia parte di un procedimento giudiziario e corrompa un pubblico ufficiale (magistrato, cancelliere, altro funzionario pubblico) al fine di ottenere un vantaggio nel procedimento stesso.

6.5 Traffico di influenze illecite (art. 346 bis c.p.)

Chiunque, fuori dei casi di concorso nei reati di cui agli articoli 318, 319, 319-ter e nei reati di corruzione di cui all'articolo 322-bis, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri, è punito con la pena della reclusione da un anno a quattro anni e sei mesi.

Si applica la sanzione pecuniaria sino a 200 quote.

La fattispecie in esame incrimina, in un'ottica di anticipazione della tutela, condotte strumentali alla realizzazione di futuri accordi illeciti, punendo in particolare chi, sfruttando relazioni esistenti con un pubblico ufficiale o incaricato di pubblico servizio, fa dare o promettere a sé o ad altri, indebitamente, denaro o altra utilità come prezzo della propria mediazione (a vantaggio dunque del mediatore) o, in alternativa, quale remunerazione destinata al pubblico ufficiale.

Il delitto punisce sia l'intermediario dell'accordo corruttivo sia il corruttore con la previsione della medesima pena. Nel caso in cui la mediazione andasse a buon fine – il trafficante di adopera effettivamente presso il pubblico funzionario e questi accetta la promessa o la dazione di denaro – si realizzerà, invece, un concorso trilaterale nel più grave reato di corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione propria (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.) ovvero contro la P.A. comunitaria ed internazionale (art. 322-bis c.p.) con assorbimento del disvalore del fatto ed esclusione della punibilità del reato di minore gravità di cui all'art. 346-bis c.p..

6.6 Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorita' giudiziaria (art. 377 bis c.p.)

Salvo che il fatto costituisca più grave reato, chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale,

quando questa ha la facoltà di non rispondere, è punito con la reclusione da due a sei anni.

Si tratta di un delitto contro l'attività giudiziaria introdotto nel Decreto Il presente articolo è stato inserito dall'articolo 4 comma 1 della legge 3 agosto 2009 n. 116 come articolo 25-novies, non tenendo conto dell'inserimento di tale articolo 25-novies da parte dell'articolo 15 comma 7 lettera c) della legge 23 luglio 2009 n. 99.

Per ragioni di organicità viene inserito in questa parte speciale del MOG.

Destinatario della condotta può essere solo chi ha facoltà di non rispondere in un processo penale, ossia l'indagato o l'imputato (anche in relazione a procedimenti connessi).

Si applica la sanzione pecuniaria fino a 500 quote.

A titolo esemplificativo e non esaustivo, si indicano una o più modalità di realizzazione per tale reato in ADOPERA:

il personale, agendo per la realizzazione di un interesse della Società, dà o promette denaro o altra utilità indebita al Pubblico Ufficiale o all'Incaricato di Pubblico Servizio il quale, abusando del proprio ufficio, compie un atto vantaggioso per la Società, ad es. omettendo di dichiarare l'assenza di adeguati DPI.

6.7 Istigazione alla corruzione (art. 322 c.p.)

Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio che riveste la qualità di pubblico impiegato, per indurlo a compiere un atto del suo ufficio, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel comma 1 dell'articolo 318, ridotta di un terzo.

Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo.

La pena di cui al comma primo si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che riveste la qualità di pubblico impiegato che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 318.

La pena di cui al comma secondo si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319.

Il reato si configura con la semplice promessa di denaro o altra utilità, purché essa sia finalizzata ad indurre il destinatario (pubblico ufficiale o incaricato di un pubblico servizio) a compiere un atto del suo ufficio e quest'ultimo la rifiuti.

Nel reato di istigazione alla cd. *corruzione impropria* (comma 3) si prevede che l'offerta di denaro o altra utilità sia sollecitata dallo stesso pubblico ufficiale o incaricato di pubblico servizio per il compimento di un atto conforme ai propri doveri.

6.8 induzione indebita a dare o promettere utilità (art. 319 quater c.p.)

Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei anni a dieci anni e sei mesi.

Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni.

Tale ipotesi di reato si configura nel caso in cui, un pubblico ufficiale o 'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induce qualcuno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità punendo, altresì, la condotta di chi dà o promette denaro o altra utilità (al pubblico ufficiale o all'incaricato di pubblico servizio).

E' prevista una sanzione pecuniaria da 300 a 800 quote.

6.9 Turbata libertà degli incanti (art. 353 c.p.)

Chiunque con violenza o minaccia o con doni promesse collusioni o altri mezzi fraudolenti impedisce o turba la gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche amministrazioni ovvero ne allontana gli offerenti è punito con la reclusione da sei mesi a cinque anni e con la multa da euro 103 a euro 1.032. Se il colpevole è persona preposta dalla legge o dall'autorità agli incanti o alle licitazioni suddette la reclusione è da uno a cinque anni e la multa da euro 516 a euro 2.065. Le pene stabilite in questo articolo si applicano anche nel caso di licitazioni private per conto di privati dirette da un pubblico ufficiale o da persona legalmente autorizzata ma sono ridotte alla metà.

E' prevista una sanzione pecuniaria sino a 500 quote o in casi più gravi da 200 a 600 quote.

6.10 Turbata libertà del procedimento di scelta del contraente (art. 353-bis)

Salvo che il fatto costituisca più grave reato chiunque con violenza o minaccia o con doni promesse collusioni o altri mezzi fraudolenti turba il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione è punito con la reclusione da sei mesi a cinque anni e con la multa da euro 103 a euro 1.032.

E' prevista una sanzione pecuniaria sino a 500 quote o in casi più gravi da 200 a 600 quote.

7 Reati corruttivi in ambito societario

Nel presente capitolo si sono voluti affrontare anche i reati corruttivi in materia societaria.

In relazione ai reati in materia societaria, previsti dal codice civile ed elencati nell'articolo 25-ter del Decreto, la Società è soggetta alle sanzioni amministrative indicate quando tali reati sono commessi nell'interesse della Società stessa da amministratori o da persone sottoposte alla loro vigilanza, qualora il fatto non si fosse realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica.

Per i reati in oggetto, il Decreto non prevede sanzioni interdittive o sanzioni accessorie mentre sarà applicabile la confisca del prezzo o del profitto del reato ai sensi dell'art. 19 del Decreto.

Le fattispecie di rilevanza penale in materia societaria disciplinate dal codice civile possono classificarsi come segue:

1) Falsità;
2) tutela del capitale sociale;
3) tutela del corretto funzionamento della Società;
4) tutela contro le frodi.

Nel presente MOG sono valutati esclusivamente i rischi legati ai seguenti reati presupposto.

7.1 Corruzione fra i privati (art. 2635 c.c. terzo comma)

Ai fini della responsabilità amministrativa ex D. Lgs. 231/01, nell'ipotesi di "corruzione tra privati" disciplinata dall'art. 2635 c.c. terzo comma rilevano comportamenti corruttivi di tipo "attivo".

Tali comportamenti sono riconducibili a casi in cui un soggetto, agendo nell'interesse o a vantaggio dell'Ente presso cui opera, realizzi condotte corruttive "tra privati" attraverso la dazione o la promessa di denaro o altra utilità ad "amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e i liquidatori" o a persone sottoposte alla direzione o alla vigilanza di tali soggetti, creando un danno alla società cui appartiene il soggetto corrotto.

Il Decreto per questi reati prevede la sanzione pecuniaria: da 400 a 600 quote con applicazione di sanzioni interdittive.

7.2 Istigazione alla corruzione fra i privati (art. 2635 – bis c.c. primo comma)

Ai fini della responsabilità amministrativa ex D. Lgs. 231/01, nell'ipotesi di "istigazione alla corruzione tra privati" disciplinata dall'art. 2635 bis c.c. primo comma rilevano comportamenti corruttivi di tipo "attivo" e "passivo".

Tali comportamenti sono riconducibili a casi in cui un soggetto, agendo nell'interesse o a vantaggio dell'Ente presso cui opera, realizzi condotte di sollecitazione od offerta quando queste non vengono accettate.

Il Decreto per questi reati prevede la sanzione pecuniaria: da 200 a 400 quote con applicazione delle sanzioni interdittive.

8. Identificazione delle attività sensibili

Le attività sensibili che Adopera ha individuato al proprio interno sono le seguenti:

1) Negoziazione, stipula e/o esecuzione di contratti con la P.A.;
2) Ottenimento e rinnovo di convenzioni e/o concessioni con la P.A.;
3) Rapporti con la P.A. per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali;
4) Rapporti con la P.A. in qualità di socio di Adopera;
5) Gestione degli adempimenti in materia ambientale e dei rapporti con enti pubblici o incaricati di pubblico servizio nell'ambito del diritto ambientale;
6) Gestione delle verifiche ispettive da parte di enti pubblici o incaricati di pubblico servizio (es. AUSL, Guardia di Finanza, NOE, Polizia Locale, Vigili del Fuoco, ecc.);
7) Gestione delle attività di acquisizione e/o gestione di contributi, sovvenzioni, gare, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici;
8) Gestione delle procedure di appalto;

9) Gestione di eventuali contenziosi giudiziali e stragiudiziali.

Con particolare riferimento alla corruzione in materia di reati presupposto societari:

1) redazione del bilancio, dei prospetti informativi e delle relazioni infra-annuali;
2) operazioni sul capitale e destinazione dell'utile;
3) gestione dei rapporti con i soci.

Oltre alle attività che determinano momenti di contatto con la P.A. in cui potrebbero verificarsi alcuni reati previsti dal Decreto, il MOG prevede specifiche attività di controllo per i processi cosiddetti "strumentali". Si tratta di attività attraverso le quali si potrebbero creare le condizioni necessarie alla commissione dei reati contro la P.A. (basti pensare ad esempio ad assunzioni di personale, parenti o funzionari della P.A. al fine di ottenere un favore illecito).

Sono considerati processi strumentali:

10) gestione dei pagamenti;
11) conferimento di incarichi di consulenza e prestazioni professionali;
12) spese di rappresentanza, gli omaggi e sponsorizzazioni;
13) selezione e assunzione del personale;
14) retribuzioni e rimborsi spese al personale.

9. Valutazione del rischio e matrice-reati

La valutazione del rischio di commissione di tale fattispecie criminosa in Adopera viene espressa attraverso il criterio già descritto al punto 3 del presente MOG.
Di seguito si riporta, quindi, la matrice di reato con individuato il rischio emerso attraverso il calcolo di P x D di cui al punto 3 del presente MOG e con specifica dei protocolli e/o procedure tali da rendere il rischio detto, ove ritenuto presente, come accettabile (intendendosi "accettabile" il rischio della commissione dei reati presupposto considerati esclusivamente attraverso l'elusione intenzionale e fraudolenta delle procedure e/o protocolli previste/i).

REATO	CONDOTTA	ATTIVITA' SENSIBILI	FUNZIONI E RISORSE UMANE COINVOLTE	QUOTE	R	PROTOCOLLI SPECIFICI	RR
Art. 321 c.p. - rif. 318 c.p. (Corruzione per un atto d'ufficio) -319 c.p (Corruzione per un atto contrario ai doveri d'ufficio).Art. 322 c.p. (Istigazione alla corruzione).	ottenere dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, e non destinarli alle predette finalità	1) Ottenimento e rinnovo di convenzioni e/o concessioni con la Pubblica Amministrazione, rapporti con le partecipate comunali; 2) Rapporti con la P.A. per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali; 3) Gestione delle verifiche ispettive da parte di enti pubblici o incaricati di pubblico servizio (es. ASL, Guardia di Finanza, NAS, Polizia Locale, Vigili del Fuoco, dogane, ecc.); 4) Gestione di eventuali contenziosi giudiziali e stragiudiziali; 5) gestione dei pagamenti 6) conferimento di incarichi di consulenza, prestazioni professionali e di servizi in genere; 7) spese di rappresentanza, gli omaggi e sponsorizzazioni; 8) selezione e assunzione del personale; 9) retribuzioni e rimborsi spese al personale; 10) gare.	Amministratore Unico, Ufficio Amministrativo, RPCT	fino 600 + interdittive		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	
Art. 316 bis (malversazione ai danni dello stato)	Tale ipotesi di reato si configura nei confronti di chiunque, estraneo alla Pubblica Amministrazione, avendo ottenuto dallo Stato, da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico inte-resse, non li destina alle predette finalità (la condotta, infatti, consiste nell'avere distratto, anche parzialmen-te, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta).	Accesso a finanziamenti, commesse da parte della PA, partecipazione gare	Amministratore Unico, Ufficio Amministrativo, RPCT	da 100 a 600 quote + interdittive		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	

Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico o delle Comunità europee (art. 316-ter c.p.)	conseguire indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute	Gestione dei rapporti con l'Agenzia delle Entrate e la Guardia di Finanza e/o di altro ente in occasione di visite ispettive, area gare	Amministratore Unico, Ufficio Amministrativo, RPCT	fino 600 + interdittive		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	
Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art. 640, comma 2, n. 1, c.p.)	indurre in errore con artifici e raggiri procurando a sé o ad altri un ingiusto profitto a danno dello Stato o di un altro ente pubblico	Gestione dei rapporti con l'Agenzia delle Entrate e la Guardia di Finanza e/o di altro ente in occasione di visite ispettive, area gare	Amministratore Unico, Ufficio Amministrativo, RPCT	fino 600 + interdittive		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	
Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)	indurre in errore con artifici e raggiri procurando a sé o ad altri un ingiusto profitto a danno dello Stato o di un altro ente pubblico se il fatto riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee	Gestione dei rapporti con l'Agenzia delle Entrate e la Guardia di Finanza e/o di altro ente in occasione di visite ispettive, area gare	Amministratore Unico, Ufficio Amministrativo, RPCT	fino 600 + interdittive		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	
Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)	procurare a sé o ad altri un ingiusto profitto a danno dello Stato, di altri enti pubblici o Comunità Europee, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti	fatturazione elettronica	Amministratore Unico, Ufficio Amministrativo, RPCT	fino 600 + interdittive		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	

Corruzione per un atto d'ufficio (art. 318 c.p.)	ricevere in qualità di pubblico ufficiale o pubblico impiegato, per sé o per un terzo, in denaro od altra utilità, una retribuzione non dovuta o accettarne la promessa, per compiere un atto del proprio ufficio	1) Ottenimento e rinnovo di convenzioni e/o concessioni con la Pubblica Amministrazione, rapporti con le partecipate comunali; 2) Rapporti con la P.A. per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali; 3) Gestione delle verifiche ispettive da parte di enti pubblici o incaricati di pubblico servizio (es. ASL, Guardia di Finanza, NAS, Polizia Locale, Vigili del Fuoco, dogane, ecc.); 4) Gestione di eventuali contenziosi giudiziali e stragiudiziali; 5) gestione dei pagamenti 6) conferimento di incarichi di consulenza, prestazioni professionali e di servizi in genere; 7) spese di rappresentanza, gli omaggi e sponsorizzazioni; 8) selezione e assunzione del personale; 9) retribuzioni e rimborsi spese al personale; 10) gare.	Amministratore Unico, Ufficio Amministrativo, RPCT, revisore unico	fino 200		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	
Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.)	ricevere in qualità di pubblico ufficiale o incaricato di pubblico servizio, per sé o per un terzo, in denaro od altra utilità, una retribuzione non dovuta o accettarne la promessa per omettere o ritardare o per aver omesso o ritardato un atto del proprio ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio	Relativamente a tale tipo di attività i reati di corruzione potrebbero verificarsi nell'interesse e a vantaggio della società mediante l'offerta o la promessa di denaro o altra utilità (es. assunzione di una persona su segnalazione del funzionario) a pubblici ufficiali o incaricati di pubblico servizio al fine di indurli ad avvantaggiare la società o danneggiare un'eventuale controparte nel processo in cui la società è parte	Amministratore Unico, Ufficio Amministrativo, RPCT	fino 600 + interdittive		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	

Pene per il corruttore (art. 321 c.p.) n.b. si vedano le corrispondenti righe relative a corruzione per un atto d'ufficio e corruzione per un atto contrario ai doveri d'ufficio e corruzione per atto di ufficio.	dare o promettere al pubblico ufficiale o all'incaricato di un pubblico servizio denaro od altra utilità	1) Ottenimento e rinnovo di convenzioni e/o concessioni con la Pubblica Amministrazione, rapporti con le partecipate comunali; 2) Rapporti con la P.A. per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali; 3) Gestione delle verifiche ispettive da parte di enti pubblici o incaricati di pubblico servizio (es. ASL, Guardia di Finanza, NAS, Polizia Locale, Vigili del Fuoco, dogane, ecc.); 4) Gestione di eventuali contenziosi giudiziali e stragiudiziali; 5) gestione dei pagamenti 6) conferimento di incarichi di consulenza, prestazioni professionali e di servizi in genere; 7) spese di rappresentanza, gli omaggi e sponsorizzazioni; 8) selezione e assunzione del personale; 9) retribuzioni e rimborsi spese al personale; 10) gare.	Amministratore Unico, Ufficio Amministrativo, RPCT	fino 600 + interdittive		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	

Circostanze aggravanti (art. 319-bis c.p.)	se la corruzione ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene nonché il pagamento o il rimborso di tributi	1) Ottenimento e rinnovo di convenzioni e/o concessioni con la Pubblica Amministrazione, rapporti con le partecipate comunali; 2) Rapporti con la P.A. per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali; 3) Gestione delle verifiche ispettive da parte di enti pubblici o incaricati di pubblico servizio (es. ASL, Guardia di Finanza, NAS, Polizia Locale, Vigili del Fuoco, dogane, ecc.); 4) Gestione di eventuali contenziosi giudiziali e stragiudiziali; 5) gestione dei pagamenti 6) conferimento di incarichi di consulenza, prestazioni professionali e di servizi in genere; 7) spese di rappresentanza, gli omaggi e sponsorizzazioni; 8) selezione e assunzione del personale; 9) retribuzioni e rimborsi spese al personale; 10) gare.	Amministratore Unico, Ufficio Amministrativo, RPCT	fino 600 + interdittive		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	
Corruzione in atti giudiziari (art. 319-ter c.p.)	corruzione per favorire o danneggiare una parte in un processo civile, penale o amministrativo	Gestione di eventuali contenziosi giudiziali e stragiudiziali	Amministratore Unico, Ufficio Amministrativo, RPCT	fino 800 + interdittive		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	

Istigazione alla corruzione (art. 322 c.p.)	offrire o promettere denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio che riveste la qualità di pubblico impiegato, qualora l'offerta o la promessa non sia accettata	1) Ottenimento e rinnovo di convenzioni e/o concessioni con la Pubblica Amministrazione, rapporti con le partecipate comunali; 2) Rapporti con la P.A. per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali; 3) Gestione delle verifiche ispettive da parte di enti pubblici o incaricati di pubblico servizio (es. ASL, Guardia di Finanza, NAS, Polizia Locale, Vigili del Fuoco, dogane, ecc.); 4) Gestione di eventuali contenziosi giudiziali e stragiudiziali; 5) gestione dei pagamenti 6) conferimento di incarichi di consulenza, prestazioni professionali e di servizi in genere; 7) spese di rappresentanza, gli omaggi e sponsorizzazioni; 8) selezione e assunzione del personale; 9) retribuzioni e rimborsi spese al personale; 10) gare.	Amministratore Unico, Ufficio Amministrativo, RPCT	fino 600 + interdittive		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	

Concussione (art. 317 c.p.)	abusare della qualità o dei poteri di pubblico ufficiale o incaricato di pubblico servizio, costringendo o inducendo taluno a dare o a promettere indebitamente, a sè o ad un terzo, denaro od altra utilità	1) Ottenimento e rinnovo di convenzioni e/o concessioni con la Pubblica Amministrazione, rapporti con le partecipate comunali; 2) Rapporti con la P.A. per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali; 3) Gestione delle verifiche ispettive da parte di enti pubblici o incaricati di pubblico servizio (es. ASL, Guardia di Finanza, NAS, Polizia Locale, Vigili del Fuoco, dogane, ecc.); 4) Gestione di eventuali contenziosi giudiziali e stragiudiziali; 5) gestione dei pagamenti 6) conferimento di incarichi di consulenza, prestazioni professionali e di servizi in genere; 7) spese di rappresentanza, gli omaggi e sponsorizzazioni; 8) selezione e assunzione del personale; 9) retribuzioni e rimborsi spese al personale; 10) gare.	Amministratore Unico, Ufficio Amministrativo, RPCT	300-800 + interdittive		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)	con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, indurre a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere	1) Ottenimento e rinnovo di convenzioni e/o concessioni con la Pubblica Amministrazione, rapporti con le partecipate comunali; 2) Rapporti con la P.A. per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali; 3) Gestione delle verifiche ispettive da parte di enti pubblici o incaricati di pubblico servizio (es. ASL, Guardia di Finanza, NAS, Polizia Locale, Vigili del Fuoco, dogane, ecc.); 4) Gestione di eventuali contenziosi giudiziali e stragiudiziali; 5) gestione dei pagamenti 6) conferimento di incarichi di consulenza, prestazioni professionali e di servizi in genere; 7) spese di rappresentanza, gli omaggi e sponsorizzazioni; 8) selezione e assunzione del personale; 9) retribuzioni e rimborsi spese al personale; 10) gare.	Amministratore Unico, Ufficio Amministrativo, RPCT	fino 500		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	

induzione indebita a dare o promettere utilità (art. 319 quater c.p.)	un pubblico ufficiale o 'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induce qualcuno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità punendo, altresì, la condotta di chi dà o promette denaro o altra utilità	1) Ottenimento e rinnovo di convenzioni e/o concessioni con la Pubblica Amministrazione, rapporti con le partecipate comunali; 2) Rapporti con la P.A. per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali; 3) Gestione delle verifiche ispettive da parte di enti pubblici o incaricati di pubblico servizio (es. ASL, Guardia di Finanza, NAS, Polizia Locale, Vigili del Fuoco, dogane, ecc.); 4) Gestione di eventuali contenziosi giudiziali e stragiudiziali; 5) gestione dei pagamenti 6) conferimento di incarichi di consulenza, prestazioni professionali e di servizi in genere; 7) spese di rappresentanza, gli omaggi e sponsorizzazioni; 8) selezione e assunzione del personale; 9) retribuzioni e rimborsi spese al personale; 10) gare.	Amministratore Unico, Ufficio Amministrativo, RPCT	300-800		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione	

corruzione fra privati (art. 2635 c.c.)	un soggetto, agendo nell'interesse o a vantaggio dell'Ente presso cui opera, realizzi condotte corruttive "tra privati" attraverso la dazione o la promessa di denaro o altra utilità ad "amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e i liquidatori" o a persone sottoposte alla direzione o alla vigilanza di tali soggetti	1) Gestione di eventuali contenziosi giudiziali e stragiudiziali; 2) gestione dei pagamenti; 3) conferimento di incarichi di consulenza e prestazioni professionali; 4) spese di rappresentanza, gli omaggi e sponsorizzazioni; 5) selezione e assunzione del personale; 6) retribuzioni e rimborsi spese al personale;	Amministratore Unico, amministrazione, commerciale, ufficio acquisti e ufficio personale, direttori tecnici	400-600		Piano dei conti - Controllo preventivo della bozza di bilancio da parte dell'Amministratore - Tracciabilità e protezione del sistema informatico e manuale, prcedure contabili aziendali, protocollo redazione ed approvazione del bilancio, ISO 9001, codice etico, mansionari, procure/deleghe/nomine/autorizzazioni (es. di spesa), protocollo sponsorizzazioni ed elargizioni, protocollo assegnazione incarichi professionali, protocollo procedimenti giudiziari e arbitrali, piano triennale anticorruzione	
istigazione alla corruzione fra privati (art. 2635 bis cc)	un soggetto, agendo nell'interesse o a vantaggio dell'Ente presso cui opera, realizzi condotte di sollecitazione od offerta quando queste non vengono accettate	1) Gestione di eventuali contenziosi giudiziali e stragiudiziali; 2) gestione dei pagamenti; 3) conferimento di incarichi di consulenza e prestazioni professionali; 4) spese di rappresentanza, gli omaggi e sponsorizzazioni; 5) selezione e assunzione del personale; 6) retribuzioni e rimborsi spese al personale;	Amministratore Unico, amministrazione, commerciale, ufficio acquisti e ufficio personale, direttori tecnici	200-400		Piano dei conti - Controllo preventivo della bozza di bilancio da parte dell'Amministratore - Tracciabilità e protezione del sistema informatico e manuale, prcedure contabili aziendali, protocollo redazione ed approvazione del bilancio, ISO 9001, codice etico, mansionari, procure/deleghe/nomine/autorizzazioni (es. di spesa), protocollo sponsorizzazioni ed elargizioni, protocollo assegnazione incarichi professionali, protocollo procedimenti giudiziari e arbitrali, piano triennale anticorruzione	

Art. 316 bis (malversazione ai danni dello stato)	Tale ipotesi di reato si configura nei confronti di chiunque, estraneo alla Pubblica Amministrazione, avendo ottenuto dallo Stato, da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico inte-resse, non li destina alle predette finalità (la condotta, infatti, consiste nell'avere distratto, anche parzialmen-te, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta).	Accesso a finanziamenti (es. INAIL), commesse da parte della PA, partecipazione gare.	Amministratore Unico, amministrazione, commerciale, Ufficio acqusiti, Ufficio de personale, Direttori Tecnici	da 100 a 600 quote + interdittive		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amministrazione, assunzione personale, protocollo procedimenti arbitrali e giudiziali, protocollo regali omaggi e sponsorizzazioni, procedure anticorruzione, piano triennale anticorruzione	
art 356 cp Frode nelle pubbliche forniture	Chiunque commette frode nell'esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo precedente, è punito con la reclusione da uno a cinque anni e con la multa non inferiore a euro 1.032. La pena è aumentata nei casi preveduti dal primo capoverso dell'articolo precedente	eventuali contratti con la pubblica amministrazione e conseguente consegna di beni del tutto difformi da quanto contrattualmente previsto; gestione dei rifiuti in forza di contratti con la PA	Amministratore Unico, amministrazione, commerciale, Ufficio acqusiti, Ufficio de personale, Direttori Tecnici	600		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amministrazione, assunzione personale, protocollo procedimenti arbitrali e giudiziali, protocollo regali omaggi e sponsorizzazioni, procedure anticorruzione, piano triennale anticorruzione	

traffico di influenze illecite art. 346 bis	Chiunque sfruttando relazioni esistenti con un pubblico ufficiale o con incaricato di pubblico servizio indebitamnte fa dare o promettere a sé e ad altri denaro o altro vantaggio patrimoniale come prezzo per la mediazione illecita…	1) Ottenimento e rinnovo di convenzioni e/o concessioni con la Pubblica Amministrazione ; 2) Rapporti con la P.A. per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali (es. iscrizione Albo Gestori rifiuti); 3) Gestione delle verifiche ispettive da parte di enti pubblici o incaricati di pubblico servizio (es. ASL, Guardia di Finanza, NAS, NOE, Polizia Locale, Vigili del Fuoco, ecc.); 4) Gestione di eventuali contenziosi giudiziali e stragiudiziali; 5) gestione dei pagamenti 6) conferimento di incarichi di consulenza e prestazioni professionali; 7) spese di rappresentanza, gli omaggi e sponsorizzazioni; 8) selezione e assunzione del personale; 9) retribuzioni e rimborsi spese al personale;	Amministratore Unico, amministrazione, commerciale, ufficio acquisti, ufficio personale direttori tecnici	200-800		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amminitrazione, procedure anticorruzione, piano triennale anticorruzione, protocollo regalie omaggi e sponsorizzazioni	A

turbata libertà degli incanti art 353 c.p.	Chiunque con violenza o minaccia o con doni promesse collusioni o altri mezzi fraudolenti impedisce o turba la gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche amministrazioni ovvero ne allontana gli offerenti è punito con la reclusione da sei mesi a cinque anni e con la multa da euro 103 a euro 1.032. Se il colpevole è persona preposta dalla legge o dall 'autorità agli incanti o alle licitazioni suddette la reclusione è da uno a cinque anni e la multa da euro 516 a euro 2.065. Le pene stabilite in questo articolo si applicano anche nel caso di licitazioni private per conto di privati dirette da un pubblico ufficiale o da persona legalmente autorizzata ma sono ridotte alla metà.	1) Ottenimento e rinnovo di convenzioni e/o concessioni con la Pubblica Amministrazione ; 2) Rapporti con la P.A. per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali (es. iscrizione Albo Gestori rifiuti); 3) Gestione delle verifiche ispettive da parte di enti pubblici o incaricati di pubblico servizio (es. ASL, Guardia di Finanza, NAS, NOE, Polizia Locale, Vigili del Fuoco, ecc.); 4) Gestione di eventuali contenziosi giudiziali e stragiudiziali; 5) gestione dei pagamenti 6) conferimento di incarichi di consulenza e prestazioni professionali; 7) spese di rappresentanza, gli omaggi e sponsorizzazioni; 8) selezione e assunzione del personale; 9) retribuzioni e rimborsi spese al personale; 10) gare	Amministratore Unico, amministrazione, commerciale, Ufficio acquisti, Ufficio de personale, Direttori Tecnici	500 o 200-600		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amministrazione	A
turbata libertà del procedimento di scelta del contraente art. 353 bis	Salvo che il fatto costituisca più grave reato chiunque con violenza o minaccia o con doni promesse collusioni o altri mezzi fraudolenti turba il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione è punito con la reclusione da sei mesi a cinque anni e con la multa da euro 103 a euro 1.032.	1) Ottenimento e rinnovo di convenzioni e/o concessioni con la Pubblica Amministrazione ; 2) Rapporti con la P.A. per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali (es. iscrizione Albo Gestori rifiuti); 3) Gestione delle verifiche ispettive da parte di enti pubblici o incaricati di pubblico servizio (es. ASL, Guardia di Finanza, NAS, NOE, Polizia Locale, Vigili del Fuoco, ecc.); 4) Gestione di eventuali contenziosi giudiziali e stragiudiziali; 5) gestione dei pagamenti 6) conferimento di incarichi di consulenza e prestazioni professionali; 7) spese di rappresentanza, gli omaggi e sponsorizzazioni; 8) selezione e assunzione del personale; 9) retribuzioni e rimborsi spese al personale; 10) gare	Amministratore Unico, amministrazione, commerciale, Ufficio acquisti, Ufficio de personale, Direttori Tecnici	500 o 200-600		separazione dei compiti attraverso deleghe/procure/nomine; codice etico, mansionario, procedure Iso 9001, protocollo rapporti con la pubblica amministrazione	A

10. Norme generali di comportamento

La presente Parte Speciale si riferisce a comportamenti posti in essere da amministratori, dirigenti e dipendenti operanti nelle aree di attività a rischio nonché da Collaboratori esterni, come già definiti nella Parte Generale (tutti definiti come "Destinatari").

E' vietato:

1) effettuare elargizioni in denaro o altre utilità a pubblici funzionari;
2) distribuire e/o ricevere omaggi e regali al di fuori di quanto previsto dal Codice. I regali offerti – salvo quelli di modico valore - devono essere documentati in modo adeguato per consentire le prescritte verifiche;
3) accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della P.A. - o in favore di terzi nel caso in cui si agisce come incaricato di pubblico servizio - che possano influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società;
4) riconoscere compensi, o effettuare prestazioni, in favore di terzi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere, di compenso ricevuto, alle caratteristiche del rapporto di partnership ed alle prassi vigenti in ambito locale;
5) riconoscere compensi in favore dei Fornitori che non trovino adeguata giustificazione in relazione al tipo di controprestazione;
6) presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
7) destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.

Ai fini dell'attuazione dei comportamenti di cui sopra:

a) i rapporti nei confronti della P.A. devono essere gestiti in modo trasparente, procedendo alla nomina di uno o più Responsabili Interni per ogni operazione o pluralità di operazioni (in caso di particolare ripetitività delle stesse);
b) gli incarichi conferiti ai Consulenti devono essere anch'essi redatti per iscritto, con l'indicazione del compenso pattuito e devono essere proposti o negoziati o verificati o approvati;
c) i contratti stipulati con i Fornitori nonché quelli stipulati con altri operatori del Settore, comprese le convenzioni per lo sviluppo della rete, devono essere redatti per iscritto con l'indicazione del compenso pattuito e delle condizioni economiche in generale e devono essere proposti, negoziati, verificati e approvati nel rispetto di procedure che garantiscono la segregazione delle funzioni;
d) nessun tipo di pagamento può esser effettuato in contanti o in natura;

e) le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere rilasciato apposito rendiconto;
f) coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità;
g) nell'ambito dei procedimenti di espropriazione in cui Adopera sia coinvolta in qualità di autorità espropriante, occorre garantire la tracciabilità di ogni fase della procedura.

11. Protocolli preventivi

Oltre ai principi preventivi di carattere generale richiamati al punto 5.3.1 del presente Modello, sono adottate le seguenti prescrizioni

Attività di report per le attività sensibili coinvolgenti la P.A. - Ogni attività sensibile che coinvolga la P.A., soprattutto quelle riferite alle attività di verifica e controllo da parte dell'Ente Pubblico in ragione della specifica attività di Adopera, nonché quelle relative all'ottenimento o rinnovo di concessioni, autorizzazioni, locazioni ecc. necessarie per lo svolgimento della sua attività, devono essere supportate da adeguata documentazione e consentire la tracciabilità delle operazioni effettuate in conformità con i principi preventivi generali.

Processo di assunzione del personale - Applicazione di criteri oggettivi nella selezione dei candidati al fine di evitare che l'assunzione sia il prezzo/utilità mediato di un'attività di corruzione. Prima dell'avvio della procedura devono essere definiti i requisiti richiesti ai candidati e definiti i criteri di valutazione (sia di carattere quantitativo, che qualitativo-curriculare), approvati dall'Amministratore Unico.

Modalità di pagamento – deve poter essere verificata la correttezza e tracciabilità di ogni pagamento corrispondente all'attività svolta, il pagamento non deve essere effettuato in contanti o con strumenti di pagamento analoghi e deve essere effettuato sul conto corrente indicato nel contratto o con le modalità richieste dalla P.A. Il pagamento in ogni caso deve essere rintracciabile e riferibile alla specifica attività per cui viene effettuato. L'indicazione della causale non deve essere generica ma consentire l'individuazione del rapporto sottostante il pagamento. I soggetti beneficiari del pagamento devono corrispondere con i soggetti individuati nel contratto, convenzione ecc. I termini e l'ammontare del pagamento devono altresì

corrispondere con quelli pattuiti. Le spese di rappresentanza devono essere motivate, documentate ed autorizzate, così pure quelle per gli omaggi.

Le spese di sponsorizzazione possono essere effettuate solo dietro presentazione della documentazione giustificativa, verificato il motivo e la corrispondenza del soggetto percipiente con il soggetto richiedente.

Si fa presente, in ogni caso che ex Art. 10, c. 8, lett. a) d.lgs. n. 33/2013, Adopera approva periodicamente il Piano triennale di prevenzione della corruzione e della trasparenza le cui procedure e protocolli devono ritenersi parte integrante di tale MOG.

REATI DI RICETTAZIONE, RICICLAGGIO, AUTORICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA, NONCHE' AUTORICICLAGGIO

Reati di ricettazione, riciclaggio e impiego di denaro, beni o altra utilità di provenienza illecita - (Art. 25 *octies* del Decreto) nonché autoriciclaggio e assolvimento degli obblighi di cui al D.Lgs. n. 231/2007 a carico delle Società Partecipate della P.A.

Il decreto, approvato dal Consiglio dei Ministri il 24 maggio 2017 (D. Lgs n. 90/17), oltre a introdurre a carico di soggetti determinati tra cui le P.A. e le Società da esse partecipate una serie di obblighi di segnalazione di operazioni sospette all'Uif, riscrive integralmente, fra gli altri, il D. Lgs n. 231/2007 in tema di contrasto al riciclaggio e al finanziamento del terrorismo, in attuazione della direttiva (UE) 2015/849 (c.d. IV Direttiva Antiriciclaggio). La previsione di obblighi di segnalazione connessi ad operazioni da cui possono discendere violazioni di disposizione contenute nella legislazione in materia di antiriciclaggio e conseguentemente configurarsi reati ricompresi in quelli di cui all'art. 25 octies del D. Lgs n. 231/01 impone alle società a partecipazione pubblica di elaborare una serie di misure organizzative ad hoc astrattamente idonee a ridurre i relativi rischi.

L'articolo 10 del D. Lgs n. 231 del 2007, in seguito alle modifiche introdotte dal D. Lgs n. 90/17, dispone infatti che anche le Società come Adopera S.r.l. (ricompresa nella definizione di Pubblica Amministrazione di cui all'art. 1, comma 2, lett. hh) comunichino all'Unità d'Informazione Finanziaria (UIF) presso la Banca d'Italia i dati e le informazioni concernenti le operazioni sospette di cui vengono a conoscenza

nell'esercizio della propria attività istituzionale, per consentire lo svolgimento di analisi finanziarie mirate a far emergere fenomeni di riciclaggio e di finanziamento del terrorismo. Per quanto attiene le pubbliche amministrazioni e le società da esse partecipate, gli ambiti rispetto ai quali, ai sensi del prefato art. 10, si applicano le disposizioni del decreto in narrativa riguardano:

1 i procedimenti finalizzati all'adozione di provvedimenti di autorizzazione o concessione;

2 le procedure di scelta del contraente per l'affidamento di lavori, forniture e servizi secondo le disposizioni di cui al codice dei contratti pubblici;

3 i procedimenti di concessione ed erogazione di sovvenzioni, contributi, sussidi, ausili finanziari, nonché attribuzioni di vantaggi economici di qualunque genere a persone fisiche ed enti pubblici e privati.

È assodato quindi il fatto che pari alle Pubbliche Amministrazioni, anche in capo alla Società Adopera s.r.l. ricadano i medesimi oneri rispetto alle procedure di cui ai punti sopra elencati, relativamente sicuramente al punto 1 e 2, che coinvolgono le attività quotidiane della società. Si ritiene, però di escludere l'applicazione del punto 3 essendo espressamente vietati dai contratti di servizio stipulati tra la società stessa e gli Enti Soci qualsiasi procedimento di concessione ed erogazione di denaro sotto varie forme.

Il D. Lgs n. 231/2007 quindi è a ritenersi essenziale anche ai fini dell'efficace attuazione del Modello organizzativo.

Sulla base di specifiche linee guida la Società deve quindi adottare "procedure interne, proporzionate alle proprie dimensioni organizzative e operative, idonee a valutare il livello di esposizione dei propri uffici al rischio" individuando le misure necessarie a mitigarlo. Tale procedura interna viene individuata nel PTPCT sotto la voce "Procedura antiriciclaggio e di segnalazione al UIF".

Sempre l'art.10 del D. Lgs n. 231/2007, al comma 5 prevede che la Società nel quadro dei programmi di formazione continua del personale, adotti misure idonee ad assicurare il riconoscimento, da parte dei propri dipendenti, delle fattispecie meritevoli di comunicazione alla Uif. Poiché le comunicazioni alla Uif, previste al comma 4 dell'art. 10 del decreto in questione, non sono una facoltà ma atto dovuto, gli Amministratori ed i dipendenti sono tenuti a sottoporre al gestore delle segnalazioni i casi da loro ritenuti sospetti ai fini di avviare la procedura di istruttoria. In favore di coloro che avviano la procedura per l'istruttoria di una comunicazione alla Uif, trovano applicazione le norme poste a tutela della loro riservatezza personale, quindi la Società deve adottare nella procedura tutte le misure idonee ad

assicurare la riservatezza dell'identità della/e persone che effettuano la segnalazione. A tal fine, a carico del gestore delle comunicazioni alla Uif, si applica il divieto quindi di riferire a terzi ogni notizia e i dati adeguatamente conservati.

Il tema della "proporzionalità" risulta estremamente rilevante e pervasivo nella gestione ed applicazione dei presidi antiriciclaggio. Vista, infatti, la vasta schiera di soggetti pubblici individuati quali destinatari dell'art. 10, D.Lgs. 231/2007, appare fondamentale calibrare gli obblighi organizzativi e segnaletici in funzione delle dimensioni e del tipo di attività svolta, favorendo nel contempo la massima integrazione di tutte le risorse destinate alla prevenzione, senza dimenticare il costante monitoraggio delle procedure e della formazione del personale.

Le fattispecie dei reati societari richiamate dall'art. 25 *octies* del Decreto

Secondo quanto emerso dall'attività di *risk assessment* tutte le fattispecie individuate dall'art. 25 octies del Decreto sono potenzialmente a rischio di commissione all'interno della Società.

Con entrata in vigore del d.lgs. 195/2021 recante attuazione della direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale (D.Lgs. 8 novembre 2021, n. 195 – G.U. 30 novembre 2021, n. 285, Suppl. ord. n. 41), si ampliano i reati presupposto dei delitti di ricettazione, riciclaggio, autoriciclaggio e impiego di beni o utilità di provenienza illecita che comprendono ora anche le contravvenzioni e nel caso di riciclaggio e autoriciclaggio anche i delitti colposi.

Le contravvenzioni sono reati "minori", puniti con arresto e ammenda, quindi con una pena meno grave rispetto ai delitti. Si tratta di reati che seppure più lievi (per gravità del fatto e punizione) sono comunque rientranti nell'ambito penale. Nel caso di riciclaggio, autoriciclaggio o impiego di denaro proveniente da contravvenzioni, la pena risulta comunque inferiore rispetto a quella prevista nel caso in cui il reato presupposto sia invece un delitto.

L'aggiunta dei delitti colposi al novero dei reati presupposto al riciclaggio porta la Società ad avere implicazioni più profonde in quanto per sussistere un reato presupposto non sarà necessario provare la sussistenza del dolo, della volontà di commettere reato, ma sarà sufficiente l'ottenimento di un illecito vantaggio economico derivante da una condotta colposa, quale ad esempio l'omessa vigilanza o l'omesso adeguamento a normativa di prevenzione specifica.

Ricettazione (art. 648 c.p.)

L'art. 648 c.p. sanziona la condotta di chi, fuori dei casi di concorso nel reato, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, ovvero comunque si intromette nel farle acquistare, ricevere od occultare.

Elemento costitutivo imprescindibile per la configurabilità della fattispecie è l'esistenza di un altro reato dal quale provengano le cose oggetto dell'azione incriminata. È altresì necessario che l'autore della ricettazione abbia come finalità quella di perseguire, per sé o per altri, un profitto che può essere anche di carattere non patrimoniale.

Riciclaggio (art. 648 bis c.p.)

L'art. 648 bis c.p. testualmente punisce chi, fuori dei casi di concorso nel reato, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.)

L'art. 648 ter c.p. sanziona la condotta di chi, fuori dai casi di concorso nei reati di ricettazione e riciclaggio, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

Autoriciclaggio (art. 648 ter-1 c.p.)

L'art. 648 ter-1 c.p. sanziona la condotta di chi, avendo commesso o concorso a commettere un delitto, impiega, sostituisce o trasferisce in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Non sono punibili le condotte attraverso le quali il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale.

Destinatari e Principi generali di comportamento

L'Amministratore Unico ed i dipendenti che svolgono le attività sensibili indicate nel paragrafo precedente, devono attenersi ai principi generali di comportamento di seguito esposti al fine di prevenire il verificarsi dei reati societari rilevanti per la Società e previsti dal Decreto.

Le deroghe, le violazioni o il sospetto di violazioni delle norme che disciplinano le attività a rischio di reato di cui alla presente Sezione sono oggetto di segnalazione da parte di tutti i dipendenti e degli organi sociali secondo le modalità previste nella Parte Generale del presente Modello.

In particolare, si stabiliscono i seguenti principi generali di comportamento:

- deve essere sempre assicurato il regolare funzionamento dei flussi finanziari della Società: sia in entrata che in uscita, questi sono costantemente monitorati e sempre tracciabili;
- la Società, ai fini dell'attuazione delle decisioni di impiego delle risorse finanziarie, si avvale soltanto di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e correttezza conformi alla disciplina dell'Unione Europea;
- i dati e le informazioni su Clienti e Fornitori sono completi ed aggiornati, in modo da garantire la corretta e tempestiva individuazione dei medesimi e una puntuale valutazione e verifica del loro profilo.

Principi specifici di comportamento

Risulta opportuno evidenziare che con l'entrata in vigore del D. Lgs n. 90/2017 il campo di azione della Società è limitato alle specifiche aree di competenza precedentemente richiamate, impedendo di fatto, l'attuazione di qualsiasi verifica di iniziativa. Ciò non esclude, nel caso in cui si assista o si sospetti il compimento di un reato, di effettuare le dovute denunce agli organi investigativi competenti.

Il D. Lgs n. 231/2007 per consentire lo svolgimento di analisi finanziarie mirate a far emergere fenomeni di riciclaggio, ha previsto la comunicazione al UIF di dati ed informazioni riguardanti le operazioni sospette di cui la Società venga a conoscenza nell'esercizio della propria attività. In questo contesto, l'Uif ha individuato i dati e le informazioni da trasmettere, le modalità ed i termini della relativa comunicazione, nonché gli indicatori per agevolare la rilevazione delle operazioni sospette. Nello specifico, il documento elaborato dal UIF è formato da diverse disposizioni (articoli da 1 a 12) e da un allegato contenente gli indicatori di anomalia elaborati al fine di agevolare l'individuazione delle operazioni sospette da parte degli uffici della Pubblica amministrazione. La società ha definito le modalità con cui approcciarsi alla tematica integrando nei termini di quanto di seguito descritto quanto declinato nel "Piano Triennale per la Prevenzione della Corruzione e della Trasparenza" con le indicazioni formulate dall'Uif al fine di assicurare la conformità alla normativa di riferimento rivolta espressamente alle P.A. e alle Società da essa partecipate. In linea generale, è fatto divieto di acquisto, ricezione, sostituzione o trasferimento di beni o denaro

effettuati per occultare o dissimulare la loro origine illecita, quando si abbia motivo di ritenere che provengano da attività delittuosa.

Oltre alle regole definite rigidamente dal D. Lgs n. 231/2007 e dalle regole generali di organizzazione individuate nella Parte Introduttiva del MOG che sono applicate in via generale in relazione a tutte le attività sensibili individuabili ai sensi del Decreto e che devono informare i presenti principi speciali oltreché i relativi protocolli e procedure aziendali, le procedure adottate da Adopera Srl volte a prevenire il rischio connesso alla commissione di potenziali reati di ricettazione, riciclaggio etc. di cui alla presente sezione e a prescindere dalle casistiche delle operazioni sospette, sono le seguenti:

i. Gestione di omaggi, liberalità, gestito dal "Codice di comportamento" integrato nel PTPCT;
ii. Procedura antiriciclaggio e di segnalazione all'UIF integrata nel PTPCT, completa di indicatori di anomalia individuati dall'UIF, schede con analisi del grado di vulnerabilità della procedura e mappatura del rischio specifico di riciclaggio etc.

L'Amministratore Unico e tutti i dipendenti quindi, anche seguendo le procedure messe a loro disposizione, devono:

1) Osservare la realtà: i dati e le informazioni sono quotidianamente sotto gli occhi dei dipendenti che effettuano le loro attività.
2) Sospetto: alla base di una operazione che, anche se rispetta il processo e la procedura, rivela contorni definiti almeno "strani" dagli operatori o per la specificità dell'operazione in sé, o per la collocazione della stessa all'interno di un quadro di eventi più o meno relazionati tra loro
3) Segnalazione: segnalare in caso di operazione sospetta al gestore delle segnalazioni designato
4) Invio segnalazione: il gestore delle segnalazioni al UIF seguirà la procedura di segnalazione al fine della corretta gestione della comunicazione.

5.Sanzioni

Le sanzioni previste dal Decreto per questa categoria di reati sono:

Sanzione pecuniaria:

a) da 200 a 800 quote;
b) da 400 a 1000 quote (nel caso in cui il denaro, beni o altre utilità provengono da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a 5 anni)

Sanzioni interdittive:

a) interdizione dall'esercizio dell'attività;

b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

c) divieto di contrattare con la pubblica amministrazione;

d) esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi;

e) divieto di pubblicizzare beni o servizi.

6. Identificazione delle attività sensibili

L'attività di risk assessment ha identificato, ai sensi dell'art. 6 del Decreto, le seguenti attività sensibili nell'ambito delle quali possono essere commessi i reati di cui all'art. 25 octies del Decreto medesimo:

1) gestione degli acquisti di beni e servizi, delle collaborazioni e delle consulenze, delle provvigioni, dei partners e delle controparti (secondo le disposizioni del codice dei contratti pubblici);
2) provvedimenti ampliativi della sfera giuridica dei destinatari privi di effetto economico diretto ed immediato per il destinatario (autorizzazioni allo scavo in area pubblica e concessioni cimiteriali);
3) coordinamento e gestione dei flussi finanziari in genere, elaborazione del bilancio;
4) gestione delle attività e degli adempimenti connessi alla fiscalità rapporti con fornitori, partner e soggetti terzi;
5) transazioni finanziarie e gestione dei flussi finanziari;
6) sponsorizzazioni, regalie e omaggi.

7. Valutazione del rischio e matrice-reati

La valutazione del rischio di commissione di tale fattispecie criminosa in Adopera viene espressa attraverso il criterio già descritto al punto 3 del presente MOG.

Di seguito si riporta, quindi, la matrice di reato con individuato il rischio emerso attraverso il calcolo di P x D di cui al punto 3 del presente MOG e con specifica dei protocolli e/o procedure tali da rendere il rischio detto, ove ritenuto presente, come accettabile (intendendosi "accettabile" il rischio della commissione dei reati presupposto considerati esclusivamente attraverso l'elusione intenzionale e fraudolenta delle procedure e/o protocolli previste/i).

REATO	CONDOTTA	ATTIVITA' SENSIBILI	FUNZIONI E RISORSE UMANE COINVOLTE	quote	RI	PROTOCOLLI SPECIFICI	RR
Ricettazione (art. 648 c.p.) modifcato ex D.lgs. 195/21	al fine di procurare a sé o ad altri un profitto, acquistare, ricevere od occultare denaro o cose provenienti da un qualsiasi delitto, o intromettersi nel farle acquistare, ricevere od occultare	1) rapporti con fornitori, consociati, partner e soggetti terzi; 2) contratti di acquisto e/o vendita con controparti; 3) transazioni finanziarie e gestione dei flussi finanziari; 4) sponsorizzazioni; gestione cassa	Amministratore Unico, Ufficio Manutenzione, Direttori Tecnici,RUP, RASA/RPCT, Uffici amministrativi cimiteriali, uffici contabilità, ufficio risorse umane	fino a 1000 + interdittive		Verifica dei soggetti e delle transazioni economiche – anagrafiche dei fornitori; procedure autorizzatorie di cassa, protocollo assegnazione incarichi professionali, protocollo acquisto beni e servizi, assegnazione incarichi professionali, protocollo regali omaggi e sponsorizzazioni, periodica formazione in materia di antiriciclaggio ed anticorruzione, procedure UIF, procedure antiriciclaggio	
Riciclaggio (art. 648-bis c.p.) modifcato ex D.lgs. 195/21	sostituire o trasferire denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compiere in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa	1) rapporti con fornitori, consociati, partner e soggetti terzi; 2) contratti di acquisto e/o vendita con controparti; 3) transazioni finanziarie e gestione dei flussi finanziari; 4) sponsorizzazioni; gestione cassa	Amministratore Unico, Ufficio Manutenzione, Direttori Tecnici,RUP, RASA/RPCT, Uffici amministrativi cimiteriali, uffici contabilità, ufficio risorse umane	fino a 1000 + interdittive		Verifica dei soggetti e delle transazioni economiche – anagrafiche dei fornitori; procedure autorizzatorie di cassa, protocollo assegnazione incarichi professionali, protocollo acquisto beni e servizi, assegnazione incarichi professionali, protocollo regali omaggi e sponsorizzazioni, periodica formazione in materia di antiriciclaggio ed anticorruzione, procedure UIF, procedure antiriciclaggio	
Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)modifcato ex D.lgs. 195/21	fuori dei casi di concorso nel reato e dei casi previsti dagli artt. 648 e 648-bis, impiegare in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto	1) rapporti con fornitori, consociati, partner e soggetti terzi; 2) contratti di acquisto e/o vendita con controparti; 3) transazioni finanziarie e gestione dei flussi finanziari; 4) sponsorizzazioni; gestione cassa	Amministratore Unico, Ufficio Manutenzione, Direttori Tecnici,RUP, RASA/RPCT, Uffici amministrativi cimiteriali, uffici contabilità, ufficio risorse umane	fino a 1000 + interdittive		Verifica dei soggetti e delle transazioni economiche – anagrafiche dei fornitori; procedure autorizzatorie di cassa, protocollo assegnazione incarichi professionali, protocollo acquisto beni e servizi, assegnazione incarichi professionali, protocollo regali omaggi e sponsorizzazioni, periodica formazione in materia di antiriciclaggio ed anticorruzione, procedure UIF, procedure antiriciclaggio	
autoriciclaggio (art. 649-ter 1 c.p.)modifcato ex D.lgs. 195/21	impiegare, sostituire, trasferire in attività economiche finanziarie imprenditoriali o speculative il denaro, i beni o le altre utilità derivanti dal delitto non colposo che lo stesso ha commesso o concorso a commettere in modo da ostacolare concretamente l'identificazione di tali beni/utilità/denaro ; non punibili le condotte di mero utilizzo o godimento personale della provvista illecita.	tutte le condotte ritenute sensibili nel presente MOG, in assenza di chiara individuazione dei limiti di applicabilità di tale norma; la società ritiene che la fattispecia debba applicarsi ai soli reati presupposto base previsti ex D.lgs. 231/01	Amministratore Unico, Ufficio Manutenzione, Direttori Tecnici,RUP, RASA/RPCT, Uffici amministrativi cimiteriali, uffici contabilità, ufficio risorse umane	fino a 1000 + interdittive		Tutti i protocolli, prassi e procedure previsti nel presente MOG per le varie tipologie di reato presupposto affrontati.	

8. Norme generali di comportamento

Con riguardo all'utilizzo tutti coloro che operano per conto della società con particolare attenzione all'attività cimiteriale, debbono conformarsi ai seguenti principi:

1) definire ruoli e responsabilità nella gestione del processo di verifica degli acquisti;
2) identificare l'attendibilità dei fornitori al fine di verificarne l'affidabilità anche sotto il profilo della correttezza e tracciabilità delle transazioni economiche con gli stessi, evitando di instaurare o proseguire rapporti con soggetti che non presentino o mantengano nel tempo adeguati requisiti di trasparenza e correttezza;
3) monitorare nel tempo, il permanere in capo ai fornitori dei requisiti di affidabilità, correttezza, professionalità e onorabilità;

4) determinare i requisiti minimi in possesso dei soggetti offerenti e fissare i criteri di valutazione delle offerte nei contratti standard;
5) verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
6) non effettuare e non accettare pagamenti in contanti;
7) operare controlli formali e sostanziali sui flussi finanziari aziendali, con riferimento ai pagamenti verso terzi e ai pagamenti/operazioni verso controllate, tenendo in particolare conto la sede legale della società controparte, degli istituti di credito utilizzati e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;
8) disciplinare la registrazione e conservazione dei dati relativi alle transazioni, ivi compresi quelli relativi ai rapporti con le controllate;
9) garantire la predisposizione e l'aggiornamento dell'anagrafica dei fornitori e dei c;
10) stabilire standard contrattuali per l'emissione di ordini/contratti di acquisto;
11) garantire la segnalazione delle operazioni che presentino profili di sospetto con riguardo alla legittimità della provenienza delle somme oggetto di transazione o all'affidabilità e trasparenza della controparte;
12) attuare la costante formazione ed informazione degli esponenti aziendali sui temi relativi alla prevenzione dei fenomeni di riciclaggio;
13) dare evidenza delle attività e dei controlli svolti.

9. Protocolli preventivi generali

Oltre ai principi preventivi di carattere generale richiamati al punto 5.3.1 del presente Modello, sono adottate le seguenti prescrizioni:

Verifica dei soggetti e delle transazioni economiche – assicurare l'identificazione, l'attendibilità e affidabilità dei fornitori e/o dei soggetti con cui la Società effettua transazioni economiche (ad esclusione delle normali transazioni con gli utenti dei servizi), evitando di instaurare o proseguire rapporti con soggetti che non presentino o mantengano nel tempo adeguati requisiti di trasparenza e correttezza e che rivelino indicatori di anomalia, come specificati nelle normative o disposizioni di settore. Deve essere verificata la regolarità dei pagamenti e la corrispondenza tra destinatario/ordinante e controparti effettivamente coinvolte nelle transazioni. Deve essere curata altresì la registrazione e conservazione dei dati relativi alle transazioni, ivi compresi quelli relativi ai rapporti con le controllate

Anagrafiche fornitori – si deve periodicamente aggiornare l'anagrafica dei fornitori con definizione di requisiti minimi e standard di qualità, affidabilità, correttezza, professionalità e onorabilità.

Anagrafiche beneficiari di regalie omaggi e sponsorizzazioni – si deve periodicamente aggiornare l'anagrafica dei beneficiari con definizione di requisiti minimi e standard di qualità, affidabilità, correttezza, professionalità e onorabilità.

PROCEDURE ANTIRICICLAGGIO E DI SEGNALAZIONE AL UIF

La Società Adopera S.r.l. è tenuta ai sensi del D. Lgs n. 231/2007 ad effettuare le comunicazioni alla UIF a prescindere dalla rilevanza e dall'importo dell'operazione sospetta.

La comunicazione di operazioni sospette alla UIF non coincide con la denuncia di reato all'Autorità giudiziaria che pubblici ufficiali e incaricati di pubblico servizio sono tenuti ad effettuare in base all'art. 331 c.p.p. quando, per informazioni acquisite nell'esercizio della funzione ovvero a causa delle funzioni o del servizio, "hanno notizia di un reato perseguibile d'ufficio" e che si fonda sull'individuazione di fatti specifici corrispondenti a diversa fattispecie penalmente rilevante. Dunque, l'eventuale invio di una comunicazione alla UIF per operazioni sospette non esclude l'obbligo di effettuare la denuncia dei medesimi fatti in presenza dei citati presupposti.

Il sospetto però deve essere basato su una compiuta valutazione degli elementi oggettivi e soggettivi acquisiti nell'ambito della propria attività, svolta anche alla luce degli indicatori di anomalia emanati dal UIF.

Detti indicatori, tratti dal documento elaborato dal UIF, attengono ad aspetti sia soggettivi (connessi all'identità od al comportamento del soggetto cui si riferisce l'operazione) che oggettivi. Alcuni sono di carattere generale, altri più specifici per i vari settori di attività (appalti e contratti pubblici, immobili e commercio, finanziamenti pubblici). Gli indicatori, elaborati dal UIF, sono volti a ridurre i margini di incertezza delle valutazioni soggettive connesse alle comunicazioni di operazioni sospette e hanno lo scopo di contribuire al contenimento degli oneri e alla correttezza e omogeneità delle comunicazioni medesime. L'elencazione degli indicatori di anomalia non è esaustiva, anche in considerazione della continua evoluzione delle modalità di svolgimento delle operazioni. L'impossibilità di ricondurre operazioni o comportamenti a uno o più degli indicatori non è sufficiente a escludere che l'operazione sia sospetta; pertanto saranno nel tempo valutati con la massima attenzione ulteriori comportamenti e caratteristiche delle operazioni che, sebbene non descritti negli indicatori, siano egualmente sintomatici di profili di sospetto e conseguentemente saranno contemplati tra gli stessi indicatori. La mera ricorrenza di operazioni o comportamenti descritti in uno o più indicatori di anomalia non è motivo di per sé sufficiente per la qualificazione dell'operazione come sospetta ai fini della comunicazione alla UIF, ma è comunque necessario svolgere una specifica analisi nel concreto e una valutazione complessiva dell'operatività avvalendosi di tutte le altre informazioni disponibili. La Società

applica gli indicatori rilevanti alla luce dell'attività in concreto svolta e si avvale degli indicatori di carattere generale unitamente a quelli specifici per tipologia attività.

Ai fini dell'applicazione degli indicatori, per "soggetto cui è riferita l'operazione" si intende il soggetto (persona fisica o entità giuridica) che entra in relazione con la Società e riguardo al quale emergono elementi di sospetto di riciclaggio, di finanziamento del terrorismo o di provenienza da attività criminosa delle risorse economiche e finanziarie. Per favorirne la lettura e la comprensione alcuni indicatori sono stati specificati in sub-indici; i sub-indici costituiscono un'esemplificazione dell'indicatore di riferimento e devono essere valutati congiuntamente al contenuto dello stesso. I riferimenti dell'indicatore a circostanze oggettive (quali, ad esempio, la ripetitività dei comportamenti o la rilevanza economica dell'operazione) ovvero soggettive (quali, ad esempio, l'eventuale incoerenza della giustificazione addotta o del profilo economico del soggetto cui è riferita l'operazione), seppure non specificamente richiamati, valgono anche con riguardo ai relativi sub-indici. Le operazioni e i comportamenti inerenti ad attività economiche svolte nei settori degli appalti e dei finanziamenti pubblici, devono essere valutati sulla base degli elementi di anomalia indicati per ciascun settore e dei seguenti criteri: incoerenza con l'attività o il profilo economico-patrimoniale del soggetto cui è riferita l'operazione; assenza di giustificazione economica; inusualità, illogicità, elevata complessità dell'attività.

Soggetti coinvolti

Tutti i dipendenti e l'Amministratore Unico sono coinvolti nella presente procedura e parte proattiva della stessa, in quanto svolgono attività che possono permettere loro di notare eventuali attività sospette.

L'Amministratore Unico e tutti i dipendenti quindi, devono:

1) Osservare la realtà: i dati e le informazioni sono quotidianamente sotto gli occhi dei dipendenti che effettuano le loro attività.
2) Sospetto: alla base di una operazione che, anche se rispetta il processo e la procedura, rivela contorni definiti almeno "strani" dagli operatori o per la specificità dell'operazione in sé, o per la collocazione della stessa all'interno di un quadro di eventi più o meno relazionati tra loro;
3) Segnalazione: segnalare, senza ritardo in caso di operazione sospetta al gestore delle segnalazioni designato.

Le comunicazioni al "soggetto gestore"

Al verificarsi di una o più delle situazioni di cui agli indicatori di anomalia elencati in calce di cui anche al provvedimento del 23 aprile 2018 della UIF, i dipendenti della Società o l'Amministratore Unico, fatti gli opportuni approfondimenti, hanno

l'obbligo di segnalare tempestivamente in forma scritta al "soggetto gestore", anche via mail all'indirizzo di posta elettronica odv@adoperasrl.it mettendo come oggetto RISERVATA – OPERAZIONE SOSPETTA, le operazioni sospette, fornendo tutte le informazioni e tutti i documenti utili a consentire un'adeguata istruttoria.

Il "soggetto gestore" è comunque tenuto a garantire il rispetto della riservatezza dei soggetti coinvolti.

Dovranno in ogni caso essere fornite tutte le informazioni, i dati e la documentazione utili a consentire al "soggetto gestore" un'adeguata istruttoria. Attraverso tale comunicazione l'operatore dovrà relazionare in modo puntuale quanto rilevato, indicando oltre a tutti gli elementi, le informazioni e i dati anche i motivi del sospetto.

Considerata la non esaustività dell'elenco di indicatori di anomalia della UIF, le segnalazioni al "soggetto gestore" devono essere fatte ogniqualvolta si abbia il ragionevole motivo di ritenere che sia stato compiuto o tentato il compimento di operazioni di riciclaggio o di finanziamento del terrorismo.

Analogamente, con riferimento agli indicatori di anomalia connessi con specifico settore di attività, trattandosi di elencazione non tassativa, l'attività di segnalazione deve estendersi a tutti i settori della Società, qualora si configurino ipotesi riconducibili a sospette attività di riciclaggio o di finanziamento del terrorismo. Risulta opportuno evidenziare che il campo di azione di Adopera s.r.l. è limitato alle specifiche aree di competenza precedentemente richiamate, impedendo di fatto, l'attuazione di qualsiasi verifica di iniziativa. Ciò non esclude, nel caso in cui si assista o si sospetti il compimento di un reato, di effettuare le dovute denunce agli organi investigativi competenti.

I compiti e le prerogative del "soggetto gestore"

Il "soggetto gestore", oltre a delineare le presenti procedure operative atte a garantire un tempestivo assolvimento degli obblighi di comunicazione verso l'Unità di Informazione Finanziaria – U.I.F. deve provvedere:

1. A verificare la formazione in materia di antiriciclaggio del personale della Società e programmarne gli aggiornamenti periodici;

2. A raccogliere le segnalazioni ed avviare senza ritardo le successive necessarie verifiche, conservandone l'esito;

3. A discernere, nell'ambito della suddetta attività di verifica, se le segnalazioni in materia di prevenzione del riciclaggio e quelle in materia di anticorruzione e

trasparenza possano essere collegate, avviando l'eventuale attività richiesta dal caso;

4. Informare delle segnalazioni ricevute direttamente l'Amministratore Unico affinché sia edotto sul caso (sempre considerando la riservatezza);

5. A garantire, nel flusso delle comunicazioni, il rispetto della riservatezza dei soggetti coinvolti;

6. A trasmettere all'UIF dati e informazioni concernenti le operazioni valutate come sospette in seguito alle attività di verifica di cui al punto 2, ai sensi dell'articolo 10, comma 4, del D. Lgs. n.231/2007;

7. A fungere da interlocutore della UIF per tutte le comunicazioni e i relativi approfondimenti, al fine di garantire efficacia e riservatezza nella gestione delle informazioni. Per lo svolgimento dei compiti assegnati, il "soggetto gestore" ha diritto d'accesso a tutta la documentazione connessa alla segnalazione pervenuta e, in ogni caso, utile a svolgere la necessaria verifica e, qualora se ne ravvisi la necessità, può sentire tutti gli operatori coinvolti, al fine di raccogliere le necessarie informazioni sulle fattispecie in esame.

Contenuti e modalità di invio della comunicazione all'UIF

Il gestore provvederà ad effettuare le comunicazioni dopo una fase di verifica approfondita del caso e della relativa documentazione, provvedendo contestualmente alla compilazione di un fascicolo che ne attesti lo studio anche tenendo conto degli indicatori come sopra descritto. Le comunicazioni saranno effettuate senza ritardo alla UIF in via telematica, attraverso la rete internet, tramite il portale INFOSTAT-UIF della Banca di Italia (adesione al sistema effettuata in data 30/08/2022). La comunicazione è contraddistinta da un numero identificativo e da un numero di protocollo attribuito in modo univoco su base annua dal sistema informativo della UIF. Le modalità per l'adesione al sistema di comunicazione on-line e per la trasmissione delle informazioni sono quelle indicate nel sito internet della UIF. Qualora siano riscontrati errori materiali o incongruenze nel contenuto di una comunicazione inviata ovvero si rilevi l'omesso riferimento di informazioni rilevanti in proprio possesso, si procede all'inoltro di una nuova comunicazione che sostituisce integralmente la precedente i cui contenuti sono indicati all'art. 9 delle Linee guida UIF.

I contenuti sono quelli indicati dall'art. 4 all'art. 8 delle istruzioni emanate dal UIF.

OMICIDIO COLPOSO E LESIONI GRAVI O GRAVISSIME IN VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

La Legge 3 agosto 2007 n. 123 ha inserito nel Decreto l'art. 25-septies che aggiunge all'elenco degli illeciti presupposto della responsabilità degli Enti i delitti di omicidio colposo e di lesioni colpose gravi o gravissime, se commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Successivamente, il D.Lgs. 9 aprile 2008 n. 81 (Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro) ha profondamente riordinato le molteplici fonti normative previgenti in materia. Per quanto concerne la responsabilità amministrativa degli enti, l'art. 300 ha modificato l'art. 25 septies del D.Lgs. 231/2001 lasciando nella sostanza immutata l'individuazione delle fattispecie penali che costituiscono reati presupposto; l'art. 30 inoltre ha esplicitato le caratteristiche che deve presentare il Modello di organizzazione, gestione e controllo al fine della prevenzione dei reati in esame.

Le fattispecie delittuose inserite all'art. 25-*septies* riguardano unicamente le ipotesi in cui l'evento sia stato determinato non già da colpa di tipo generico (e dunque per imperizia, imprudenza o negligenza) bensì da "colpa specifica" che richiede che l'evento si verifichi a causa della inosservanza delle norme per la prevenzione degli infortuni sul lavoro.

Ad oggi Adopera esercita la sua attività nel rispetto dei precetti di cui al TU 81/08 pur in assenza di un sistema di gestione certificato.

1. Omicidio colposo (art. 589 c.p.)

Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni.

Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a sette anni. (…)

Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici.

2. Lesioni personali colpose (art. 590 c.p.)

Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a 309 euro.

Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da 123 euro a 619 euro; se è gravissima, della reclusione da tre mesi a due anni o della multa da 309 euro a 1.239 euro.

Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni. (…)

Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque.

Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale.

Per lesioni gravi si intendono quelle consistenti in una malattia che metta in pericolo la vita o provochi una incapacità di attendere alle ordinarie occupazioni per un periodo superiore ai **quaranta giorni**, oppure in un indebolimento permanente di un senso o di un organo.

Per lesioni gravissime si intendono la malattia probabilmente insanabile, la perdita di un senso, di un arto, di un organo o della capacità di procreare, la difficoltà permanente nella favella, la deformazione o lo sfregio permanente del viso.

3.Sanzioni

Le sanzioni previste dal Decreto per i reati sopra citati sono:

1) nel caso in cui l'omicidio colposo o le lesioni gravi o gravissime avvengano con omessa valutazione dei rischi e adozione del Documento di Valutazione dei Rischi (DVR):
   a) Sanzione pecuniaria pari a 1000 quote;
   b) Sanzione interdittive da 3 mesi a 1 anno.

2) nel caso di omicidio colposo con violazione delle norme sulla tutela della salute e sicurezza sul lavoro:

a) Sanzione pecuniaria da 250 a 500 quote:
b) Sanzione interdittive da 3 mesi a 1 anno.

3) nel caso di lesioni gravi o gravissime con violazione delle norme sulla tutela della salute e sicurezza sul lavoro:
a) Sanzione pecuniaria fino a 250 quote;
b) Sanzioni interdittive fino a 6 mesi.

Le sanzioni interdittive sono quelle previste dall'art. 9 comma 2 del Decreto, ossia:
a) interdizione dall'esercizio dell'attività;
b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c) divieto di contrattare con la pubblica amministrazione salvo che per ottenere le prestazioni di un pubblico servizio;
d) esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi;
e) divieto di pubblicizzare beni o servizi.

4. Identificazione delle attività sensibili

La gestione dei rischi in materia di salute e sicurezza sul lavoro riguarda qualunque tipologia di attività finalizzata a sviluppare ed assicurare un sistema di prevenzione e protezione dei rischi esistenti sul luogo di lavoro, in ottemperanza a quanto previsto dal D.Lgs. n.81/2008 (di seguito Testo Unico).

Tutte le aree di attività aziendale pertanto sono a rischio di commissione dei reati di natura colposa contemplati nella presente parte speciale, pur se con differenti tipologie e gradi di rischio.

1) attuazione misure di miglioramento a seguito valutazione dei rischi;
2) gestione della sicurezza - attività di verifiche, controlli e sorveglianza;
3) valutazione dei rischi: in caso di rischio non valutato o insufficientemente valutato.

5. Valutazione del rischio e matrice-reati

La valutazione del rischio di commissione di tale fattispecie criminosa in Adopera viene espressa attraverso il criterio già descritto al punto 3 del presente MOG.

Di seguito si riporta, quindi, la matrice di reato con individuato il rischio emerso attraverso il calcolo di P x D di cui al punto 3 del presente MOG e con specifica dei

protocolli e/o procedure tali da rendere il rischio detto, ove ritenuto presente, come accettabile (intendendosi "accettabile" il rischio della commissione dei reati presupposto considerati esclusivamente attraverso l'elusione intenzionale e fraudolenta delle procedure e/o protocolli previste/i).

REATO	CONDOTTA	ATTIVITA' SENSIBILI	FUNZIONI E RISORSE UMANE COINVOLTE	quote	RI	PROTOCOLLI SPECIFICI	RR
Omicidio colposo (art. 589 c.p.)	cagionare per colpa la morte di una persona	1) Valutazione dei rischi su tutte le attività lavorative svolte dal personale di RADIS: in caso di rischio non valutato o insufficientemente valutato, mancata attuazione e formazione delle procedure del sistema di gestione salute e sicurezza interno; 2) Mancata attuazione del D.Lgs. 81/08 art. 30 co.1 lett. a) rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici. Mancata attuazione del D.Lgs. 81/08 art. 30 co.1 lett. c) attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza.3) Mancata attuazione del D.Lgs. 81/08 art. 30 co.1 lett. d) attività di sorveglianza sanitaria.4)Mancata attuazione del D.Lgs. 81/08 art. 30 co.1 lett. e) attività di informazione e formazione dei lavoratori.5)Mancata attuazione del D.Lgs. 81/08 art. 30 co.1 lett. g) acquisizione di documentazioni e certificazioni obbligatorie di legge.6)Mancata attuazione del D.Lgs. 81/08 art. 30 co.1 lett. h) periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate. 6)Mancata attuazione del D.Lgs. 81/08 art. 30 co.3 Sistema sanzionatorio. 7)Mancata attuazione del D.Lgs. 81/08 art. 30 co.4 Controllo adeguatezza e riesame del sistema.	D.L. - M.C. - RSPP - Diregente procurato, Responsabili Tecnici e preposti.	fino 1000 + interditti ve		attuazione Procedure operative interne emesse ai fini salute e sicurezza nei luoghi di lavoro	
Lesioni personali colpose gravi (art. 590 c.p)	cagionare colposamente una lesione o malattia che metta in pericolo la vita della persona offesa ovvero che determini una incapacità di attendere alle ordinarie occupazioni per un tempo superiore a 40 giorni, ovvero se il fatto produce l'indebolimento permanente di un senso o di un organo, in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro	1) Valutazione dei rischi su tutte le attività lavorative svolte dal personale di RADIS: in caso di rischio non valutato o insufficientemente valutato, mancata attuazione e formazione delle procedure del sistema di gestione salute e sicurezza interno; 2) Mancata attuazione del D.Lgs. 81/08 art. 30 co.1 lett. a) rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici. Mancata attuazione del D.Lgs. 81/08 art. 30 co.1 lett. c) attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza.3) Mancata attuazione del D.Lgs. 81/08 art. 30 co.1 lett. d) attività di sorveglianza sanitaria.4)Mancata attuazione del D.Lgs. 81/08 art. 30 co.1 lett. e) attività di informazione e formazione dei lavoratori.5)Mancata attuazione del D.Lgs. 81/08 art. 30 co.1 lett. g) acquisizione di documentazioni e certificazioni obbligatorie di legge.6)Mancata attuazione del D.Lgs. 81/08 art. 30 co.1 lett. h) periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate. 6)Mancata attuazione del D.Lgs. 81/08 art. 30 co.3 Sistema sanzionatorio. 7)Mancata attuazione del D.Lgs. 81/08 art. 30 co.4 Controllo adeguatezza e riesame del sistema.	D.L. - M.C. - RSPP - Diregente procurato, Responsabili Tecnici e preposti.	fino 1000 + interditti ve		attuazione Procedure operative interne emesse ai fini salute e sicurezza nei luoghi di lavoro	

6. Organigramma

Vedi organigramma allegato al DVR.

7. Norme generali di comportamento. La gestione per la Salute e Sicurezza in Adopera

Adopera si impegna a rispettare tutte le prescrizioni normative previste dal D.lgs 81/08 e le altre disposizioni relative alla salute e alla sicurezza sui luoghi di lavoro. A tal fine la società si è dotata di un sistema di gestione interno in linea con la ISO 45001:18 peraltro certificato, implementando specifiche procedure ed istruzioni operative parti integranti di questo MOG.

7.1 Requisiti generali

Adopera assicura l'adempimento di tutti gli obblighi giuridici relativi a:

1) rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;

2) attività di valutazione e di predisposizione delle misure di prevenzione e protezione conseguenti;

3) attività di natura organizzativa quali emergenze di primo soccorso, gestione appalti, riunioni periodiche di sicurezza;

4) attività di sorveglianza sanitaria;

5) attività di informazione e formazione;

6) attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

7) acquisizione di documentazioni e certificazioni obbligatorie;

8) periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate;

9) attività di registrazione delle attività e degli adempimenti;

10) previsione di un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio;

11) attività di riesame e aggiornamento del Modello;

12) sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate dal Modello.

7.2 Politica per la Salute e Sicurezza

L'Amministratore Unico di Adopera dispone che le tematiche relative alla salute e sicurezza sul lavoro siano prioritarie nell'ambito delle politiche aziendali, che ad esse sia posta una particolare attenzione in termini di conformità legislativa, che vengano periodicamente analizzate in ottica di miglioramento continuo e che il personale sia adeguatamente informato e formato in materia.

7.3 Pianificazione

7.3.1 Identificazione del pericolo, valutazione e controllo del rischio

Adopera ha stabilito e mantiene aggiornati nel DVR i criteri per la continua identificazione dei pericoli, la valutazione dei rischi e l'attuazione delle misure di controllo necessarie. Tali attività comprendono:

a) le operazioni ordinarie, straordinarie, periodiche o occasionali (es. manutenzione, pulizia);

b) le attività di tutte le persone che hanno accesso ai luoghi di lavoro (inclusi sub-appaltatori e visitatori);

c) il comportamento umano, le capacità e altri fattori umani;

d) i pericoli originati all'esterno del luogo di lavoro, capaci di avere effetti negativi sulla salute e la sicurezza delle persone che sono sotto il controllo di Adopera all'interno del luogo di lavoro;

e) i pericoli, creati nelle vicinanze del luogo di lavoro da attività correlate al lavoro eseguito sotto il controllo di Adopera;

f) i servizi presenti nei luoghi di lavoro, siano o meno forniti da Adopera;

g) le infrastrutture, gli equipaggiamenti e i materiali presenti sui luoghi di lavoro forniti sia da Adopera che da terzi;

h) cambiamenti o proposte di cambiamenti all'interno dell'organizzazione, delle attività o delle attrezzature/materiali;

i) modifiche riguardanti la gestione della Salute e della Sicurezza nei luoghi di lavoro, compresi cambiamenti provvisori, e i loro impatti sulle operazioni, i processi e le attività;

j) tutti gli obblighi legali applicabili relativi alla valutazione dei rischi e all'implementazione dei necessari controlli;

k) la disposizione delle aree di lavoro, i processi, le installazioni, i macchinari/ equipaggiamenti, le procedure operative e l'organizzazione lavorativa, inclusi il loro adattamento alle capacità umane;

l) le situazioni di emergenza.

Nel determinare i controlli o nel valutare l'adeguatezza dei controlli in essere, Adopera tiene in considerazione tutte le possibilità di riduzione del rischio con il seguente ordine:

- eliminazione del rischio;
- sostituzione del rischio con altro rischio di grado inferiore;
- introduzione di automatismi;
- segnalazioni e/o controlli documentali;
- dispositivi di protezione individuale.

Nel DVR Adopera mantiene registrazione dell'identificazione dei pericoli della valutazione dei rischi e della determinazione dei controlli.

I rischi per la salute e sicurezza sono presi in considerazione nella determinazione degli obiettivi di miglioramento secondo quanto stabilito nella definizione dei criteri di valutazione dei rischi contenuta nel DVR.

7.3.2 Acquisizione di luoghi/impianti e attrezzature di terzi

Adopera assicura la valutazione preventiva dell'idoneità dei luoghi/impianti e attrezzature di terzi prima del loro utilizzo da parte del personale. A tal fine la figura apicale del servizio interessato, in collaborazione con l'RSPP si preoccupa di:

- verificare le attestazioni di conformità in base alla legislazione vigente;
- effettuare un sopralluogo per l'identificazione dei pericoli;
- valutare eventuali rischi per la salute e sicurezza in base ai criteri stabiliti;
- stabilire le responsabilità per la gestione ed il controllo dei dispositivi di prevenzione e protezione.

7.3.3 Prescrizioni legali e altre

L'identificazione e l'accesso ai requisiti legali in tema di salute e sicurezza nei luoghi di lavoro applicabili alla realtà di Adopera, viene assicurata a cura del RSPP attraverso la consultazione di apposite banche dati informatizzate e/o con l'ausilio di società di consulenza specializzate.

Il RSPP collabora inoltre con i preposti e il Datore di Lavoro nella valutazione degli obblighi contenuti nei contratti di appalto, d'opera o di somministrazioni e in quelli dei cantieri temporanei e mobili. Individuata una nuova prescrizione legislativa o nuove disposizioni derivanti dai contratti, il RSPP provvede a:

- verificare se il requisito legale sia applicabile alle proprie attività e ai propri dipendenti;
- comunicare le informazioni, attinenti ai requisiti legali o di altri tipi, alle persone che lavorano sotto il controllo dell'organizzazione o ad altre parti interessate;
- provvedere, ove necessario, all'aggiornamento delle procedure di Sistema e delle registrazioni (ad esempio scadenziari).

7.3.4 Obiettivi e programmi

Nell'ambito della riunione periodica annuale in materia di sicurezza sono definiti, per ogni funzione e livello pertinente all'interno dell'azienda, gli obiettivi derivanti dalla Politica la Salute e Sicurezza. Nel fissare gli obiettivi in materia di Salute e Sicurezza, Adopera assicura che siano presi in considerazione i risultati della valutazione dei rischi e dell'efficacia dei controlli stabiliti. Gli obiettivi sono descritti nel documento "Programma degli interventi", allegato alla valutazione dei rischi e sono posti in relazione a:

1) l'impegno alla prevenzione degli incidenti nei luoghi di lavoro e delle malattie professionali;

2) il rispetto delle prescrizioni legali applicabili e delle altre prescrizioni che Adopera sottoscrive;

3) l'impegno al miglioramento continuo.

Per raggiungere gli obiettivi ed i traguardi vengono definite:

- le fasi necessarie al conseguimento dei risultati attesi;
- le responsabilità relative all'attuazione di ogni singola fase;
- lo sviluppo temporale previsto.

Gli obiettivi sono revisionati a cadenza annuale in occasione della riunione periodica annuale in materia di Sicurezza, programmi con sviluppo temporale inferiore ad un anno o programmi complessi possono prevedere controlli più frequenti in modo da assicurare il corretto svolgimento delle fasi.

7.4 Attuazione e funzionamento

7.4.1 Risorse, ruoli, responsabilità ed autorità

Adopera ha definito le funzioni aziendali, con le rispettive responsabilità e nomine, nonché i collegamenti tra le funzioni (organigramma), in modo da favorire l'efficace raggiungimento degli obiettivi di tutela della salute e sicurezza stabiliti.

L'organizzazione per la salute e sicurezza è formalizzata in apposito organigramma conservato e aggiornato dal Datore di Lavoro e reso disponibile al personale mediante affissione nelle bacheche aziendali.

I compiti e le responsabilità del Datore di Lavoro, del RSPP, del Rappresentate dei Lavoratori per la Sicurezza e dei Preposti sono definiti a livello legislativo. Per quanto riguarda la gestione per la Salute e Sicurezza si specificano i seguenti compiti:

7.4.2 La Direzione per la Sicurezza

E' costituita dal Datore di Lavoro, dal Dirigente Procurato, dal medico competente, dal RSPP ed ha lo scopo di effettuare le riunioni periodiche al fine del monitoraggio, della verifica dell'andamento dei piani per il raggiungimento di obiettivi e programmi, dell'aggiornamento sulla valutazione dei rischi, dell'esame sugli infortuni e mancati infortuni, delle malattie professionali, dell'idoneità dei mezzi di protezione individuale, dell'aggiornamento normativo, documentale e delle procedure, della verifica del piano di informazione e formazione.

7.4.3 Responsabile del Servizio di Prevenzione e Protezione (RSPP)

Gestisce la Documentazione. Convoca, d'accordo con il Datore di Lavoro, la riunione ex art. 35 e ne mantiene registrazione. Coordina le eventuali attività di audit interno. Gestisce le non conformità e le segnalazioni di infortunio, e ne dà comunicazione al Datore di Lavoro. Coordina e gestisce gli obiettivi di miglioramento e ne controlla lo stato di avanzamento. Gestisce le comunicazioni dalle parti interessate, in particolare i reclami in tema di salute e sicurezza. Assicura l'identificazione dei pericoli e la comunicazione dei rischi di interferenze e delle misure di controllo per il personale esterno che opera presso i siti aziendali. Analizza i risultati dei controlli periodici dei preposti. Gestisce e controlla l'efficacia della formazione svolta.

7.4.4 Dirigenti

I Dirigenti collaborano con il RSPP in occasione della valutazione dei rischi, mettendo a disposizione le conoscenze specifiche sui dipendenti, luoghi di lavoro, mezzi e attrezzature del proprio settore.

Assicurano la tempestiva informazione del RSPP a riguardo di nuovi servizi e attività, con particolare riferimento a nuovi contratti.

Informano il Datore di Lavoro, il RSPP e l'OdV di ogni anomalia sulla salute e sicurezza riscontrata in azienda, compresi gli infortuni.

Informano il Datore di Lavoro, il RSPP e l'OdV di ogni eventuale necessità di addestramento, formazione e sensibilizzazione dei dipendenti che operano nel proprio settore.

Collaborano con il Datore di Lavoro e il RSPP nella definizione delle azioni correttive e preventive necessarie per il mantenimento e miglioramento delle condizioni di salute e sicurezza nel proprio settore.

Collaborano con il Datore di Lavoro e il RSPP nell'individuazione e gestione degli obiettivi di miglioramento.

Adopera ha individuato attualmente un dirigente ai fini sicurezza nei settori infrastrutture/verde, impianti, edifici/cimiteri munito di procura notarile.

7.4.5 Preposti

I Preposti di primo grado coordinano i lavoratori e allo stesso tempo svolgono attività operative.

I Preposti sorvegliano le attività nei settori di competenza controllando la messa in atto delle disposizioni di prevenzione e controllo dei rischi stabilite nel DVR.

Informano il RSPP di ogni anomalia sulla salute e sicurezza riscontrata in azienda, compresi gli infortuni e i mancati incidenti.

I Preposti controllano il rispetto delle modalità operative e dei comportamenti stabiliti, sulla base di apposite check list compilate con la frequenza.

In Adopera i preposti sono stati specificatamente nominati e formati.

7.4.6 Rappresentante dei lavoratori per la Sicurezza

Partecipa all'identificazione dei pericoli, alla valutazione dei rischi e alla determinazione dei controlli. Approva il DVR. Si fa carico di riportare alla Direzione eventuali osservazioni o richieste dei dipendenti in materia di salute e sicurezza. Partecipa alla Riunione Annuale sulla Sicurezza.

7.4.7 Competenza, consapevolezza e addestramento

Adopera definisce, le competenze minime in tema di salute e sicurezza che sono necessarie a svolgere le specifiche mansioni. Tali competenze sono riviste in occasione della riunione periodica annuale della sicurezza e costituiscono uno degli elementi per la corretta assunzione del personale e per la corretta definizione dei fabbisogni formativi.

Per informazione si intende il complesso delle attività dirette a fornire conoscenze utili all'identificazione, alla riduzione e alla gestione dei rischi in ambienti di lavoro e degli aspetti e impatti ambientali ed energetici.

Per formazione si intende: processo educativo attraverso il quale trasferire ai lavoratori e ad altri soggetti del sistema, conoscenze e procedure utili all'acquisizione di competenze per:

- lo svolgimento in sicurezza dei rispettivi compiti in azienda, nel rispetto dell'ambiente e dell'efficienza energetica dei propri compiti in azienda
- l'identificazione, riduzione e gestione dei rischi e degli aspetti e impatti ambientali/energetici.

Per addestramento si intende il complesso delle attività dirette a far apprendere ai lavoratori l'uso corretto di attrezzature, macchine, impianti, sostanze, dispositivi, anche di protezione individuale, e le procedure di lavoro.

Le esigenze formative nascono dalla valutazione del possesso delle competenze minime individuate e da necessità di addestramento e formazione derivanti da modifiche di carattere organizzativo, nuovi servizi, impianti e attrezzature. Le esigenze formative sono descritte nel "Piano della formazione della Sicurezza", inserito all'interno del Programma degli interventi.

La formazione è progettata tenendo conto degli obblighi normativi imposti dall'accordo Stato Regioni.

Il Piano della formazione viene attuato a cura del RSPP che mantiene registrazione dell'attività di addestramento e formazione svolta internamente o a cura di Ente esterno.

In attuazione dell'accordo Stato Regioni per le attrezzature di lavoro quali ad esempio i sollevatori a forche, è prevista, entro le scadenze indicate nell'accordo stesso, l'abilitazione all'uso delle stesse.

Nell'ambito della riunione periodica annuale della sicurezza, il Datore di Lavoro verifica lo stato di avanzamento del Piano di formazione stabilito, eventuali necessarie modifiche ed integrazioni.

Per i nuovi assunti è assicurata la formazione tramite affiancamento a personale esperto, la consegna di materiale informativo sulla salute e sicurezza, e la formazione sui rischi specifici della/e mansione/i affidata/e (quest'ultima organizzata dal RSPP in base alle disponibilità).

7.4.8 Comunicazione, partecipazione e coinvolgimento

Con riferimento ai rischi per la salute e sicurezza e alla gestione della Salute e Sicurezza, Adopera predispone idonei mezzi per:

- assicurare la comunicazione interna tra i diversi livelli e funzioni aziendali;
- comunicare con i fornitori e i visitatori che accedono ai luoghi di lavoro che Adopera controlla;
- ricevere, documentare e rispondere a rilevanti comunicazioni che pervengono dalle parti interessate.

Adopera assicura la partecipazione e coinvolgimento dei dipendenti nelle fasi di:

1) identificazione dei pericoli, valutazione dei rischi e determinazione dei controlli; a tal fine il Rappresentante dei Lavoratori approva il DVR dopo averne verificata l'adeguatezza;

2) approvazione degli obiettivi e dei traguardi. A tal fine il Rappresentante dei Lavoratori partecipa alla riunione periodica annuale della sicurezza;

4) gestione di modifiche e cambiamenti che hanno effetti sulla salute e sicurezza. Ogni modifica comporta l'aggiornamento del DVR e la comunicazione/formazione dei dipendenti rispetto alle misure di contenimento e controllo stabilite.

I lavoratori, attraverso le rappresentanze sindacali, nominano un numero adeguato di propri Rappresentati, in base a quanto previsto dal D.Lgs 81/08 e ss.mm.ii. che li rappresentano nelle questioni attinenti la salute e la sicurezza.

7.4.9 Documentazione

La documentazione include:

- gli obiettivi di miglioramento;
- documenti e registrazioni che Adopera ritenga necessari per condurre efficacemente la pianificazione ed il controllo dei processi in materia digestione per la Salute e Sicurezza;
- Procedure di sistema (PRO) e moduli operativi (MOD) relativi al sistema ISO 45001:18 ad oggi certificato.

7.4.10 Controllo dei documenti

I documenti sono emessi e controllati in modo da assicurare che:

- la documentazione appropriata sia sempre disponibile quando e dove è necessaria;
- la documentazione obsoleta sia prontamente eliminata o, comunque, siano evidenziati i casi per i quali rimane, in via transitoria, ancora valida;

- ogni documento sia verificato ed autorizzato prima della diffusione;
- ogni modifica ad un documento sia evidenziata e approvata dalle medesime funzioni che hanno emesso la versione precedente;
- non siano diffusi ed utilizzati documenti non autorizzati;
- l'archiviazione sia effettuata secondo criteri atti a garantire la sicurezza e la reperibilità dei documenti;
- assicurare che la documentazione di origine esterna definita da Adopera come necessaria per la pianificazione e la gestione del Sistema Integrato sia identificata e la sua distribuzione sia controllata.

7.4.11 Controllo operativo

Nell'ambito dell'identificazione dei pericoli, Adopera individua le attività che sono associate ai rischi per la salute e sicurezza e determina i controlli necessari per minimizzare e controllare il rischio, compresa la gestione delle modifiche.

Per tali operazioni e attività Adopera, nel DVR:

a) identifica i controlli operativi;

b) stabilisce le modalità dei controlli dei rischi associati alla presenza di visitatori e appaltatori;

c) stabilisce le regole per gestire situazioni nelle quali l'assenza delle stesse può costituire pericolo per la salute e sicurezza e scostamento rispetto alla Politica e agli Obiettivi stabiliti;

d) pone criteri operativi per gestire situazioni nelle quali l'assenza delle stesse può costituire pericolo per la salute e sicurezza e scostamento rispetto alla Politica e agli Obiettivi stabiliti.

7.4.12 Preparazione alle emergenze e risposta

Adopera individua le possibili situazioni di emergenza e stabilisce le modalità di risposta in apposite procedure.

Nel DVR sono identificati i pericoli connessi alle emergenze che possono verificarsi durante le normali attività, ne sono valutati i rischi e vengono stabilite le procedure di prevenzione e di risposta necessarie a contenere il rischio.

Per quanto attiene ai luoghi di lavoro viene svolta una specifica analisi del Rischio incendio, in base alla quale vengono definite procedure di emergenza (Piani di emergenza) periodicamente sperimentate per verificarne l'adeguatezza.

Il personale incaricato di gestire l'emergenza (addetto antincendio) viene formato anche in base a quanto richiesto dalla legislazione applicabile. Il RSPP assicura che:

- a tutti i dipendenti venga fornita adeguata formazione sulla preparazione alle emergenze (Piano di formazione);
- gli addetti antincendio siano individuati e adeguatamente formati (identificazione nominativi nel DVR e raccolta attestati di formazione);
- le prove di emergenza siano condotte a livello annuale (registrazione e conservazione dell'esito delle prove).

In fase seguente ad eventuali emergenze occorse la Direzione analizza l'efficacia delle procedure di risposta stabilite e attiva, se necessario, azioni correttive per la revisione o il miglioramento delle stesse.

7.5 Controllo

7.5.1 Monitoraggio e misurazione delle performance

Per assicurare il costante monitoraggio dei processi in merito agli aspetti legati alla salute e alla sicurezza nei luoghi di lavoro, Adopera predispone una apposita check list "Sicurezza". Tale check-list è oggetto di costante aggiornamento da parte del Responsabile del Sistema sulla base delle osservazioni che possono provenire dal Datore di lavoro, dal Responsabile del Servizio Prevenzione e Protezione, dal Rappresentante dei Lavoratori per la Sicurezza e dai lavoratori, dal Medico Competente o dall'OdV. La compilazione di tale check-list è assegnata ai Preposti con frequenza mensile. Eventuali scostamenti rilevati in occasione dei controlli dei preposti sono gestiti a cura del RSPP secondo quanto descritto nel capitolo riservato alle non conformità e azioni correttive.

In considerazione di peculiari situazioni e specifiche problematiche legate alla salute e alla sicurezza delle diverse aree, la check list di riferimento può contenere quesiti di dettaglio della specifica area.

Adopera adotta inoltre analisi e indicatori in grado di monitorare e misurare le prestazioni in tema di salute e sicurezza, tra cui:

- analisi degli infortuni;
- analisi delle comunicazioni dalle parti interessate, tra cui i dipendenti;
- analisi delle comunicazioni dalle parti interessate, tra cui i Fornitori e subappaltatori che svolgono attività presso le sedi di Adopera;
- analisi dei Report delle verifiche ispettive;
- monitoraggio dello stato di avanzamento degli obiettivi fissati;
- monitoraggio dell'efficacia dei controlli periodici svolti a cura dei preposti sulla base di apposite check list.

I risultati dell'analisi dei dati vengono presentati periodicamente in occasione della riunione periodica della sicurezza e degli incontri trimestrali tra RSPP, RLS e

Delegato alla sicurezza. Tali risultati vengono utilizzati per intraprendere le opportune azioni correttive e preventive.

7.5.2 Valutazione di conformità

Adopera, coerentemente con l'impegno alla conformità legislativa stabilito nella politica, effettua periodiche valutazioni alla conformità con i requisiti legali applicabili in tema di salute e sicurezza nei luoghi di lavoro e ad eventuali altri requisiti sottoscritti. Tali verifiche vengono effettuate dal RSPP nell'ambito delle verifiche ispettive interne e la loro esecuzione può essere demandata a società di consulenza esterne. Per la gestione delle registrazioni (Piani di verifica, Rapporti di verifica) si rimanda al capitolo delle verifiche ispettive interne.

7.5.3 Analisi degli incidenti, non conformità, azioni correttive e preventive

7.5.3.1 Analisi degli incidenti

Adopera registra, indaga e analizza gli incidenti in modo da:

- determinare le implicite carenze rispetto alle condizioni di salute e sicurezza nei luoghi di lavoro, che possono essere la causa o aver contribuito all'avvenimento dell'incidente;
- individuare il bisogno di azione correttiva;
- individuare opportunità di azione preventiva;
- individuare opportunità di miglioramento continuo;
- comunicare i risultati di tale indagine.

Le indagini sono eseguite in modo tempestivo. Il Datore di Lavoro e il RSPP individuano le seguenti situazioni per determinare le implicite carenze rispetto alle condizioni di salute e sicurezza nei luoghi di lavoro e stabilire le azioni correttive o preventive necessarie ad evitarne il ripetersi:

- incidenti occorsi con infortunio.

L'analisi viene formalizzata su specifico documento. Eventuali azioni correttive o preventive sono gestite in base a quanto stabilito nei paragrafi seguenti.

L'esito della valutazione degli incidenti e le azioni correttive e preventive intraprese vengono presentate nelle riunioni tra Direttori Tecnici e comunque nella Riunione Annuale della Sicurezza a cura del RSPP. Dall'analisi complessiva degli incidenti occorsi possono nascere ulteriori opportunità di miglioramento. La comunicazione ai dipendenti degli incidenti occorsi e delle azioni intraprese è assicurata dalla partecipazione del Rappresentante dei Lavoratori alla Riunione Annuale della Sicurezza.

Gli incidenti con infortunio sono comunicati dai dipendenti con consegna del certificato medico all'Ufficio Amministrazione che provvede a:

- comunicare l'accaduto la figura apicale del servizio interessato;
- comunicare l'accaduto al RSPP per l'analisi delle cause come sopra descritto e l'attivazione delle necessarie azioni;
- inoltrare la denuncia di infortunio e il certificato medico agli Enti competenti in base a quanto disposto dalle vigenti normative;
- aggiornare il registro infortuni;
- conservare copia delle comunicazioni in apposto fascicolo;
- informare l'OdV.

Il RSPP analizza l'evento e dispone eventuali trattamenti immediati registrando le decisioni. Eventuali azioni correttive o preventive sono gestite in base a quanto stabilito nei paragrafi seguenti.

7.5.3.2 Non conformità azioni correttive e preventive

Adopera gestisce le non conformità riscontrate o che potrebbero essere riscontrate e le azioni correttive e preventive in tema di salute e sicurezza. Per non conformità si intende qualsiasi scostamento rispetto alle istruzioni, alle procedure operative stabilite ed ai requisiti legali. Le non conformità possono essere identificate:

- a cura degli operatori nello svolgimento quotidiano delle attività. In questo caso gli operatori sono stati sensibilizzati alla pronta comunicazione della non conformità al RSPP o al Preposto che compilano specifico modulo;
- a cura dei preposti durante le verifiche periodiche della sicurezza. In questo caso la non conformità viene registrata sulla check list di controllo che viene consegnata al responsabile del Sistema.

L'RSPP analizza la non conformità e stabilisce il trattamento più idoneo con l'eventuale collaborazione di personale o altri uffici interessati.

In fase di analisi di ogni non conformità riscontrata e in fase di valutazione annuale delle non conformità gestite, il RSPP, in accordo con la Direzione, stabilisce la necessità di attivazione di azioni correttive per eliminare la causa della non conformità ed evitarne così il ripetersi.

Eventuali azioni preventive vengono inoltre intraprese per eliminare le cause di potenziali non conformità.

Qualora le azioni correttive e preventive individuino rischi o controlli nuovi o modificati, il RSPP effettua una valutazione preventiva del rischio. Le azioni correttive e preventive vengono poste in relazione all'entità del problema riscontrato e sono commisurate al rischio per la salute e sicurezza.

Ogni necessaria modifica viene messa in atto dal RSPP con appropriato aggiornamento della documentazione, con conseguente tempestiva comunicazione alla Direzione e all'OdV.

7.5.4 Controllo delle registrazioni

Adopera mantiene registrazioni per dimostrare la conformità alla normativa e per dare evidenza dei risultati raggiunti.

In generale:

- le registrazioni cartacee sono conservate in appositi contenitori archiviati presso gli Uffici.
- le registrazioni elettroniche sono salvate su server. Apposite procedure di salvataggio periodico, avviate in automatico, garantiscono la conservazione delle informazioni.

L'Area Amministrazione sotto la supervisione del Dirigente procurato, garantisce il salvataggio periodico delle registrazioni elettroniche su nastro magnetico, attraverso apposite procedure di back up.

7.5.5. Verifiche ispettive interne

RSPP svolge periodicamente delle verifiche ispettive interne, al fine di rilevare eventuali difformità o situazioni potenzialmente non conformi nei luoghi di lavoro.

RSPP effettua periodicamente, con il supporto di Consulente esterno sicurezza, l'analisi dei documenti aziendali relativi alla sicurezza sul lavoro, per mantenerli costantemente allineati alle disposizioni vigenti.

Qualora a seguito delle verifiche periodiche suddette emergessero delle Non Conformità, RSPP si attiva per mettere in campo le relative Azioni Correttive, se del caso concordate con la figura apicale del servizio interessato dalla NC.

Dei risultati delle verifiche periodiche operative e documentali si tiene conto in fase di Riunione annuale per la sicurezza.

7.5.5. Verifiche ispettive esterne

Adopera ha implementato apposite procedure volte a vigilare sul rispetto da parte di propri fornitori/partner dei precetti in materia di sicurezza e salute nei luoghi di lavoro anche con apposite clausole contrattuali.

7.6.1 Riunione Annuale della Sicurezza

Il risultato della Riunione Annuale della Sicurezza che, in conformità con quanto previsto dalla legislazione vigente, viene svolta a cura di:

- datore di lavoro;
- dirigente procurato;
- responsabile del servizio di prevenzione e protezione dai rischi;
- medico competente;
- rappresentante dei lavoratori per la sicurezza.

Nel corso della riunione il datore di lavoro sottopone all'esame dei partecipanti:

1) il Documento di Valutazione dei Rischi;

2) l'andamento degli infortuni e delle malattie professionali e della sorveglianza sanitaria;

3) i criteri di scelta, le caratteristiche tecniche e l'efficacia dei dispositivi di protezione individuale;

4) i programmi di informazione e formazione dei dirigenti, dei preposti e dei lavoratori ai fini della sicurezza e della protezione della loro salute.

La riunione ha luogo almeno una volta all'anno e in occasione di eventuali significative variazioni delle condizioni di esposizione al rischio, compresa la programmazione e l'introduzione di nuove tecnologie che hanno riflessi sulla sicurezza e salute dei lavoratori.

Della riunione viene redatto un verbale che viene archiviato e messo a disposizione dei partecipanti dal RSPP.

Alle riunioni ex art. 35 D.lgs. 81/2008 può partecipare anche l'OdV.

8. Sanzioni disciplinari

In ordine al mancato rispetto delle prescrizioni in materia di salute e sicurezza sul lavoro contenute nel presente Modello, nelle istruzioni e procedure aziendale e comunque impartite dalle funzioni aziendali a ciò abilitate, si rinvia al paragrafo specifico del presente MOG intitolata "Sanzioni disciplinari".

9. Verifiche dell'Organismo di vigilanza e flusso di comunicazione nei suoi confronti

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i Reati di cui all'art. 25 septies del Decreto sono i seguenti:

1) svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la loro efficacia a prevenire la commissione dei Reati di cui all'art. 25 septies del Decreto. Con riferimento a tale punto l'OdV - avvalendosi

eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà ai soggetti competenti di Adopera eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sulla tutela della salute e sicurezza sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;

2) proporre e collaborare alla predisposizione delle istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;

3) esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti, l'OdV può:

- partecipare agli incontri della Direzione ed alla Riunione Annuale;
- incontrare periodicamente l'RSPP;
- accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti. Adopera istituisce – con il coinvolgimento del RSPP – a favore dell'OdV flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli infortuni, delle criticità nonché notizie di eventuali malattie professionali accertate o presunte.

L'OdV, nell'espletamento delle attività di cui sopra, può avvalersi di tutte le risorse competenti nell'ambito di Adopera.

REATI AMBIENTALI

La presente Parte Speciale si riferisce ai reati ambientali di cui all'art. 25-undecies del D. Lgs. 231/2001 (di seguito anche Decreto), limitatamente alle attività sensibili che possono configurarsi in capo a Centro Iperbarico.

La presente parte speciale disciplina la responsabilità amministrativa delle persone giuridiche chiamate a rispondere dell'illecito conseguente alla consumazione, nel loro interesse o vantaggio, dei reati ambientali indicati nell'art. 25 undecies, commessi dagli apicali dell'Ente o da soggetti sottoposti.

Il legislatore ha introdotto la responsabilità degli enti da reati ambientali a partire dal D.Lgs. 121/2011, decreto di attuazione della Direttiva 2008/99/CE sulla tutela

penale dell'ambiente e della Direttiva 2009/123/CE sull'inquinamento marino provocato dalle navi.

Con l'emanazione della L. n. 68/2015, recante "Disposizioni in materia di delitti contro l'ambiente", in vigore dal 29 maggio 2015, è stato ampliato il catalogo dei reati presupposto di cui all'art. 25-undecies del D. Lgs. 231/2001. La L. 68 ha introdotto un nuovo titolo VI bis (dei delitti contro l'ambiente) nel Codice Penale e modificato alcuni provvedimenti normativi, tra cui il D.Lgs. 231/01 introducendo alcune nuove fattispecie di reato, in particolare il reato di inquinamento e disastro ambientale anche colposo.

Con la pubblicazione del testo del D.L. 8 agosto 2025, n. 116, coordinato con la Legge di conversione 3 ottobre 2025, n. 147 "Disposizioni urgenti per il contrasto alle attività illecite in materia di rifiuti, per la bonifica dell'area denominata Terra dei fuochi e per l'istituzione del Dipartimento per il Sud, nonché in materia di assistenza alla popolazione colpita da eventi calamitosi ", sono entrate in vigore, dal 8 ottobre 2025, disposizioni normative di particolare impatto sulla Responsabilità amministrative degli Enti in ambito "reati ambientali".

L'obiettivo della norma mira a intensificare il contrasto ai reati ambientali e la tutela della salute pubblica e l'ambiente, per impedire le attività illecite in materia di rifiuti su tutto il territorio nazionale e, per incentivare gli interventi di bonifica nell'area denominata Terra dei fuochi.

La nuova normativa ha comportato modifiche al Testo Unico ambientale (D. Lgs. 152/2006), al Codice penale, al D. Lgs. n. 49/2014 (sui RAEE) ed al D. Lgs. 231/2001.

Di particolare interesse:

– l'introduzione di nuove fattispecie di reato ambientale (es. abbandono di rifiuti in casi particolari) e di nuove sanzioni accessorie (es. sospensione della licenza per il trasporto beni conto terzi e confisca veicolo);

- l'ampliamento delle condotte sanzionabili e l'inasprimento del quadro sanzionatorio, mediante la previsione di pene detentive, nei casi più gravi, e aggravanti per i fatti commessi nell'ambito di un'attività d'impresa (con responsabilità per omessa vigilanza) o in siti contaminati;

In relazione all'art. 25 undecies, così come modificato, in particolare si segnala:
- l'avvenuta introduzione dei reati di:
- impedimento del controllo - art. 452 septies c.p.;
- omessa bonifica - art. 452 terdecies c.p.;

- attività organizzate per il traffico illecito di rifiuti (riferibile in precedenza al reato di cui all'art. 260 c. amb.) - art. 452 quaterdecies c.p.;
- abbandono di rifiuti non pericolosi in casi particolari e di rifiuti pericolosi - art. 255 bis e 255 ter c.amb.;
- attività di gestione di rifiuti non autorizzata - art. 256 c.amb.;
- combustione illecita di rifiuti - art. 256 bis c.amb.;
- la modifica di fattispecie già previste dall'art. 25 undecies.

E' il caso del reato di traffico illecito di rifiuti (ex art. 259 c.amb.), la cui rubrica è stata innovata in spedizione illegale di rifiuti, trasformato da fattispecie contravvenzionale in delitto.

- la previsione di un'attenuante di cui all'art. 25 undecies c. 2 bis, che comporta una significativa mitigazione delle sanzioni in caso di commissione colposa di alcuni delitti (abbandono di rifiuti non pericolosi in casi particolari, abbandono di rifiuti pericolosi, attività di gestione di rifiuti non autorizzata e spedizione illegale di rifiuti) se commessi per colpa;
- l'estensione del catalogo di reati per i quali può essere disposta, ai sensi dell'art. 34 D. Lgs. 159/2011, la misura di prevenzione dell'amministrazione giudiziaria dei beni connessi
ad attività economiche e delle aziende, includendovi pure alcune ipotesi di illeciti penali in materia di rifiuti.

CENTRO IPERBARICO SRL ritiene che i protocolli e procedure in materia ambientale con particolare riferimento alle procedure ispirate alla ISO 14001/04 siano idonee a gestire il rischio della commissione anche dei cd. ecoreati di cui alla L 68/15.

1. Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c. p.)

L'art. 727-bis c.p. punisce, salvo che il fatto costituisca più grave reato, diverse tipologie di condotte illecite nei confronti di specie animali e vegetali selvatiche protette e cioè:

a) di chi, fuori dai casi consentiti, uccide, cattura o detiene esemplari appartenenti ad una specie animale selvatica protetta (comma l);

b) di chi, fuori dai casi consentiti, distrugge, preleva o detiene esemplari appartenenti ad una specie vegetale selvatica protetta (comma 2).

Il legislatore delegato, peraltro, adeguandosi alle previsioni comunitarie (art. 3, par. l, lett. f) della direttiva n. 2008/99/CE), esclude la configurabilità del reato nei

casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie.

Ai fini dell'applicazione dell'articolo 727-bis c.p., per "specie animali o vegetali selvatiche protette" si intendono quelle indicate nell'allegato IV della direttiva 92/43/CE e nell'allegato I della direttiva 2009/147 /CE (art. l, comma 2, D. Lgs. 121/2011).

Il richiamo riguarda, da un lato, la direttiva 92/43/CEE del Consiglio, del 21 maggio 1992, relativa alla conservazione degli habitat naturali e seminaturali e della flora e della fauna selvatiche (c.d. direttiva «Habitat») e, dall'altro, la direttiva 2009/147/CE del Parlamento Europeo e del Consiglio del 30 novembre 2009, concernente la conservazione degli uccelli selvatici (che abroga la direttiva 79/409/CEE la c.d. direttiva «Uccelli»).

2. Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis cod. pen.)

L'art. 733-bis c.p. punisce chiunque, fuori dai casi consentiti, distrugge un habitat all'interno di un sito protetto o comunque lo deteriora compromettendone lo stato di conservazione.

Ai fini dell'applicazione dell'art. 733-bis c.p. per "habitat all'interno di un sito protetto" si intende qualsiasi habitat di specie per le quali una zona sia classificata come zona di protezione speciale a norma dell'art. 4, paragrafi l o 2, della direttiva 2009/147 /CE, o qualsiasi habitat naturale o un habitat di specie per cui un sito sia designato come zona speciale di conservazione a norma dell'art. 4, paragrafo 4, della direttiva 92/43/CEE».

La delimitazione dell'ambito oggettivo di applicazione della fattispecie penale in base alla vigente normativa italiana deve essere svolta in forza delle seguenti disposizioni: a) D.M. ambiente e tutela del territorio 3 settembre 2002 "Linee guida per la gestione dei siti Natura 2000" (G.U. 24 settembre 2002, n. 224); b) d.P.R. 8 settembre 1997, n. 357 "Regolamento recante attuazione della direttiva 92/43/CEE relativa alla conservazione degli habitat naturali e seminaturali, nonché della flora e della fauna selvatiche" (G.U. 23 ottobre 1997, n. 248), come modificato dal d.P.R. 12 marzo 2003, n. 120 (G.U. n.124 del 30 maggio 2003); c) D.M. ambiente e tutela del territorio e del mare 14 marzo 2011 (G.U. 4 aprile 2011, n. 77, S.O. n. 90) contenente il "Quarto elenco aggiornato dei siti di importanza comunitaria per la regione biogeografica alpina in Italia ai sensi della Direttiva 92/43/CEE"; d) D.M. ambiente e tutela del territorio e del mare 14 marzo 2011 (G.U. 4 aprile 2011, n. 77, S.O. n. 90) contenente il "Quarto elenco aggiornato dei siti di importanza comunitaria per la regione biogeografica mediterranea in Italia ai sensi della Direttiva 92/43/CEE"; e) D.M. ambiente e tutela del territorio e del mare 14 marzo 2011 (G.U. 4 aprile 2011, n. 77, S.O. n. 90) contenente il "Quarto elenco

aggiornato dei siti di importanza comunitaria per la regione biogeografica continentale in Italia ai sensi della Direttiva 92/43/CEE"; f) D.M. ambiente e tutela del territorio e del mare 17 ottobre 2007 (G.U. 6 novembre 2007, n. 258) recante "Criteri minimi uniformi per la definizione di misure di conservazione relative a Zone speciali di conservazione (ZSC) e a Zone di protezione speciale (ZPS)", come da ultimo modificato dal D.M. ambiente e tutela del territorio e del mare 22 gennaio 2009 (G.U. 10 febbraio 2009, n. 33); g) D.M. ambiente e tutela del territorio e del mare 19

giugno 2009 (G.U. 9 luglio 2009, n. 157) contenente l' "Elenco delle zone di protezione speciale (ZPS) classificate ai sensi della Direttiva 79/409/CEE"

3. Fattispecie di reato di cui all'art.137 Codice Ambientale

Risultano rilevanti per le finalità di cui al Decreto le seguenti condotte:

a) scarico di acque reflue industriali senza autorizzazione o con autorizzazione sospesa o revocata

L'art. 137, commi 2 e 3, Cod. Amb. è sanziona la condotta di chiunque effettui nuovi scarichi di acque reflue industriali contenenti sostanze pericolose senza osservare le prescrizioni dell'autorizzazione o le altre prescrizioni delle autorità competenti ai sensi degli articoli 107, comma 1, e 108, comma 4 Cod. Amb.

Si precisa che in relazione alle condotte di cui sopra, per "sostanze pericolose" si intendono quelle espressamente indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza Cod. Amb. a cui si fa rinvio.

b) scarico di acque industriali eccedenti limiti tabellari

L'articolo 25-undecies, comma 2, primo periodo, del Decreto e 137, comma 5, Cod. Amb. prevedono l'irrogazione di sanzioni nei confronti di chiunque nell'effettuare uno scarico di acque reflue industriali superi i limiti fissati dalla legge o dalle autorità competenti ai sensi dell'art. 107 Cod. Amb.

Si precisa che tale condotta rileva esclusivamente in relazione alle sostanze indicate nella tabella 5 dell'Allegato 5 alla parte terza del Codice dell'Ambiente e che i valori limite a cui fa riferimento la suddetta norma sono indicati alle tabelle 3 e 4 dello stesso Allegato S.

Anche la criminalizzazione di tale condotta è punita con una sanzione pecuniaria più elevata qualora vengano superati particolari valori limite fissati per le sostanze di cui alla tabella 3/A dell'Allegato 5 al Codice dell'Ambiente.

c) violazione del divieto di scarico sul suolo, nel suolo e nelle acque sotterranee

All'art. 137 comma 11, primo periodo è sanzionata la condotta di chiunque, nel caso di scarico sul suolo, di cui alla tabella 4 dell'allegato 5 alla Parte terza del Codice dell'Ambiente, non osservi i divieti di scarico previsti dagli artt. 103 e 104 Cod. Amb.

Ai sensi dell 'art. 74 comma l lett. ff) Cod. Amb. per "scarico" si intende "qualsiasi immissione effettuata esclusivamente tramite un sistema stabile di collettamento che collega senza soluzione di continuità il ciclo di produzione del refluo con il corpo ricettore acque superficiali, sul suolo, nel sottosuolo e in rete fognaria, indipendentemente dalla loro natura inquinante, anche sottoposte a preventivo trattamento di depurazione".

d) violazione del divieto di scarico in mare da parte di navi e aereomobili di sostanze vietate;

Ai sensi dell'art. 137, comma 13, Cod. Amb. è punito lo scarico da parte di navi od aeromobili nelle acque del mare contenente sostanze o materiali per i quali è imposto il divieto assoluto di sversamento ai sensi delle disposizioni contenute nelle convenzioni internazionali vigenti in materia e ratificate dall'Italia, salvo che siano in quantità tali da essere resi rapidamente innocui dai processi fisici, chimici e biologici, che si verificano naturalmente in mare e purché in presenza di preventiva autorizzazione da parte dell'autorità competente.

4. Fattispecie di reato di cui all'art. 256 Cod.Amb.

L'art. 256 Cod. Amb. sanziona penalmente una pluralità di condotte che, configurandosi prevalentemente come violazione di disposizioni normative relative alla gestione di rifiuti, sono potenzialmente lesive dell'ambiente.

Le attività illecite previste dall'art. 256 Cod. Amb. Sono riconducibili alla categoria dei "reati di pericolo astratto", per i quali la messa in pericolo del bene giuridico protetto (i.e. l'ambiente) è presunta dal legislatore, senza necessità di verificare concretamente la sussistenza del pericolo. La semplice violazione delle norme relative alle attività di Gestione dei Rifiuti o l'impedimento dei controlli predisposti in via amministrativa costituiscono, quindi, di per sé fattispecie di reato punibili.

Assumono rilevanza ai fini del Decreto:

a) Gestione non autorizzata di Rifiuti ai sensi dell'art. 256 primo comma Cod. Amb.

Il primo comma dell'art. 256 Cod. Amb. punisce una pluralità di condotte connesse alla Gestione non autorizzata dei Rifiuti, ossia le attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di Rifiuti di qualsiasi genere - pericolosi e non pericolosi - poste in essere in mancanza della specifica

autorizzazione, iscrizione o comunicazione prevista dagli artt. da 208 a 216 Cod. Amb .

Si precisa che, ai sensi dell'art. 193 comma 9 Cod . Amb., per le "attività di trasporto" non rilevano gli spostamenti di Rifiuti all'interno di un'area privata.

Una responsabilità del Produttore potrebbe, tuttavia, configurarsi a titolo di concorso nel reato. Ciò, non solo in caso di conoscenza della natura illecita dell'attività di Gestione dei Rifiuti concessa in appalto, ma anche in caso di violazione di specifici obblighi di controllo sul soggetto incaricato alla raccolta e smaltimento dei Rifiuti prodotti.

Si tenga, infatti, presente che tutti i soggetti coinvolti nel complesso delle attività di Gestione dei Rifiuti - tra cui anche il Produttore - sono tenuti, non solo al rispetto delle disposizioni normative relative al proprio ambito di attività, ma anche ad un controllo sulla corretta esecuzione delle attività precedenti o successive alla propria. Di conseguenza, il Produttore è tenuto a controllare che il soggetto a cui venga affidata la raccolta, il trasporto o lo smaltimento dei Rifiuti prodotti svolga tali attività in modo lecito. In caso contrario, l'inosservanza di obblighi precauzionali potrebbe determinare un "concorso colposo nel reato doloso".

b) gestione di discarica non autorizzata ai sensi dell'art. 256 terzo comma Cod. Amb.

Il comma terzo della stessa disposizione punisce chiunque realizzi o gestisca una Discarica non autorizzata, con specifico aggravamento di pena nel caso in cui la stessa sia destinata allo smaltimento di Rifiuti Pericolosi.

In particolare, si precisa che nella definizione di Discarica non rientrano "gli impianti in cui i rifiuti sono scaricati al fine di essere preparati per il successivo trasporto in un impianto di recupero, trattamento o smaltimento, e lo stoccaggio di rifiuti in attesa di recupero o trattamento per un periodo inferiore a tre anni come norma generale, o lo stoccaggio di rifiuti in attesa di smaltimento per un periodo inferiore a un anno".

La Corte di Cassazione ha peraltro chiarito che deve considerarsi "discarica" anche la zona interna al luogo di produzione dei Rifiuti destinata stabilmente allo smaltimento degli stessi (Cass. Pen. Sent. 26 gennaio 2007 n. 10258).

Al fine di determinare la condotta illecita di realizzazione e gestione di discarica non autorizzata devono quindi sussistere le seguenti condizioni:

- una condotta ripetuta nel tempo di accumulo dei rifiuti in un'area o anche il semplice allestimento dell'area attraverso lo spianamento o la recinzione del terreno;

- il degrado dell'area stessa, consistente nell'alterazione permanente dello stato dei luoghi, nonché
- il deposito di una quantità consistente di rifiuti.

Ai fini della configurabilità della "gestione abusiva", infine , si deve dar luogo ad un'attività autonoma, successiva alla realizzazione, che implichi l'attivazione di un'organizzazione di mezzi e persone volti al funzionamento della Discarica stessa.

c) Miscelazione di Rifiuti Pericolosi ai sensi dell'art. 256 quinto comma Cod. Amb.

Sono punite, ai sensi del comma quinto dell'art. 256 Cod. Amb., le attività non autorizzate di Miscelazione dei Rifiuti aventi differenti caratteristiche di pericolosità ovvero di Rifiuti Pericolosi con Rifiuti non Pericolosi.

Si ricorda che la Miscelazione dei Rifiuti Pericolosi - che non presentino la stessa caratteristica di pericolosità, tra loro o con altri rifiuti, sostanze o materiali - è consentita solo se espressamente autorizzata ai sensi e nei limiti di cui all'art. 187 Cod. Amb. Tale condotta pertanto assume rilevanza penale solo se eseguita in violazione di tali disposizioni normative.

Il reato in oggetto può essere commesso da chiunque abbia la disponibilità di rifiuti pericolosi e non pericolosi.

d) deposito temporaneo di rifiuti sanitari pericolosi ai sensi dell'art. 256 sesto comma primo periodo del Cod. Amb.

Può considerarsi integrata ai sensi del comma sesto dell'art. 256 del Cod. Amb., la violazione del divieto di deposito temporaneo di rifiuti sanitari pericolosi presso il luogo di produzione previsto dall'art 227 Cod. Amb.

Si precisa che il reato può considerarsi integrato qualora sussistano le seguenti condizioni:

a) si tratti di rifiuti sanitari pericolosi a rischio infettivo compresi nell'elenco esemplificativo previsto dall'Allegato I del D.P.R. 15 luglio 2003 n. 254 "Regolamento recante disciplina della gestione dei rifiuti sanitari a norma dell'articolo 24 della L. 31 luglio 2002, n. 179";

b) siano violati i limiti temporali o quantitativi previsti dall'art. 8 del D.P.R. 254/2003, il quale dispone che il deposito temporaneo di rifiuti sanitari pericolosi può avere una durata massima di cinque giorni dal momento della chiusura del contenitore. Tale termine può essere esteso a trenta giorni per quantitativi di rifiuti inferiori a 200 litri.

5. Fattispecie di reato di cui all'art. 257 Cod.Amb.

L'art. 257 Cod. Amb., concernente la disciplina penale della bonifica dei siti, prevede due distinte fattispecie di reato:

- l'omessa bonifica del sito inquinato;
- la mancata comunicazione dell'evento inquinante alle autorità competenti secondo le modalità indicate dall'art. 242 Cod. Amb ..

a) omessa bonifica

In particolare, ai sensi dell'art. 257 Cod. Amb. è in primo luogo punito chiunque cagioni l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee, con il superamento delle concentrazioni soglia di rischio, se non provvede alla bonifica in conformità al progetto approvato dall'autorità competente nell'ambito dell'apposito procedimento amministrativo delineato dagli articoli 242 e ss. Cod. Amb ..

Presupposti per la configurabilità della suddetta fattispecie di reato sono:

- il superamento delle concentrazioni soglia di rischio (CSR);
- la mancata bonifica in conformità al progetto approvato dall'autorità competente nell'ambito del procedimento di cui agli articoli 242 e seguenti.

Trattasi di reato di evento a condotta libera o reato causale puro, sottoposto a condizione obiettiva di punibilità, dove l'evento di reato è previsto solo come evento di danno, ossia

come inquinamento, e l'inquinamento è definito come superamento delle concentrazioni soglia di rischio ("CSR"), che è un livello di rischio superiore ai livelli di attenzione individuati dalle concentrazioni soglia di contaminazione ("CSC") e quindi ai livelli di accettabilità già definiti dal D.M. n. 471/1999.

Non è punito, pertanto, l'inquinamento in sé, ma la mancata bonifica da eseguirsi secondo le regole fissate nell'apposito progetto. In proposito, la Suprema Corte ha precisato che « la configurabilità del reato richiede necessariamente il superamento della concentrazione soglia di rischio (CSR) ma la consumazione del reato non può prescindere dall'adozione del progetto di bonifica ex art. 242. Infatti l'art. 257 prevede ora che la bonifica debba avvenire in conformità al progetto di cui agli artt. 242 e seguenti che regolano la procedura di caratterizzazione e il progetto di bonifica così superando la formulazione dell'art. 51-bis del D. Lgs. n. 22/1997 che si limitava a prevedere la bonifica secondo il procedimento di cui all'art. 17. Si deve ritenere, quindi, che in assenza di un progetto definitivamente approvato non possa nemmeno essere configurato il reato di cui all'art. 257» (Cass. penale, sez. III, 9 giugno 2010 (ud. 13 aprile 2010), n. 22006).

Il reato è aggravato qualora l'inquinamento sia provocato da sostanze pericolose, secondo quanto previsto dall'art. 257, comma 2, Cod. Amb .

b) mancata effettuazione della comunicazione ex art. 242 Cod. Amb.

Al verificarsi di un evento che sia potenzialmente in grado di contaminare il sito, il responsabile della contaminazione deve, entro le 24 ore successive alla realizzazione dell'evento, adottare le necessarie misure di prevenzione e darne immediata comunicazione ai sensi e con le modalità di cui all'art. 304, comma 2, Cod. Amb.

In tal caso, diversamente dal reato di omessa bonifica, «la segnalazione che il responsabile dell'inquinamento è obbligato a effettuare alle autorità indicate in base all'art. 242 è dovuta a prescindere dal superamento delle soglie di contaminazione e la sua omissione è sanzionata dall'art. 257» (Cassazione penale, sez. III, 29 aprile 2011 (ud. 12 gennaio 2011), n. 16702).

6. Fattispecie di reato di cui all'art. 258 comma 4, secondo periodo Cod. Amb. Falsita' nella predisposizione di un certificato di analisi dei rifiuti

Ai sensi del 258 comma 4, secondo periodo del Cod. Amb., è punito chiunque, nella predisposizione di un certificato di analisi di rifiuti, fornisca false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nonché chiunque faccia uso di un certificato falso durante il trasporto.

Tale fattispecie di reato va inserita nel quadro degli adempimenti previsti dall'art. 188 bis del Cod. Amb. relativamente alla tracciabilità dei rifiuti, dal momento della produzione e sino alla loro destinazione finale. A tal riguardo il legislatore ha disposto che la tracciabilità dei rifiuti può avvenire:

- adempiendo agli obblighi di tenuta dei registri di carico e scarico nonché del formulario di identificazione di cui agli artt. 190 e 193 del Cod. Amb.

Si precisa che la fattispecie di reato in oggetto si riferisce a tutte le imprese ed enti produttori di rifiuti che, sono obbligati a tenere i suddetti registri e formulari.

7. Fattispecie di reato di cui all'art. 259 Cod. Amb. - Traffico illecito di rifiuti ·

Ai sensi dell'art. 259 comma I del Cod. Amb, sono punite due fattispecie di reato connesse ai traffici e alle spedizioni transfrontaliere dei rifiuti.

Il traffico illecito di rifiuti si concretizza allorchè vengono poste in essere le condotte espressamente previste dall'art. 2 del regolamento CEE del I febbraio 1993, n. 259, ossia qualsiasi spedizione di rifiuti effettuata:

a) senza invio di notifica e/ o senza il consenso delle autorità competenti interessate;

b) con il consenso delle autorità competenti interessate ottenuto mediante falsificazioni, false dichiarazioni o frode;

c) senza essere concretamente specificata nel documento di accompagnamento;

d) in modo tale da comportare uno smaltimento o un recupero in violazione delle norme comunitarie o internazionali;

e) in violazione dei divieti di importazione ed esportazione dei rifiuti previsti dagli articoli 14, 16, 19 e 21 del suddetto Regolamento 259/1993.

La fattispecie di reato si configura anche in relazione alla spedizione di rifiuti destinati al recupero (specificamente elencati nell'Allegato II del suddetto Regolamento 259/1993).

La condotta criminosa si configura ogni qualvolta vengano violate le condizioni espressamente previste dall'art. l comma 3 dello stesso (i rifiuti devono sempre essere destinati ad impianti autorizzati, devono poter essere oggetto di controlli da parte delle autorità competenti etc.).

8. Fattispecie di reato di cui all'art. 260 primo e secondo comma Cod. Amb. - Attività organizzate per il traffico illecito di rifiuti

Ai sensi dell'art. 260, comma primo, del Cod. Amb. è punito chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti. Il reato è aggravato qualora i rifiuti siano ad alta radioattività, secondo quanto previsto dall'art. 260 comma 2, Cod. Amb .

Il predetto articolo è stato abrogato e sostituito integralmente dall’art. 452 quaterdecies c.p. introdotto dalla L. n. 21/2018 nel Codice Penale.

9. Fattispecie di reato di cui all'art. 279 Cod. Amb. - Emissione in atmosfera di gas inquinanti oltre i limiti consentiti

Ai sensi dell'art. 279, quinto comma, del Cod. Amb., è punito chiunque, nell'esercizio di uno stabilimento, viola i valori limite di emissione o le prescrizioni stabiliti dall'autorizzazione, dagli Allegati I, II, III o V alla parte quinta del Cod. Amb., dai piani e dai programmi o dalla normativa di cui all'articolo 271 Cod. Amb. o le prescrizioni

altrimenti imposte dall'autorità competente, determinando anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa.

10. Fattispecie di cui alla L.n. 549/1993

In tema di tutela dell'ozono stratosferico (L. 549/1993), sono invece punite la produzione, il consumo, l'importazione, l'esportazione, la commercializzazione e la detenzione delle sostanze lesive secondo quanto previsto dal Regolamento CE n. 3093/94 (quest'ultimo abrogato e sostituito da ultimo dal Regolamento CE n. 1005/2009).

11. Fattispecie di cui alla L. n. 150/1992

In tema di protezione di specie della flora e della fauna selvatiche mediante il controllo del loro commercio, è punito chiunque, in violazione di quanto previsto dal Regolamento n. 338/97 e successive attuazioni e modificazioni, per gli esemplari appartenenti alle specie elencate negli allegato A, B e C del Regolamento medesimo, tra l'altro:

a) importa, esporta o riesporta esemplari sotto qualsiasi regime doganale senza il prescritto certificato o licenza, ovvero con certificato o licenza non validi;

b) omette di osservare le prescrizioni finalizzate all'incolumità degli esemplari, specificate in una licenza o in un certificato rilasciato in conformità al Regolamento;

c) utilizza i predetti esemplari in modo difforme dalla prescrizioni contenute nei provvedimenti autorizzativi o certificativi rilasciati unitamente alla licenza di importazione o certificati successiva mente;

d) trasporta o fa transitare, anche per conto terzi, esemplari senza licenza o certificato prescritti;

e) commercia piante riprodotte artificialmente in contrasto con le prescrizioni contenute nell'art. 7 del regolamento;

f) detiene, utilizza per scopi di lucro, acquista, vende, espone o detiene per la vendita o per fini commerciali, offre in vendita o comunque cede esemplari senza la prescritta documentazione.

12. Fattispecie di cui alla L. n. 202/2007

In relazione all'inquinamento provocato dalle navi, è punito il comandante, di una nave nonché i membri dell'equipaggio, il proprietario e l'armatore della nave che determinino il versamento in mare di sostanze inquinanti o causare lo sversamento di dette sostanze. Il reato è aggravato da ciò derivino danni permanenti o, comunque,

di particolare gravità, alla qualità delle acque, a specie animali o vegetali o a parti di queste.

13. Fattispecie di cui alla L. n. 68/14

In relazione agli eco reati, la Legge 68/14 aggiunge all'art. 25 undecies i seguenti reati:

- Inquinamento ambientale art. 452 bis cp (quote 250-600 + interdittive);
- Disastro ambientale art. 452 ter cp (quote 400 – 800 + interdittive);
- Delitti colposi contro l'ambiente art. 452 quinques c.p. (quote 200-500) riferito a disastro e inquinamento;
- Art. 452 septies impedito controllo: Il reato punisce chi ostacola, elude o rende difficoltose le attività ispettive o di vigilanza delle autorità competenti in materia ambientale. Può consistere, ad esempio, nel falsificare registri, occultare rifiuti o impedire fisicamente l'accesso ai luoghi sottoposti a controllo. La legge ha esteso la fattispecie anche alle società concessionarie e appaltatrici di servizi pubblici ambientali.
- Delitti associativi aggravati art. 452 octies c.p. (quote 300-1000);
- Delitto di traffico e abbandono di materiale ad alta radioattività art. 452 sexies c.p. (quote 250-600)
- Attività organizzate per il traffico illecito di rifiuti art. 452 quaterdecies cp (quote 300-500 per la violazione il primo comma; 400-800 per la violazione del secondo comma);

Ebbene, l'Organizzazione ritiene l'aspetto gestito attraverso le procedure ed i protocolli previsti per la matrice ambiente con particolare riferimento alle procedure ambientali in essere secondo linee ISO 14001:15 seppur ad oggi sistema non certificato (IO AMB).

14 Omessa bonifica (art. 452-terdecies c.p.)

È punito chi, avendo l'obbligo di bonificare un sito inquinato, omette di provvedervi o non adempie alle prescrizioni delle autorità. L'obbligo può derivare da un provvedimento amministrativo, da un giudizio civile o penale, o dall'aver causato l'inquinamento. La Legge 147/2025 ha chiarito che il reato sussiste anche se la bonifica è solo parzialmente eseguita o eseguita in modo inefficace.

15 Abbandono di rifiuti non pericolosi in casi particolari (art. 255-bis D.Lgs. 152/2006)

È introdotta una nuova fattispecie che punisce chi abbandona o deposita in modo incontrollato rifiuti non pericolosi in aree pubbliche o private, ovvero li immette nelle acque superficiali o sotterranee. Il reato si realizza anche in assenza di pericolo concreto per la salute, essendo sufficiente l'abbandono in violazione delle norme di gestione. Le pene sono aggravate se la condotta riguarda quantità ingenti o aree vincolate.

16 Abbandono di rifiuti pericolosi (art. 255-ter D.Lgs. 152/2006)

Punisce l'abbandono o il deposito incontrollato di rifiuti pericolosi, quali oli esausti, solventi, batterie o materiali contenenti sostanze tossiche o cancerogene. La pena è più elevata rispetto ai rifiuti non pericolosi, e aumenta ulteriormente se l'abbandono avviene da parte di un'impresa o di un ente. È sufficiente anche una sola condotta di abbandono deliberato per integrare il reato.

17 Combustione illecita di rifiuti (art. 256-bis D.Lgs. 152/2006)

La norma punisce chiunque bruci rifiuti, pericolosi o non, in assenza di autorizzazione o in modo difforme dai titoli ambientali. La condotta può consistere anche nella combustione all'aperto (roghi), tipica dei fenomeni della 'Terra dei Fuochi'. L'introduzione di questa fattispecie mira a colpire sia gli autori materiali sia gli organizzatori o i gestori delle aree interessate.

18 Spedizione illegale di rifiuti (art. 259 D.Lgs. 152/2006)

È punito chi effettua spedizioni transfrontaliere di rifiuti in violazione delle norme europee (Reg. UE 1013/2006). Rientrano le esportazioni verso Paesi extra-UE senza le necessarie notifiche o autorizzazioni, o con documentazione falsa. La Legge 147/2025 ha sostituito la precedente nozione di 'traffico illecito' con una fattispecie più grave e precisa di 'spedizione illegale'.

19 Aggravante per attività di impresa (art. 259-bis D.Lgs. 152/2006)

Introduce un'aggravante quando i reati di gestione, trasporto, abbandono o spedizione di rifiuti sono commessi nell'ambito di un'attività d'impresa o di un'organizzazione stabile. In tali casi, le pene sono aumentate e il profitto illecito può essere confiscato anche per equivalente.

20 Violazione degli obblighi di comunicazione, registri e formulari (art. 258 D.Lgs. 152/2006)

Sanziona chi non tiene, non aggiorna o falsifica i registri di carico e scarico, i formulari di identificazione o le comunicazioni ambientali obbligatorie. La legge ha trasformato alcune ipotesi da sanzione amministrativa a reato, introducendo anche pene accessorie quali la sospensione da albi o l'interdizione temporanea dall'attività

24. Sanzioni

In relazione ai Reati Ambientali di cui all'art. 25 undecies del D.Lgs. 231/2001 sono previste sanzioni pecuniarie da un minimo di Euro 40.000 ad un massimo di Euro 1.250.000.

Le sanzioni interdittive sono previste, ai sensi dell'art. 25 undecies comma 7 del D.Lgs. 231/2001 solo per determinate fattispecie di reato (ad es. lo scarico di acque reflue industriali, la discarica destinata allo smaltimento di rifiuti pericolosi, il traffico illecito di rifiuti) e comunque per un periodo non superiore a sei mesi.

La sanzione interdittiva definitiva è prevista se l'ente ha come scopo unico o prevalente quello di consentire o agevolare le attività finalizzate al traffico illecito di rifiuti (art. 260 Codice Ambiente) e per il reato di inquinamento doloso provocato dalle navi (art. 9 D. Lgs. 202/2007).

25. Identificazione delle attività sensibili

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificamente a rischio sono le seguenti:

1) gestione dei rifiuti come produttore, gestione verde pubblico, sevizi cimiteriali;

2) approvvigionamento idrico;

3) attività di selezione e gestione dei fornitori di servizi di analisi;

4) modifiche dei processi produttivi, degli impianti o installazione di nuovi impianti tecnologici;

5) attività di emissione in atmosfera;

6) scarico di acque reflue industriali (es. gestione piazzali);

7) inquinamento del suolo durante le attività in appalto;

8) gestione degli adempimenti e dichiarazioni obbligatorie per legge in materia ambientale.

17. Valutazione del rischio e matrice-reati

La valutazione del rischio di commissione di tale fattispecie criminosa in Adopera viene espressa attraverso il criterio già descritto al punto 3 del presente MOG.

Di seguito si riporta, quindi, la matrice di reato con individuato il rischio emerso attraverso il calcolo di P x D di cui al punto 3 del presente MOG e con specifica dei protocolli e/o procedure tali da rendere il rischio detto, ove ritenuto presente, come accettabile (intendendosi "accettabile" il rischio della commissione dei reati presupposto considerati esclusivamente attraverso l'elusione intenzionale e fraudolenta delle procedure e/o protocolli previste/i).

REATO	CONDOTTA	ATTIVITA' SENSIBILI	FUNZIONI E RISORSE UMANE COINVOLTE	quote	RI	PROTOCOLLI SPECIFICI	RR
727 bis c.p. - Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette	1) uccidere, catturare o detenere quantità non trascurabile di esemplari appartenenti ad una specie animale selvatica protetta; 2) distruggere, prelevare o detenere quantità non trascurabile di esemplari appartenenti ad una specie vegetale selvatica protetta;	manutenzione del verde	Amministratore Unico, Direttori Tecnici	100-200		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	
733 bis c.p. - Distruzione o deterioramento di habitat all'interno di un sito protetto	distruggere un habitat all'interno di un sito protetto o comunque deteriorarlo compromettendone lo stato di conservazione						
art. 137 comma 1 e 2 D.Lgs. 152/2006 - scarichi di acque reflue industriali	effettuare nuovi scarichi di acque reflue industriali contenenti anche sostanze pericolose senza autorizzazione o con autorizzazione scaduta	dilavamento piazzale, gestione reflui lavaggio mezzi	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	200-300 + interdittive		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	
art. 137 comma 3 D.Lgs. 152/2006 - scarichi di acque reflue industriali in difformità da prescrizioni	effettuare nuovi scarichi di acque reflue industriali contenenti sostanze pericolose senza osservare le prescrizioni dell'autorizzazione, o le altre prescrizioni dell'autorità competente	dilavamento piazzale, gestione reflui lavaggio mezzi	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	150-250		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	
art. 137 comma 5 D.Lgs. 152/2006 - scarichi di acque reflue industriali eccedendo i limiti tabellari	effettuare nuovi scarichi di acque reflue industriali contenenti sostanze pericolose superando i valori limite fissati nella tabella 3 o, nel caso di scarico sul suolo, nella tabella 4 dell'Allegato 5	dilavamento piazzale, gestione reflui lavaggio mezzi	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	150-250		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	
art. 137 comma 11 D.Lgs. 152/2006 - violazione del divieto di scarico sul suolo, nel suolo e nelle acque sotterranee	effettuare scarichi sul suolo, nel sottosuolo o nelle acque sotterranee al di fuori dalle deroghe disposte dall'art. 103 e 104 D.Lgs. 152/2006	gestione rifiuti in produzione (es. oli, gestione vasche interrate ecc.)	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	200-300 + interdittive		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	
art. 137 comma 13 D.Lgs. 152/2006 - violazione del divieto di scarico in mare da parte di navi e aereomobili di sostanze vietate	scaricare nel mare sostanze o materiali per i quali è imposto il divieto assoluto di sversamento ai sensi delle convenzioni internazionali, salvo che siano in quantità tali da essere resi rapidamenti innocui e purchè in presenta di preventiva autorizzazione da parte dell'autorità competente						
art. 256 comma 1 lett. a) D.Lgs. 152/2006 - Gestione non autorizzata di rifiuti	effettuare raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	100-250		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	
art. 256 comma 1 lett. b) D.Lgs. 152/2006 - Gestione non autorizzata di rifiuti pericolosi	effettuare raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti pericolosi in mancanza della prescritta autorizzazione, iscrizione o comunicazione	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	150-250		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	

art. 256 comma 3/1 D.Lgs. 152/2006 Discarica abusiva	realizzare o gestire una discarica non autorizzata	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	150 250		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	
art. 256 comma 3/2 D.Lgs. 152/2006 Discarica abusiva er rifiuti pericolosi	realizzare o gestire una discarica non autorizzata se essa è destinata anche in parte allo smaltimento di rifiuti pericolosi	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	150 250 + interditi ve		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice	
art. 256 comma 4 D.Lgs. 152/2006 Inosservanza delle prescizioni o assenza dei requisiti per iscrizioni/comunicazioni	inosservanza delle prescrizioni contenute o richiamate nelle autorizzazioni, o carenza dei requisiti e delle condizioni richiesti per le iscrizioni o comunicazioni.	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	150 250		interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	
art. 256 comma 5 D.Lgs. 152/2006 Miscelazione di Rifiuti Pericolosi	effettuare attività non consentite di miscelazione di rifiuti	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	150 250		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	
art. 256 comma 6/1 D.Lgs. 152/2006 deposito temporaneo di rifiuti sanitari pericolosi	effettuare il deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi, con violazione delle disposizioni di cui all'articolo 227, comma 1, lettera b)	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	100 250		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	
art. 257 comma 1 e 2 D.Lgs. 152/2006 omessa bonifica dei siti	cagionare l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio e non provvedere alla bonifica in conformità al progetto approvato dall'autorità competente nell'ambito del procedimento di cui agli articoli 242 e seguenti o non effettua la prevista comunicazione	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	100 250		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	
art. 258 comma 4/2 D.Lgs. 152/2006 predisposizione e utilizzo di certificato di analisi falso	nella predisposizione di un certificato di analisi di rifiuti, fornire false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico fisiche dei rifiuti o fare uso di un certificato falso durante il trasporto	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	150 250		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	
art. 259 comma 1 D.Lgs. 152/2006 traffico illecito di rifiuti	effettuare una spedizione di rifiuti costituente traffico illecito ai sensi dell'articolo 26 delregolamento (CEE) 1° febbraio 1993, n. 259, o effettuare una spedizione di rifiuti elencati nell'Allegato II del citato regolamento in violazione dell'articolo 1, comma 3, lettere a), b), c) e d), del	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	150 250		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	
art. 279 comma 5 D.Lgs. 152/2006 Emissione in atmosfera con superamento dei limiti	Nell'esercizio di uno stabilimento, violare i valori limite di emissione o le prescrizioni stabiliti dall'autorizzazione, dagli Allegati I, II, III o V alla parte quinta del presente decreto, dai piani e dai programmi o dalla normativa di cui all'articolo 271 o le prescrizioni altrimenti imposte dall'autorita' competente ed il superamento dei valori limite di emissione determina anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa.	gestione officina, gestione rifiuti, gestione polveri di piazzale	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	100 250		procedure ambientali interne secondo linee guida ISO 14001, verifiche/controlli, codice etico, mansionario	

art. 452 quatordecies cp - Attività organizzata per il traffico illecito di rifiuti	allestire mezzi e attività continuative organizzate a cedere, ricevere, trasportare, esportare, importare, o comunque gestiscere abusivamente ingenti quantitativi di rifiuti	gestione rifitui	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	comma 1 300-500, comma 2 400-800 + interditti ve		procedure linee guida ISO 14001, verifiche/controlli, codice etico, mansionario
art 452 bis cp	inquinamento ambientale	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	250-600		procedure linee guida ISO 14001, verifiche/controlli, codice etico, mansionario
art 452 quater cp	disastro ambientale	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	400-800		procedure linee guida ISO 14001, verifiche/controlli, codice etico, mansionario
art. 452 quinquies cp	delitti colposi contro l'ambiente	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	200-500		procedure linee guida ISO 14001, verifiche/controlli, codice etico, mansionario
art 452 sexies cp	traffico ed abbandono di materiale ad alta radioattività	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	250-600		procedure linee guida ISO 14001, verifiche/controlli, codice etico, mansionario
art. 452 quatordecies cp - Attività organizzata per il traffico illecito di rifiuti	allestire mezzi e attività continuative organizzate a cedere, ricevere, trasportare, esportare, importare, o comunque gestiscere abusivamente ingenti quantitativi di rifiuti	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei riifuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere	comma 1 300-500, comma 2 400-800 + interditti ve		procedure linee guida ISO 14001, verifiche/controlli, codice etico, mansionario

Abbandono di rifiuti non pericolosi in casi particolari (art. 255 bis D.Lgs. 152/2006)	È introdotta una nuova fattispecie che punisce chi abbandona o deposita in modo incontrollato rifiuti non pericolosi in aree pubbliche o private, ovvero li immette nelle acque superficiali o sotterranee. Il reato si realizza anche in assenza di pericolo concreto per la salute, essendo sufficiente l'abbandono in violazione delle norme di gestione. Le pene sono aggravate se la condotta riguarda quantità ingenti o aree vincolate.	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei rifiuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere			attuazione procedure interne, Moduli, allegati di sistema e istruzioni operative interne emesse ai fini ambientali, secondo linee iso 14001:15, verifiche controlli registrati e scritti, codice etico, mansionario,	
Abbandono di rifiuti pericolosi (art. 255 ter D.Lgs. 152/2006)	Punisce l'abbandono o il deposito incontrollato di rifiuti pericolosi, quali oli esausti, solventi, batterie o materiali contenenti sostanze tossiche o cancerogene. La pena è più elevata rispetto ai rifiuti non pericolosi, e aumenta ulteriormente se l'abbandono avviene da parte di un'impresa o di un ente. È sufficiente anche una sola condotta di abbandono deliberato per integrare il reato.	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei rifiuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere			attuazione procedure interne, Moduli, allegati di sistema e istruzioni operative interne emesse ai fini ambientali, secondo linee iso 14001:15, verifiche controlli registrati e scritti, codice etico, mansionario,	
Combustione illecita di rifiuti (art. 256 bis D.Lgs. 152/2006)	La norma punisce chiunque bruci rifiuti, pericolosi o non, in assenza di autorizzazione o in modo difforme dai titoli ambientali. La condotta può consistere anche nella combustione all'aperto (roghi), tipica dei fenomeni della 'Terra dei Fuochi'. L'introduzione di questa fattispecie mira a colpire sia gli autori materiali sia gli organizzatori o i gestori delle aree interessate.	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei rifiuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere			attuazione procedure interne, Moduli, allegati di sistema e istruzioni operative interne emesse ai fini ambientali, secondo linee iso 14001:15, verifiche controlli registrati e scritti, codice etico, mansionario,	
Impedimento del controllo (art. 452 septies c.p.)	Il reato punisce chi ostacola, elude o rende difficoltose le attività ispettive o di vigilanza delle autorità competenti in materia ambientale. Può consistere, ad esempio, nel falsificare registri, occultare rifiuti o impedire fisicamente l'accesso ai luoghi sottoposti a controllo. La legge ha esteso la fattispecie anche alle società concessionarie e appaltatrici di servizi pubblici ambientali.	sopralluoghi e accessi di qualsiasi genere da parte delle autorità/polizia giudiziaria, GDF, PA	Amministratore Unico, amministrazione, commerciale, Ufficio acquisti, Ufficio del personale, Direttori Tecnici			Protocollo rapporto con la PA, procedure in tema anticorruzione	
Omessa bonifica (art. 452 terdecies c.p.)	È punito chi, avendo l'obbligo di bonificare un sito inquinato, omette di provvedervi o non adempie alle prescrizioni delle autorità. L'obbligo può derivare da un provvedimento amministrativo, da un giudizio civile o penale, o dall'aver causato l'inquinamento. La Legge 147/2025 ha chiarito che il reato sussiste anche se la bonifica è solo parzialmente eseguita o eseguita in modo inefficace.	attività/modalità di gestione rifiuti, trasportatori e mezzi, destinatari dei rifiuti, appalti	Amministratore Unico, Direttori Tecnici, addetti servizi cimiteriali, magazziniere			attuazione procedure interne, Moduli, allegati di sistema e istruzioni operative interne emesse ai fini ambientali, secondo linee iso 14001:15, verifiche controlli registrati e scritti, codice etico, mansionario,	

14. Norme generali di comportamento

E' fatto divieto ai Destinatari di porre in essere o in qualsiasi modo contribuire alla realizzazione di comportamenti che possano integrare le fattispecie di reato previste all'art. 25 undecies del Decreto.

In particolare tutti i Destinatari hanno l'obbligo di:

1) operare nel rispetto delle leggi e delle normative nazionali ed internazionali vigenti in materia ambientale;

2) osservare le regole della presente Parte Speciale e delle procedure aziendali in materia ambientale;

3) redigere e custodire la documentazione relativa al rispetto delle prescrizioni in materia ambientale, consentendo il controllo sui comportamenti e le attività svolte

4) segnalare immediatamente ogni situazione di pericolo percepita, sia potenziale che reale, in tema di tutela ambientale.

In relazione alla Gestione dei Rifiuti, è necessario:

1) adoperarsi per uno smaltimento orientato al recupero, al reimpiego e al riciclaggio dei materiali, al fine di garantire un maggior grado di protezione della salute dell'uomo e dell'ambiente.

A tal fine si prescrive di:

- gestire i rifiuti in conformità ai principi di precauzione, prevenzione, sostenibilità, proporzionalità, responsabilizzazione e cooperazione di tutti i soggetti coinvolti nella produzione, distribuzione, utilizzo e consumo di beni da cui originano i rifiuti;
- gestire i rifiuti secondo criteri di efficacia, efficienza, economicità, trasparenza, fattibilità tecnica ed economica, nonché nel rispetto delle norme in materia ambientale;

2) definire i principali adempimenti da adottare in ambito aziendale in merito alla Gestione delle diverse tipologie di rifiuti - pericolosi e non pericolosi - al fine di operare in modo uniforme su tutto il territorio nazionale;

3) provvedere alla classificazione dei rifiuti prodotti nell'ambito delle attività aziendali in conformità a quanto stabilito dalle disposizioni legislative vigenti e dalle autorità competenti e a tal fine informa e fornisce adeguata formazione al personale delle unità produttive di rifiuti sulle base delle rispettive attribuzioni;

4) affidare le attività di raccolta, trasporto, recupero e smaltimento dei rifiuti esclusivamente ad imprese autorizzate, nel rispetto delle procedure aziendali relative alla qualificazione dei Fornitori. A tal riguardo, in particolare assicura che gli operatori economici inseriti nell'albo delle imprese qualificate che svolgano attività di Gestione dei Rifiuti siano sottoposti a costante monitoraggio e aggiornamento, anche

attraverso la consultazione dell'Albo Nazionale dei Gestori Ambientali tenuto presso il Ministero dell'Ambiente e della Tutela del Territorio e del Mare;

5) verificare, in sede di affidamento delle attività di smaltimento o recupero di rifiuti alle imprese autorizzate:

- la data di validità dell'autorizzazione;
- la tipologia e la quantità di rifiuti per i quali è stata rilasciata l'autorizzazione ad esercitare attività di smaltimento o recupero;
- la localizzazione dell'impianto di smaltimento
- il metodo di trattamento o recupero;
- l'iscrizione al sistema informatico gestione rifiuti (quando attuato)

6) verificare, in fase di esecuzione delle attività di trasporto di rifiuti alle imprese autorizzate:

- la data di validità dell'autorizzazione;
- la tipologia e la targa del mezzo;
- i codici CER autorizzati;
- l'iscrizione al sistema informatico gestione rifiuti (quando attuato)

7) effettuare la tenuta regolare del registro di carico e scarico e curare che lo stesso, unitamente ai formulari identificativi del rifiuto, siano compilati in modo corretto e veritiero, astenendosi dal porre in essere operazioni di falso ideologico o materiale (ad esempio in relazione alle informazioni sulle caratteristiche qualitative o quantitative dei rifiuti). A tal fine si deve prevedere in apposite procedure e istruzioni operative:

- le istruzioni per la tenuta, la compilazione e l'archiviazione del registro di carico scarico e del formulario di identificazione, nonché della documentazione relativa al sistema informatico gestione rifiuti (quando attuato);
- i controlli sulla restituzione della IV copia del formulario di identificazione controfirmato e datato;
- i controlli periodici sulla correttezza e veridicità dei suddetti documenti connessi alla Gestione dei Rifiuti;
- la segnalazione da effettuare alle Direzioni competenti e all'Organismo di Vigilanza, se del caso, su eventuali anomalie riscontrate nei documenti all'esito dei controlli effettuati;

8) effettuare il Deposito Temporaneo per categorie omogenee di rifiuti e nel rispetto delle relative norme tecniche nonché, per i Rifiuti Pericolosi, nel rispetto delle norme che disciplinano il deposito delle sostanze pericolose in essi contenute;

9) sottoporre le procedure aziendali relative alla gestione dei rifiuti ad un costante monitoraggio al fine di valutare periodicamente l'opportunità di aggiornamenti in ragione di interventi normativi in materia ambientale;

10) vigilare costantemente sulla corretta Gestione dei Rifiuti anche attraverso audit sui partner/fornitori, segnalando eventuali irregolarità alla Direzione e all'Organismo

di Vigilanza al fine di porre in essere le conseguenti azioni di tipo amministrativo e contrattuale oltre che le eventuali azioni di tipo legale dinanzi alle competenti autorità.

In relazione alla **Emissione di effluenti gassosi in atmosfera**, è necessario:

Valutare la oresenza di emissioni eventualmente soggette ad autorizzazione;
Rispettare i limiti autorizzati di inquinanti emessi e di portata oraria degli impianti con emissioni in atmosfera;
Effettuare periodici controlli analitici sugli effluenti gassosi, al fine di dimostrare il rispetto dei limiti suddetti;
Annotare i controlli periodici su apposito Registro delle Emissioni, vidimato dall'ARPAE competente per zona;
Mantenere i consumi dei prodotti vernicianti entro il limite autorizzato, provvedendo al monitoraggio, alla registrazione dei consumi sul Registro degli Indicatori e comunicando annualmente agli Enti indicati in autorizzazione il quantitativo utilizzato nell'anno precedente;
Mantenere in efficienza gli impianti di aspirazione ed i sistemi filtranti ad essi connessi, rispettando le prescrizioni contenute nell'atto autorizzativo;
Attrezzare e rendere accessibili e campionabili le emissioni oggetto della autorizzazione, per le quali sono fissati limiti di inquinanti e autocontrolli periodici, sulla base delle normative tecniche e delle normative vigenti sulla sicurezza ed igiene del lavoro, come indicato nell'atto autorizzativo.
Ogni emissione elencata in Autorizzazione deve essere numerata ed identificata univocamente con scritta indelebile in prossimità del punto di emissione. I punti di misura/campionamento devono essere collocati in tratti rettilinei di condotto a sezione regolare (circolare o rettangolare), preferibilmente verticali, lontano da ostacoli, curve o qualsiasi discontinuità che possa influenzare il moto dell'effluente.
Segnalare alle Direzioni competenti e all'Organismo di Vigilanza, se del caso, su eventuali anomalie riscontrate nei documenti e negli impianti che possano pregiudicare la qualità dell'emissione.

In relazione allo **scarico di acque reflue**, è necessario:

Valutare l'assoggettabilità ad autorizzazione di eventuali reflui ritenuti industriali;

Rispettare i limiti autorizzati di inquinanti scaricati, in riferimento alla tabella 3 dell'Allegato 5 del D.lgs 152/06;

Effettuare periodici controlli analitici sugli effluenti scaricati, al fine di dimostrare il rispetto dei limiti suddetti;

Mantenere in efficienza gli impianti di depurazione delle acque, conservando l'evidenza documentale delle periodiche manutenzioni effettuate ed annotandole su apposito registro delle manutenzioni;

Che i pozzetti di controllo e manutenzione a monte dell'immissione nella pubblica fognatura dovranno essere mantenuti accessibili per i sopralluoghi e gli eventuali campionamenti da parte degli organi di controllo;

Evitare la diluizione degli scarichi con acque prelevate a questo scopo;

Evitare la contaminazione della rete fognaria interna, mettendo in atto le procedure di sistema relative al contenimento e gestione degli sversamenti di sostanze chimiche;
Segnalare alle Direzioni competenti e all'Organismo di Vigilanza, se del caso, su eventuali anomalie riscontrate nei documenti e negli impianti che possano pregiudicare la qualità dello scarico.

In relazione alla **bonifica di siti inquinati**, è necessario:

Che chiunque rilevi una possibile contaminazione del suolo o sottosuolo a seguito di sversamenti di sostanze pericolose, malfunzionamento dei sistemi di controllo dei serbatoi interrati, cedimenti o rotture degli stessi, avvisi immediatamente la Direzione Aziendale e l'Organismo di Vigilanza;

Dotarsi di specifiche procedure di gestione delle emergenze (es. sversamenti);

Gestire correttamente i rifiuti evitando il deposito direttamente a suolo ed, evitando, in ogni caso il dilavamento o la dispersione degli stessi in deposito temporaneo.

Per tutti gli ambiti sono pianificati controlli periodici attraverso check list scritte.

IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE (ARTT- 12 e 22 D.Lgs. 286/98) E INTERMEDIAZIONE ILLECITA E SFRUTTAMENTO DEL LAVORO (art. 603 bis cpp) XENOFOBIA E RAZZISMO L. 199/16

Il reato ex art. 22 D.lgs. 286/98 punisce il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, con permesso di soggiorno scaduto del quale non sia stato chiesto il rinnovo entro i termini di legge o con permesso revocato o annullato.

Le pene sono aumentate se si verificano una delle seguenti aggravanti:

- i lavoratori occupati sono in numero superiore a tre;
- i lavoratori occupati sono minori in età non lavorativa;

- i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dall'art. 603- bis del codice penale.

Il Decreto per questi reati prevede le seguenti sanzioni:

Sanzione pecuniaria: da 100 fino a 200 quote.

Si dà evidenza, altresì che in data 4 novembre 2016, inoltre, è entrata in vigore la legge 29 ottobre 2016, n. 199 che ha ulteriormente ampliato l'ambito dei reati previsti dal D. Lgs 231/01.

La legge ha modificato il testo dell'art. 603bis c.p. concernente il reato di "Intermediazione illecita e sfruttamento del lavoro" ampliandone la previsione originaria. A tal proposito l'art. 6 della Legge introduce tale reato in seno all'art. 25 quinquies co. 1, lett. a) del D. Lgs 231/01 prevedendo sia sanzioni pecuniarie (d 400 a 1000 quote) che interdittive per una durata non inferiore ad 1 anno e anche definitive nel caso di utilizzo stabile dell'organizzazione allo scopo unico o prevalente di consentire o agevolare la commissione del reato.

ADOPERA ritiene il rischio di commissione di tale fattispecie criminosa gestito attraverso i protocolli e le procedure già previste per il reato di cui all'art. 22 D.lgs. 286/98.

Ancora, si dà atto che in data 19 novembre 2017, è entrata in vigore la legge 17 ottobre 2017, n. 161 "Modifica al codice delle leggi antimafia e delle misure di prevenzione" che ha previsto l'ampliamento dell'ambito dei reati rilevanti ai sensi del D.lgs. 231/2001 anche alle disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3 bis, 3 ter e 5 D.lgs. 286/1998), già contemplate nel catalogo dei reati rilevanti ai sensi del D.lgs. 231/2001 se commessi in modalità transazionale e, a seguito di tale modifica, divenuti rilevanti anche se commessi in modalità nazionale. L'articolo 12, nei commi sopra indicati, punisce chiunque, in violazione delle disposizioni del Testo Unico sull'Immigrazione, promuove, dirige, organizza, finanzia o effettua il trasporto di stranieri nel territorio dello Stato ovvero compie altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato, ovvero di altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente nonché, il favoreggiamento dell'immigrazione clandestina.

Inoltre con l'introduzione dell'art. 25 terdecies occorre fare riferimento anche al reato in materia di razzismo e xenofobia di cui alla L 654/75 che prevede una sanzione pecuniaria da 200 a 800 e che punisce la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale, ratificato ai sensi della legge 12 luglio 1999, n. 232.

1. Identificazione delle attività sensibili

Le attività sensibili che Adopera ha individuato al proprio interno sono le seguenti:

1) selezione del personale al momento dell'assunzione;
2) attività in appalto/subappalto nazionale ed esteri;
3) sponsorizzazioni, regalie, omaggi

2. Valutazione del rischio e matrice-reati

La valutazione del rischio di commissione di tale fattispecie criminosa in Adopera viene espressa attraverso il criterio già descritto al punto 3 del presente MOG.

Di seguito si riporta, quindi, la matrice di reato con individuato il rischio emerso attraverso il calcolo di P x D di cui al punto 3 del presente MOG e con specifica dei protocolli e/o procedure tali da rendere il rischio detto, ove ritenuto presente, come accettabile (intendendosi "accettabile" il rischio della commissione dei reati presupposto considerati esclusivamente attraverso l'elusione intenzionale e fraudolenta delle procedure e/o protocolli previste/i).

REATO	CONDOTTA	ATTIVITA' SENSIBILI	FUNZIONI E RISORSE UMANE COINVOLTE	QUOTE	R	PROTOCOLLI SPECIFICI	RR
ART. 22 D.Lgs. 286/98	Il reato punisce il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, con permesso di soggiorno scaduto del quale non sia stato chiesto il rinnovo entro i termini di legge o con permesso revocato o annullato.	Assunzione, appalti, assegnazione	Amminmistratore Unico, Direttori Tecnici, Ufficio risorse umane, Uffico Amministrazione	100-200		procedure specifiche in fase di assunzione (quesiti e documentazione da richiedere), cluasole contrattuali a salvaguardia.	
art 603 bis cpp	intermediazione e sfruttamento del lavoro	Assunzione, appalti, assegnazione	Amminmistratore Unico, Direttori Tecnici, Ufficio risorse umane, Ufficio Amministrazione	400-1000		procedure specifiche in fase di assunzione (quesiti e documentazione da richiedere), cluasole contrattuali, procedura DUVRI	
art 3 comma 3 bis L 65	Propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale, ratificato ai sensi della legge 12 luglio 1999, n. 232.	sponsorizzazioni, omaggi, regalie, spazi pubblicitari	Amminmistratore Unico, Direttori Tecnici, Ufficio risorse umane, Ufficio Amministrazione	200-800		Verifica dei soggetti e delle transazioni economiche – anagrafiche dei beneficiari; protocollo sponsorizzazioni ed elargizioni, protocollo assegnazione incarichi professionali, ISO 9001	

3. Norme generali di comportamento

Dipendenti e gli Organi Sociali devono adottare e rispettare:

1. il sistema di controllo interno, e quindi le procedure aziendali, la documentazione e le disposizioni inerenti la struttura gerarchico/funzionale aziendale e organizzativa;
2. il sistema disciplinare;
3. in generale, la normativa applicabile.

In particolare gli Organi Sociali (in via diretta), i lavoratori dipendenti ed i consulenti di Adopera (limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche clausole contrattuali) hanno il divieto di:

- favorire e/o promuovere l'impiego di lavoratori stranieri privi del permesso di soggiorno o con permesso scaduto rispetto al quale non sia stato chiesto, entro i termini di legge, il rinnovo oppure con permesso revocato o annullato;

- ridurre o mantenere i lavoratori in stato di soggezione continuativa;

- sottoporre i lavoratori a condizioni di sfruttamento, ad esempio esponendoli a situazioni di grave pericolo, in considerazione della prestazione da svolgere e del contesto lavorativo.

E' fatto inoltre divieto di assegnare incarichi di fornitura a terzi nei casi in cui si abbia notizia, o anche solo il sospetto, del mancato rispetto da parte del fornitore delle norme a tutela del lavoratore ed in materia di immigrazione.

A tale proposito, la Società, in caso di rapporti di fornitura in ambiti particolarmente sensibili (ad esempio aree geografiche a forte presenza di lavoro irregolare o comparti di attività storicamente esposti a tali rischi) sensibilizza i propri fornitori, anche a mezzo di apposite clausole contrattuali, in merito ai principi cui l'attività degli stessi deve ispirarsi, nell'ambito della collaborazione con Adopera in tema di garanzie legali e morali dei lavoratori

(rispetto della legge, non discriminazione, divieto di lavoro minorile, divieto di forme di coercizione mentale o fisica, divieto di abusi e molestie, rispetto delle norme in tema di sicurezza e salute sui luoghi di lavoro, rispetto dei minimi salariali e degli orari di lavoro, rispetto delle libertà di associazione, rispetto della tutela dell'ambiente, ecc.).

Tutti gli accordi contrattuali con soggetti terzi devono comunque contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti all'utilizzo di lavoratori stranieri "irregolari").

Si devono inoltre prevedere apposite procedure per la selezione del personale con elenco della documentazione minima richiesta.

REATI INFORMATICI E ILLECITO TRATTAMENTO DEI DATI

La legge 18 marzo 2008 n. 48 ha ratificato ed eseguito la Convenzione di Budapest del 23 novembre 2001, promossa dal Consiglio d'Europa in tema di criminalità informatica e riguardante, in particolare, i reati commessi avvalendosi in qualsiasi modo di un sistema informatico od in suo danno, ovvero che pongano in qualsiasi modo l'esigenza di raccogliere prove in forma informatica.

Ai sensi dell'art. 1 della Convenzione, rientra nella nozione di "sistema informatico" *"qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati".*

Tra i "dati informatici" rientra inoltre *"qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato,*

incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione".

Con il termine *"service provider"* (fornitore di servizi) si indica:

a) qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico;

b) qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio;

Per *"trasmissione di dati"* si vuole infine indicare qualsiasi informazione computerizzata relativa ad una comunicazione attraverso un sistema informatico che costituisce una parte nella catena di comunicazione, indicando l'origine della comunicazione, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo del servizio.

L'art. 24-bis del Decreto contempla la responsabilità degli enti con riguardo a tre distinte categorie:

1) reati che comportano un "danneggiamento informatico" (art. 24-bis, co. 1);
2) reati derivanti dalla detenzione o diffusione di codici o programmi atti al danneggiamento informatico (art. 24-bis, co. 2);
3) reati relativi al falso in documento informatico e frode del soggetto che presta servizi di certificazione attraverso la firma digitale (art. 24-bis, co. 3).

L'art. 24-bis prevede la responsabilità degli enti in relazione a sette distinti reati che hanno come fattore comune il "danneggiamento informatico", ossia che determinano l'interruzione del funzionamento di un sistema informatico o il danneggiamento del software, sotto forma di programma o dato. Più in particolare, ricorre il danneggiamento informatico quando, considerando sia la componente hardware che quella software, anche separatamente, si verifica una modifica tale da impedirne, anche temporaneamente, il funzionamento.

1. Accesso abusivo ad un sistema telematico o informatico (art. 615 ter c.p.)

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al

servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

La norma ai fini della punibilità prescinde dalla rivelazione a terzi delle informazioni indebitamente captate o dal danneggiamento del sistema, incorrendo – in quest'ultimo caso – nell'ulteriore concorso di circostanze aggravanti. Il dolo richiesto è generico e consiste nella volontà di introdursi o mantenersi nella memoria interna di un elaboratore in assenza del consenso del titolare del diritto di escluderlo e con la consapevolezza che quest'ultimo ha predisposto misure di protezione per i dati che vi sono memorizzati.

Nel contesto aziendale il reato può essere commesso anche da un dipendente che, pur possedendo le credenziali di accesso al sistema, acceda a parti di esso a lui precluse, oppure acceda, senza esserne legittimato, a banche dati della Società (o anche di terzi concesse in licenza alla Società) mediante l'utilizzo delle credenziali di altri colleghi abilitati.

Le sanzioni previste dal Decreto per questa categoria di reati sono:

Sanzione pecuniaria da 100 a 500 quote

Sanzioni interdittive:

a) interdizione dall'esercizio dell'attività;
b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c) divieto di pubblicizzare beni o servizi;

2. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a 5.164 euro.

Sanzione pecuniaria da 100 a 300 quote

3. Diffusione di apparecchiature dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.)

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

Le fattispecie descritte nei precedenti due reati, entrambe perseguibili d'ufficio, intendono reprimere anche la sola abusiva detenzione o diffusione di credenziali d'accesso o di programmi (virus, spyware) o dispositivi potenzialmente dannosi indipendentemente dalla messa in atto degli altri crimini informatici sopra illustrati, rispetto ai quali le condotte in parola possono risultare propedeutiche.

La prima fattispecie richiede che il reo agisca a scopo di lucro o di altrui danno ed è prodromica all'accesso abusivo vero e proprio. Si tratta di un reato di pericolo che si consuma non in dipendenza del danno o del turbamento effettivo del sistema, ma per il fatto di essere venuti a conoscenza degli strumenti descritti nella norma o di avere ceduto informazioni utili ad operare accessi.

Peraltro, nella valutazione di tali condotte potrebbe assumere preminente rilevanza la considerazione del carattere obiettivamente abusivo di trasmissioni di dati, programmi, e mail, etc., da parte di chi, pur non essendo mosso da specifica finalità di lucro o di causazione di danno, sia a conoscenza della presenza in essi di virus che potrebbero determinare gli eventi dannosi descritti dalla norma.

Le sanzioni previste dal Decreto per questa categoria di reati sono:

Sanzione pecuniaria fino a 300 quote

Sanzioni interdittive:

a) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

b) divieto di pubblicizzare beni o servizi;

4. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

1. Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)

Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

La condotta punita dall'art. 617 quater c.p. consiste nell'intercettare fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più

sistemi, o nell'impedimento o interruzione delle stesse. Integra la medesima fattispecie, salvo che il fatto non costituisca un più grave reato, anche la diffusione mediante qualsiasi mezzo di informazione al pubblico del contenuto delle predette comunicazioni.

L'intercettazione può avvenire sia mediante dispositivi tecnici, sia con l'utilizzo di software (c.d. spyware). L'impedimento od interruzione delle comunicazioni (c.d. "Denial of service") può anche consistere in un rallentamento delle comunicazioni e può realizzarsi non solo mediante impiego di virus informatici, ma anche ad esempio sovraccaricando il sistema con l'immissione di numerosissime comunicazioni fasulle.

Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali rientrano le condotte commesse in danno di un sistema utilizzato dallo Stato o da altro ente pubblico o da imprese esercenti servizi pubblici o di pubblica necessità o con abuso della qualità di operatore di sistema.

Nell'ambito aziendale l'impedimento o l'interruzione potrebbero essere ad esempio causati dall' installazione non autorizzata di un software da parte di un dipendente.

L'art. 617 quinquies punisce il solo fatto della istallazione, fuori dai casi consentiti dalla legge, di apparecchiature atte a intercettare, impedire o interrompere le comunicazioni, indipendentemente dal verificarsi di tali eventi. Il delitto è perseguibile d'ufficio.

Le sanzioni previste dal Decreto per questa categoria di reati sono:

Sanzione pecuniaria da 100 a 500 quote

Sanzioni interdittive:

a) interdizione dall'esercizio dell'attività;
b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c) divieto di pubblicizzare beni o servizi.

2. Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

3. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

L'art. 635 bis c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera, sopprime, informazioni, dati o programmi informatici altrui.

Secondo un'interpretazione rigorosa, nel concetto di "programmi altrui" potrebbero ricomprendersi anche i programmi utilizzati dal soggetto agente in quanto a lui concessi in licenza dai legittimi titolari.

L'art. 635 ter c.p., salvo che il fatto costituisca più grave reato, punisce le condotte anche solo dirette a produrre gli eventi lesivi descritti dall'articolo che precede, a prescindere dal prodursi in concreto del risultato del danneggiamento, che se si verifica costituisce circostanza aggravante della pena. Deve però trattarsi di condotte dirette a colpire informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. Rientrano pertanto in tale fattispecie anche le condotte riguardanti dati, informazioni e programmi utilizzati da enti privati, purché siano destinati a soddisfare un interesse di pubblica necessità.

Entrambe le fattispecie sono aggravate se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema. Qualora le condotte descritte conseguano ad un accesso abusivo al sistema esse saranno punite ai sensi del sopra illustrato art. 615 ter c.p..

Le sanzioni previste dal Decreto per questa categoria di reati sono:

Sanzione pecuniaria da 100 a 500 quote

Sanzioni interdittive:

a) interdizione dall'esercizio dell'attività;

b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

c) divieto di pubblicizzare beni o servizi;

4. Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

5. Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)

Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata. L' art. 635 quater c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635 bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento. Per dirsi consumato il reato in oggetto, il sistema su cui si è perpetrata la condotta criminosa deve risultare danneggiato o reso, anche in parte, inservibile o ne deve venire ostacolato il funzionamento.

L'art. 635 quinquies c.p. punisce le medesime condotte descritte nell'articolo che precede anche se gli eventi lesivi non si realizzino in concreto; il loro verificarsi costituisce circostanza aggravante della pena (va però osservato che il concreto ostacolo al funzionamento del sistema non rientra espressamente fra gli "eventi" aggravanti). Deve però trattarsi di condotte che mettono in pericolo sistemi informatici o telematici di pubblica utilità.

In questa previsione, a differenza di quanto previsto all'art. 635 ter, non vi è più alcun riferimento all'utilizzo da parte di enti pubblici: per la configurazione del reato in oggetto, parrebbe quindi che i sistemi aggrediti debbano essere semplicemente "di pubblica utilità"; non sarebbe cioè, da un lato, sufficiente l'utilizzo da parte di enti pubblici e sarebbe, per altro verso, ipotizzabile che la norma possa applicarsi anche al caso di sistemi utilizzati da privati per finalità di pubblica utilità.

Entrambe le fattispecie sono perseguibili d'ufficio e prevedono aggravanti di pena se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema.

E' da ritenere che le fattispecie di danneggiamento di sistemi assorbano le condotte di danneggiamento di dati e programmi qualora queste rendano inutilizzabili i sistemi o ne ostacolino gravemente il regolare funzionamento.

Qualora le condotte descritte conseguano ad un accesso abusivo al sistema, esse saranno punite ai sensi del sopra illustrato art. 615 ter c.p..

Le sanzioni previste dal Decreto per questa categoria di reati sono:

Sanzione pecuniaria da 100 a 500 quote

Sanzioni interdittive:

a) interdizione dall'esercizio dell'attività;
b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c) divieto di pubblicizzare beni o servizi;

10. Falsità nei documenti informatici (art. 491 bis c.p.)

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici .

L'art. 419 *bis* c.p. estende le norme in materia di delitti di falsità in atti ai documenti informatici pubblici, da intendersi come ogni rappresentazione di dati, informazioni o

concetti suscettibili di essere utilizzata in un sistema o con un programma informatico.

Si tratta di una serie di reati posti a tutela della fede pubblica documentale, cioè della fiducia e sicurezza che le persone ripongono in determinati documenti, alla luce dell'efficacia probatoria riconosciuta dall'ordinamento (e, in particolare, ad atti pubblici, ma anche certificati ed autorizzazioni amministrative).

Il concetto di documento informatico è nell'attuale legislazione svincolato dal relativo supporto materiale che lo contiene, in quanto l'elemento penalmente determinante ai fini dell'individuazione del documento informatico consiste nell'attribuibilità allo stesso di un'efficacia probatoria secondo le norme civilistiche.

Ai sensi del Codice dell'amministrazione digitale (art. 1 lettera p) del D. Lgs. n. 82/2005), il documento informatico è "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", ma:

a) se non è sottoscritto con una firma elettronica (art. 1 lettera q), non può avere alcuna efficacia probatoria, ma può al limite, a discrezione del Giudice, soddisfare il requisito legale della forma scritta (art. 20 comma 1 bis);
b) anche quando sia firmato con una firma elettronica "semplice" (cioè non qualificata) può non avere efficacia probatoria (il giudice dovrà infatti tener conto, per attribuire tale efficacia, delle caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità del documento informatico);
c) il documento informatico sottoscritto con firma digitale o altro tipo di firma elettronica qualificata ha l'efficacia prevista dall'articolo 2702 del codice civile (al pari della scrittura privata), fa cioè piena prova, fino a querela di falso, se colui contro il quale è prodotto ne riconosce la sottoscrizione.

Nei reati di falsità in atti è fondamentale la distinzione tra le falsità materiali e le falsità ideologiche: ricorre la falsità materiale quando vi sia divergenza tra l'autore apparente e l'autore reale del documento o quando questo sia stato alterato (anche da parte dell'autore originario) successivamente alla sua formazione; ricorre la falsità ideologica quando il documento contenga dichiarazioni non veritiere o non fedelmente riportate.

Con riferimento ai documenti informatici aventi efficacia probatoria, il falso materiale potrebbe compiersi mediante l'utilizzo di firma elettronica altrui, mentre appare improbabile l'alterazione successiva alla formazione.

Non sembrano poter trovare applicazione, con riferimento ai documenti informatici, le norme che puniscono le falsità in fogli firmati in bianco (artt. 486, 487, 488 c.p.).

Il reato di uso di atto falso (art. 489 c.p.) punisce chi pur non essendo concorso nella commissione della falsità fa uso dell'atto falso essendo consapevole della sua falsità.

Le sanzioni previste dal Decreto per questa categoria di reati sono:

Sanzione pecuniaria fino a 400 quote

Sanzioni interdittive:

a) divieto di contrarre con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio;

b) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;

c) divieto di pubblicizzare beni o servizi

11. Frode informatica (art. 640 ter c.p.)

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro.

La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

La fattispecie è contemplata nell'art. 24 del Decreto e viene qui trattata per questione di omogeneità con le fattispecie delittuose successivamente introdotte all'art. 24 bis dalla L. 48/2008.

Le condotte poste in essere attraverso tale reato sono due:

1) alterazione del funzionamento di un sistema informatico o telematico, ossia in una modifica del regolare svolgimento di un processo di elaborazione o di trasmissione dati: l'alterazione provoca i suoi effetti materiali sul sistema informatico o telematico;

2) intervento, senza diritto, con qualsiasi modalità, su dati, informazioni o programmi contenuti nel sistema, e pertanto ogni forma di interferenza diversa dall'alterazione del funzionamento del sistema. L'intervento senza diritto ha per oggetto i dati, le informazioni o i programmi.

L'evento si realizza con il danno patrimoniale altrui e l'ingiusto profitto dell'agente o di un terzo.

L'intervento senza diritto a cui fa menzione il legislatore nel primo comma dell'art. 640-ter c.p. si verifica quando l'agente non è autorizzato - né da una legge né dal titolare - ad eseguire l'attività non consentita sul sistema informatico.

Alla stregua della truffa, la frode informatica richiede il dolo qenerico, cioè la coscienza e la volontà di realizzare il fatto tipico che consiste nell'ottenere o nel procurare un ingiusto profitto con altrui danno.

Le sanzioni previste dal Decreto per questa categoria di reati sono:

Sanzione pecuniaria:

a) fino a 500 quote;

b) da 200 a 600 quote (nei casi di profitto o danno rispettivamente di rilevante entità o particolare gravità);

Sanzioni interdittive:

a) divieto di contrarre con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio;

b) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;

c) divieto di pubblicizzare beni o servizi.

Reati informatici e cybersicurezza – art. 24-bis e art. 25-octies.1 D.Lgs. 231/01

La Società, in recepimento della Legge 28 giugno 2024, n. 90 (attuazione Direttiva UE 2022/2555 – NIS2), aggiorna il Modello Organizzativo 231 al fine di prevenire i reati informatici di cui all'art. 24-bis e le violazioni degli obblighi di cybersicurezza di cui al nuovo art. 25-octies.1 del D.Lgs. 231/2001.

Presidi organizzativi

• adozione di una Cybersecurity Policy e delle procedure interne in materia di sicurezza informatica;

• definizione di ruoli e responsabilità (in particolare il Responsabile Sicurezza Informatica / CISO);

• gestione controllata di accessi, credenziali e profili utente;

• procedure di onboarding/offboarding e classificazione dei dati.

Presidi tecnici

• utilizzo di sistemi di autenticazione forte (MFA), crittografia, segmentazione di rete;

• programmi periodici di patching, vulnerability assessment e monitoraggio degli eventi di sicurezza;

• sistemi di backup sicuri e testati;
• utilizzo di soluzioni antivirus/EDR/XDR.

Incident Response

La Società adotta una procedura di gestione degli incidenti informatici che disciplina:
• identificazione, contenimento, analisi e ripristino;
• registrazione dell'evento e conservazione dei log;
• notifica agli organismi competenti (CSIRT/ACN) nei tempi previsti dalla normativa NIS2.

Formazione e consapevolezza

È previsto un programma annuale di formazione del personale sui rischi informatici e sulle misure di tutela, con specifiche iniziative rivolte alle funzioni IT e agli amministratori di sistema.

Fornitori critici

Per i fornitori di servizi IT, cloud e infrastrutture digitali sono introdotti specifici requisiti contrattuali e controlli di sicurezza.

Flussi informativi verso l'OdV

Il Responsabile della Sicurezza Informatica trasmette all'OdV:
• report periodici sullo stato delle misure di sicurezza;
• esiti degli audit e delle verifiche di vulnerabilità;
• segnalazioni di incidenti informatici di ogni livello.

Sistema disciplinare

Costituisce violazione del Modello l'inosservanza delle policy di sicurezza informatica, la mancata adozione delle misure prescritte e l'omessa segnalazione di incidenti o eventi anomali.

12. Identificazione delle attività sensibili

Le attività sensibili che ADOPERA ha individuato al proprio interno sono le seguenti:

Gestione e protezione delle infrastrutture informatiche e di rete
Gestione delle credenziali, profili utente e ruoli di accesso
Manutenzione e assistenza tecnica remota
Gestione dei fornitori ICT e servizi cloud
Gestione e protezione della proprietà intellettuale software
Gestione della fatturazione elettronica e sistemi ERP
Gestione incidenti informatici e data breach
Formazione, consapevolezza e cultura della sicurezza digitale

13. Valutazione del rischio e matrice-reati

La valutazione del rischio di commissione di tale fattispecie criminosa in ADOPERA viene espressa attraverso il seguente criterio già descritto al punto 3 del presente MOG.

Di seguito si riporta, quindi, la matrice di reato con individuato il rischio emerso attraverso il calcolo di P x D di cui al punto 3 del presente MOG e con specifica dei protocolli e/o procedure tali da rendere il rischio detto, ove ritenuto presente, come accettabile (intendendosi "accettabile" il rischio della commissione dei reati presupposto considerati esclusivamente attraverso l'elusione intenzionale e fraudolenta delle procedure e/o protocolli previste/i).

REATO	CONDOTTA	ATTIVITA' SENSIBILI	FUNZIONI E RISORSE UMANE COINVOLTE	quote	RI	PROTOCOLLI SPECIFICI	RR
Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.)	Falsificazione di documento informatico pubblico o avente efficacia probatoria	Tale reato potrebbe essere integrato mediante la contraffazione o l'alterazione di scritture private e/o attestato contenuto in supporti informatici, quali ad es. invio del F24 o mediante la falsa attestazione, in atti e documenti informatici, di fatti dei quali l'atto o il documento stesso è destinato a provare la verità (sostitutive di certificazione o dell'atto di notorietà ai sensi del D.P.R. 28 dicembre 2000, n. 445); gestione Sistri	CDA, AREA FINANZIARIA, AREA AMMINISTRAZIONE	fino 400 + interdittive		Mansionario, suddivisione dei compiti, codice etico, nomina DPO, procedure ex DPR 679/'16, gestione accessi, log, backup crittografati, incident response, formazione	A
Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)	Introduzione abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero mantenersi contro la volontà espressa o tacita di chi ha il diritto di escluderlo	1) accesso agli strumenti informatici aziendali da parte di dipendenti, amministratori e terzi autorizzati; 2) trattamento dei dati; 3) uso di hardware e software; 4) gestione e uso della posta elettronica 5) gestione Sistri	chiunque ha accesso ai pc aziendali	100 500 + interdittive		Mansionario, suddivisione dei compiti, codice etico, nomina DPO, procedure ex DPR 679/'16, gestione accessi, log, backup crittografati, incident response, formazione	A
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)	Procurarsi, riprodurre, diffondere, comunicare o consegnare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornire indicazioni o istruzioni idonee al predetto scopo, a fini di procurare a sé o ad altri un profitto o di arrecare ad altri un danno	1) accesso agli strumenti informatici aziendali da parte di dipendenti, amministratori e terzi autorizzati; 2) trattamento dei dati; 3) uso di hardware e software; 4) gestione e uso della posta elettronica 5) gestione Sistri	chiunque ha accesso ai pc aziendali	100 300		Mansionario, suddivisione dei compiti, codice etico, nomina DPO, procedure ex DPR 679/'16, gestione accessi, log, backup crittografati, incident response, formazione	A

Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)	distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici altrui	1) accesso agli strumenti informatici aziendali da parte di dipendenti, amministratori e terzi autorizzati; 2) trattamento dei dati; 3) uso di hardware e software; 4) gestione e uso della posta elettronica 5) gestione Sistri	chiunque ha accesso ai pc aziendali	LCC SCC + interattive		Backup giornaliero crittografato e verifica ripristino Controllo accessi e tracciamento log Monitoraggio integrità dati e file system Segnalazione incidenti a DPO	A
Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)	distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	1) accesso agli strumenti informatici aziendali da parte di dipendenti, amministratori e terzi autorizzati; 2) trattamento dei dati; 3) uso di hardware e software; 4) gestione e uso della posta elettronica 5) gestione Sistri	chiunque ha accesso ai pc aziendali			Segmentazione delle reti pubbliche / private Cifratura end-to-end dei flussi Accesso VPN certificato e autenticazione forte Audit log dedicato ai progetti pubblici	A
Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)	distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici altrui ovvero ostacolare gravemente il funzionamento di detti sistemi, mediante la introduzione o la trasmissione di dati, informazioni o programmi, distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ostacolarne gravemente il funzionamento	1) accesso agli strumenti informatici aziendali da parte di dipendenti, amministratori e terzi autorizzati; 2) trattamento dei dati; 3) uso di hardware e software; 4) gestione e uso della posta elettronica 5) gestione Sistri	chiunque ha accesso ai pc aziendali	LCC SCC + interattive		Ridondanza e continuità operativa (server mirror, backup on-site/off-site) Monitoraggio uptime e alert automatici Test periodici di disaster recovery Controlli fisici/logici accesso ai server Aggiornamenti di sicurezza e patch management	A
Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.)	distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità ovvero ostacolarne gravemente il funzionamento	1) accesso agli strumenti informatici aziendali da parte di dipendenti, amministratori e terzi autorizzati; 2) trattamento dei dati; 3) uso di hardware e software; 4) gestione e uso della posta elettronica 5) gestione Sistri	chiunque ha accesso ai pc aziendali	LCC SCC + interattive		Restrizioni accesso remoto e manutenzioni autorizzate Test di resilienza e simulazioni di blackout informatici	A

14. Norme generali di comportamento

Con riguardo all'utilizzo e gestione dei sistemi, strumenti, documenti o dati informatici, tutti coloro che operano per conto della società debbono conformarsi ai seguenti principi:

- rispetto delle procedure per la gestione della sicurezza informatica, delle procedure e policy nell'utilizzo degli strumenti informatici, delle reti aziendali, nella gestione delle password, della posta elettronica ecc.;
- applicazione delle procedure atte a prevenire e/o impedire la realizzazione di illeciti informatici da parte degli esponenti aziendali;
- rispetto procedure previste ex GDPR 679/16.

Nell'ambito dei suddetti comportamenti è fatto divieto in particolare di:

1) utilizzare gli strumenti, i dati ed i sistemi informatici in modo da recare danno a terzi, in particolare interrompendo il funzionamento di un sistema informatico o l'alterazione di dati o programmi informatici, anche a seguito dell'accesso abusivo, ovvero dell'intercettazione di comunicazioni;
2) detenere o diffondere indebitamente codici o programmi atti al danneggiamento informatico;
3) alterare o falsificare documenti informatici di qualsiasi natura o utilizzare indebitamente la firma elettronica;
4) porre in essere comportamenti in contrasto con leggi e regolamenti in materia di protezione e sicurezza di dati personali e sistemi informatici (in particolare, Codice in materia di protezione dei dati personali; provvedimenti del Garante della Privacy).

Ai fini dell'attuazione dei comportamenti di cui sopra sono individuate – in base al principio della separazione dei ruoli – le strutture aziendali preposte alla gestione della sicurezza dei dati e delle informazioni, nonché alla gestione delle infrastrutture di rete e dei sistemi e sono attribuiti alle medesime specifici compiti in materia di prevenzione dei delitti informatici e di trattamento illeciti di dati (rif. specifiche nomine e lettere d'incarico).

A seguito di quanto disposto nel provvedimento generale del 27.11.2008 del Garante per la protezione dei dati personali (in G.U. n. 300 del 24/12/2008 – "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"), ADOPERA ha provveduto alla nomina dell'amministratore di sistema ed ha implementato misure idonee alla registrazione e archiviazione degli accessi logici di sistema effettuati da tali soggetti (rif. "Lettera di incarico gestione e manutenzione dei sistemi informativi").

Le registrazioni sono inalterabili e comprendono le seguenti informazioni:

a) riferimenti temporali di log-in e log-out;
b) tipologia di accesso;
c) server di accesso;
d) nome login utente (solo amministratore);
e) dominio di accesso;
f) nome del PC e indirizzo IP

Si deve inoltre prevedere:

1) un monitoraggio periodico affinché la gestione del sistema informatico sia adeguata e corretta, avendo particolare riguardo alla verifica dei log di sistema ed applicativi al fine di individuare tempestivamente l'esistenza di attività che potrebbero determinare il mancato rispetto delle regole aziendali e al controllo della rete al fine di verificare l'esistenza di accessi e dispositivi non autorizzati;
2) la predisposizione di strumenti tecnologici atti a prevenire e/o impedire la realizzazione di illeciti informatici da parte del personale attraverso l'uso indebito o non autorizzato delle password, la detenzione o installazione di software non previsto dalle procedure aziendali, ivi compresi virus e spyware di ogni genere e natura e dispositivi atti all'interruzione di servizi o alle intercettazioni, l'accesso a siti protetti ovvero non visitabili, il collegamento non consentito di hardware alla rete aziendale.

Tali misure devono in particolare prevedere regole in merito:

- le restrizioni all'accesso fisico ai luoghi in cui sono collocati gli strumenti informatici/telematici;
- all'attribuzione e revoca delle password, tenendo conto delle mansioni aziendali per la quale viene richiesta/concessa;
- alla rimozione dei diritti di accesso al termine del rapporto di lavoro;
- al controllo e la tracciabilità degli accessi;
- alle modalità di svolgimento delle attività di gestione e manutenzione dei sistemi; alla previsione di controlli sulla idoneità della rete aziendale e sul suo corretto instradamento;

3) l'adozione di specifiche misure a garanzia del corretto utilizzo dei materiali coperti da diritti di proprietà intellettuale, anche attraverso procedure di controllo della installazione di software sui sistemi operativi;
4) l'adozione di specifici strumenti per la individuazione, prevenzione e ripristino dei sistemi rispetto a virus e altre vulnerabilità;
5) il costante aggiornamento del Documento Programmatico sulla Sicurezza aziendale;

6) la previsione di programmi di informazione, formazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali.

15. Protocolli preventivi

Oltre ai principi preventivi di carattere generale richiamati al punto 5.3.1 del presente Modello ed al "Manuale per la sicurezza ad uso degli incaricati", sono adottate le seguenti prescrizioni:

Governance e responsabilità

Adozione di una **Politica per la sicurezza informatica** approvata dalla Direzione.

Individuazione di un **Responsabile Sicurezza ICT** e coordinamento con il **DPO**.

Integrazione dei flussi informativi e delle segnalazioni cyber all'**Organismo di Vigilanza (OdV)**.

Gestione degli accessi e delle credenziali

Implementazione dell'**autenticazione a più fattori (MFA)** per tutti gli utenti con accesso ai sistemi sensibili.

Definizione di **livelli di accesso profilati** in base ai ruoli e alle mansioni.

Registro utenti e credenziali con procedure di attivazione, revoca e verifica periodica.

Rotazione trimestrale delle password e blocco automatico dopo tentativi multipli.

Divieto di condivisione delle credenziali e log delle attività utente.

Gestione infrastrutture e reti

Protezione delle reti aziendali mediante **firewall, antivirus, IDS/IPS e proxy sicuri**.

Segmentazione delle reti interne e separazione delle reti sanitarie da quelle amministrative.

Controllo e aggiornamento periodico delle patch di sicurezza.

Monitoraggio continuo degli accessi ai sistemi (audit-trail automatici).

Controlli fisici sugli accessi ai locali server e data center.

Verifica periodica di **integrità e ripristinabilità dei backup**.

Procedure per la **classificazione e gestione dei dati sensibili**, in linea con il GDPR.

Tracciabilità delle operazioni di inserimento, modifica o cancellazione dati.

Controllo versioni e **sicurezza del codice sorgente** (accessi limitati ai repository).

Verifica dell'integrità delle **release software e firmware** mediante checksum/hash.

Autorizzazione scritta per ogni intervento di manutenzione o aggiornamento remoto.

Audit di sicurezza informatica su piattaforme e dispositivi connessi.

Gestione dei fornitori ICT e servizi cloud

Selezione dei fornitori ICT su base di **requisiti di sicurezza e affidabilità tecnica**.

Inserimento nei contratti di **clausole 231, GDPR e SLA di sicurezza**.

Verifica periodica delle misure adottate dai cloud provider.

Obbligo di **notifica immediata di incidenti o vulnerabilità** da parte dei fornitori.

Adozione di un Piano di Incident Response integrato.

Identificazione di una **Cyber Incident Response Team (CIRT)** aziendale.

Segnalazione immediata a **DPO e OdV** in caso di data breach o evento cyber rilevante.

Conservazione dei **log e delle evidenze digitali** per analisi post-evento.

Comunicazione alle Autorità competenti entro i termini previsti (art. 33 GDPR).

Continuità operativa e disaster recovery

Redazione e aggiornamento annuale del **Business Continuity Plan (BCP)**.

Test di **disaster recovery** almeno una volta all'anno.

Definizione di **responsabilità, tempi e priorità di ripristino** dei servizi critici.

Documentazione delle simulazioni e reporting all'OdV.

Programma annuale di formazione obbligatoria su sicurezza informatica, privacy e reati informatici 231.

Campagne di **awareness contro phishing e social engineering**.

Sessioni periodiche di simulazione di incidenti informatici.

Formazione specifica per R&D, IT e personale sanitario su cyber-risk e data integrity.

Collegamento con gli altri strumenti di controllo

I protocolli ICT e cyber-security si coordinano con:

- la **Politica aziendale di sicurezza informatica**;
- il **Modello Privacy / GDPR**;
- i **contratti e gli SLA con fornitori ICT**.

Utilizzo strumentazione - E' fatto divieto di installare qualunque software sulla strumentazione in uso, notebook o workstation, qualora ciò non risulti espressamente richiesto ed autorizzato dalla Società. La Società si riserva di eliminare qualsiasi elemento hardware e/o software la cui installazione non sia stata appositamente prevista o autorizzata.
In caso di allontanamento dalla propria postazione di lavoro per più di 10 minuti, è fatto obbligo al dipendente di disconnettersi dal sistema (ciò può avvenire in modo automatico bloccando lo schermo).
Qualora si rendessero necessarie modifiche alle configurazioni impostate sul PC in uso, occorre darne comunicazione all'Amministratore di Sistema.

Utilizzo internet - Non è consentito l'uso improprio della "navigazione" in Internet (consistente in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività).
Non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo nei casi direttamente autorizzati dal Responsabile del trattamento dei dati e con il rispetto delle normali procedure di acquisto.
E' vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
Non è permessa la partecipazione, per motivi non professionali, a Forum, a social network, l'utilizzo di chat line e le registrazioni in guest book anche utilizzando pseudonimi (o nickname) potendo esporre a rischi di sicurezza la rete aziendale.
E' prevista, a cura dell'Amministratore di Sistema secondo quando impartito dal Responsabile del Trattamento, la configurazione di sistemi o l'utilizzo di filtri nel firewall che prevengano determinate operazioni a rischio.
E' richiesta la cancellazione periodica (almeno settimanale) dei file temporanei di internet, la cronologia, i cookie, le password eventuali salvate e le informazioni dei moduli. Tale funzione potrà essere impostata automaticamente sul browser internet utilizzato.
Attivare dei filtri idonei ad evitare navigazioni in siti non correlati all'attività lavorativa in relazione a parametri valutativi definiti dal Responsabile del Trattamento dei dati con la collaborazione dell'Amministratore si Sistema.
Attivare sistemi di monitoraggio della navigazione aziendale secondo le previsioni di cui al Provvedimento del Garante in materia di trattamento dati personali, Provvedimento del 1^ marzo 2007, effettuando monitoraggio generalizzato ed anonimo dei log di connessione (per il solo numero e durata delle sessioni internet) ed escludendo qualsiasi possibilità di risalire e /o identificare qualsiasi riferimento ai siti web visitati.

Utilizzo posta elettronica aziendale - Le caselle di posta elettronica date in uso al dipendente sono destinate ad un utilizzo di tipo aziendale.
Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita;
Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum, newsletter o mail-list, non attinenti all'attività lavorativa.
E' fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti in ottemperanza agli obblighi di fedeltà e correttezza.

Il dipendente /collaboratore è invitato, in caso di assenze programmate e comunque in caso di necessità, ad inserire nelle proprie e-mail, messaggi di avviso che contengano le "coordinate" di altro soggetto. In tal caso si dovrà contattare l'Amministratore di Sistema.
E' consentito che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato deleghi un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. L'interessato sarà informato alla prima occasione utile e di seguito provvederà alla sostituzione della propria password.
E' richiesta l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.
La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, è preferibile non usarla per inviare documenti di lavoro "Strettamente Riservati".
La gestione della posta elettronica certificata aziendale (non personale) è a cura dell'Amministrazione che provvede a soddisfare le richieste del personale della Società.

Inventario e verifica hardware e software – Tutte le apparecchiature hardware ed i software aziendali devono essere inventariati in apposito registro, indicando gli identificativi di macchina e/o di licenza e con attribuzione di una sigla/numero da apporre sull'apparecchiatura o sulla confezione del software ai fini dell'identificazione, della verifica e tracciabilità. Sui PC in uso non devono essere installati programmi che non siano regolarmente muniti di licenza.

Utilizzo supporti magnetici e dati - È fatto obbligo conservare, custodire e controllare i supporti informatici removibili contenenti dati, informazioni, notizie o immagini di attinenza aziendale, affinché nessun soggetto terzo non autorizzato ne prenda visione o possesso.
Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul pc in uso del dipendente.

In mansionario è esplicitamente previsto chi fa uso o meno di PC aziendali.

DELITTI IN VIOLAZIONE DELLA NORMATIVA SUL DIRITTO D'AUTORE

1. Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171 L. 633/1941)

Salvo quanto previsto dall'art. 171-bis e dall'art. 171-ter, è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:
(…)
a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;
(…)
La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

La norma punisce la messa a disposizione del pubblico, mediante immissione in un sistema di reti telematiche e/o con connessioni di qualunque genere, di un'opera dell'ingegno protetta o anche solo una parte di essa. Ai sensi del comma 2 dell'articolo 171, il reato previsto alla lettera a-*bis* è estinto con il pagamento, prima dell'apertura del dibattimento o prima dell'emissione del decreto penale di condanna, di una somma pari alla metà del massimo della pena stabilita al comma 1 (multa da euro 51 a euro 2.065);
tale previsione, che sarebbe comunque inapplicabile, ai sensi del comma 3, nel caso in cui la violazione della lettera a-*bis* fosse commessa in danno di un'opera inedita o con usurpazione della paternità, non modifica la rilevanza dell'illecito commesso ai fini della responsabilità amministrativa dell'ente in quanto essa continua a sussistere ogniqualvolta il reato si estingua per una causa diversa dall'amnistia (si veda l'art. 8, comma 1, lett. b) del D.Lgs. 231/01).

Il comma 3 prevede tre distinte circostanze aggravanti dei reati di cui al comma 1 poste a protezione degli interessi morali e personali degli autori delle opere dell'ingegno.

- La prima ipotesi aggravante concerne la protezione dell'opera altrui non destinata alla pubblicazione; la disposizione tutela l'interesse morale dell'autore che si concretizza nella riservatezza dell'opera e nella libertà di decidere sull'opportunità di renderla pubblica.

- La seconda aggravante è costituita dall'usurpazione della paternità dell'opera che si realizza con l'indicazione di una paternità dell'opera non rispondente al vero.
- La terza ipotesi aggravante punisce l'offesa all'onore e alla reputazione dell'autore realizzate attraverso le condotte di deformazione, modificazione o mutilazione dell'opera.

Il Decreto per questi reati prevede le seguenti sanzioni:

Sanzione pecuniaria: fino a 500 quote;
Sanzioni interdittive:
a) l'interdizione dall'esercizio dell'attività;
b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
e) il divieto di pubblicizzare beni o servizi.

2. Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171 bis L. 633/1941)

1. Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità.
2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli articoli 64-quinquies *e* 64-sexies*, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli* articoli 102-bis *e* 102-ter*, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità.*

L'ipotesi principale di reato è costituita dalla abusiva duplicazione o detenzione di software orientata al fine di trarne profitto, ricomprendendovi anche quei comportamenti che non sono sorretti dallo specifico scopo di conseguire un guadagno di tipo prettamente economico, bensì anche un'utilità mediata corrispondente al risparmio ottenuto utilizzando il programma abusivo.

Il Decreto per questi reati prevede le seguenti sanzioni:

Sanzione pecuniaria: fino a 500 quote;
Sanzioni interdittive:
a) l'interdizione dall'esercizio dell'attività;
b) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
e) il divieto di pubblicizzare beni o servizi.

3. Identificazione delle attività sensibili

Le attività sensibili che ADOPERA ha individuato al proprio interno sono le seguenti:

1) utilizzo di materiale (sia esso costituito da foto, opere letterarie, testi ecc.) per comunicazione, pubblicità, pubblicazione sul sito web della Società;
2) approvvigionamento di software, sua gestione e utilizzo

4. Valutazione del rischio e matrice-reati

La valutazione del rischio di commissione di tale fattispecie criminosa in ADOPERA viene espressa attraverso il seguente criterio già descritto al punto 3 del presente MOG.

Di seguito si riporta, quindi, la matrice di reato con individuato il rischio emerso attraverso il calcolo di P x D di cui al punto 3 del presente MOG e con specifica dei protocolli e/o procedure tali da rendere il rischio detto, ove ritenuto presente, come accettabile (intendendosi "accettabile" il rischio della commissione dei reati presupposto considerati esclusivamente attraverso l'elusione intenzionale e fraudolenta delle procedure e/o protocolli previste/i).

REATO	CONDOTTA	ATTIVITA' SENSIBILI	FUNZIONI E RISORSE UMANE COINVOLTE	LIVELLO	PI	PROTOCOLLI SPECIFICI	PR
Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171, L. n. 633/1941 comma 1 lett.a) bis)	Mettere a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa	Uso non autorizzato di software o immagini in materiale commerciale; uso improprio o installazione non autorizzata di programmi informatici aziendali; diffusione non autorizzata di opere, mancata cessione dei diritti	Amministratore Unico, amministrazione, commerciale, Ufficio acquisti, Ufficio ce personale, Direttori Tecnic	fino 500 + interdittive		Inventario e gestione licenze software -Verifica legale licenze open-source (component compliance); - Audit periodici repository e codice sorgente; Registro licenze e contratti di manutenzione -Controlli IT sugli installati - Clausole di utilizzo nel regolamento informatico aziendale; Verifica delle fonti e licenze immagini/testi -Archivio proof-of-license; Policy copyright aziendale -Controllo IT sui file caricati nei portali - Autorizzazione preventiva per software demo e materiali multimediali;Clausole contrattuali su titolarità e cessione dei diritti -Verifica dei diritti di proprietà delle opere commissionate	A
Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171, L. n. 633/1941 comma 3)	Mettere a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa, non destinata alla pubblicazione qualora ne risulti offesa l'onore o la reputazione	Uso non autorizzato di software o immagini in materiale commerciale; uso improprio o installazione non autorizzata di programmi informatici aziendali; diffusione non autorizzata di opere, mancata cessione dei diritti	Amministratore Unico, amministrazione, commerciale, Ufficio acquisti, Ufficio ce personale, Direttori Tecnic	fino 500 + interdittive		Inventario e gestione licenze software -Verifica legale licenze open-source (component compliance); - Audit periodici repository e codice sorgente; Registro licenze e contratti di manutenzione -Controlli IT sugli installati - Clausole di utilizzo nel regolamento informatico aziendale; Verifica delle fonti e licenze immagini/testi -Archivio proof-of-license; Policy copyright aziendale -Controllo IT sui file caricati nei portali - Autorizzazione preventiva per software demo e materiali multimediali;Clausole contrattuali su titolarità e cessione dei diritti -Verifica dei diritti di proprietà delle opere commissionate	A
Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-bis L. n. 633/1941 comma 1;	duplicare abusivamente, per trarne profitto, di programmi per elaboratore; importare, distribuire, vendere o detenere a scopo commerciale o imprenditoriale o concedere in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisporre mezzi per rimuovere o eludere dispositivi di protezione di programmi per elaboratori	Uso non autorizzato di software o immagini in materiale commerciale; uso improprio o installazione non autorizzata di programmi informatici aziendali; diffusione non autorizzata di opere, mancata cessione dei diritti	Amministratore Unico, amministrazione, commerciale, Ufficio acquisti, Ufficio ce personale, Direttori Tecnic	fino 500 + interdittive		Inventario e gestione licenze software -Verifica legale licenze open-source (component compliance); - Audit periodici repository e codice sorgente; Registro licenze e contratti di manutenzione -Controlli IT sugli installati - Clausole di utilizzo nel regolamento informatico aziendale; Verifica delle fonti e licenze immagini/testi -Archivio proof-of-license; Policy copyright aziendale -Controllo IT sui file caricati nei portali - Autorizzazione preventiva per software demo e materiali multimediali;Clausole contrattuali su titolarità e cessione dei diritti -Verifica dei diritti di proprietà delle opere commissionate	A
Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-bis L. n. 633/1941 comma 2;	Riprodurre, trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in pubblico, il contenuto di una banca dati; estrarre o reimpiegare la banca dati, distribuire, vendere o concedere in locazione banche di dati in violazione degli artt. 64 quinquies e sexies L.A.	Uso non autorizzato di software o immagini in materiale commerciale; uso improprio o installazione non autorizzata di programmi informatici aziendali; diffusione non autorizzata di opere, mancata cessione dei diritti	Amministratore Unico, amministrazione, commerciale, Ufficio acquisti, Ufficio ce personale, Direttori Tecnic	fino 500 + interdittive		Inventario e gestione licenze software -Verifica legale licenze open-source (component compliance); - Audit periodici repository e codice sorgente; Registro licenze e contratti di manutenzione -Controlli IT sugli installati - Clausole di utilizzo nel regolamento informatico aziendale; Verifica delle fonti e licenze immagini/testi -Archivio proof-of-license; Policy copyright aziendale -Controllo IT sui file caricati nei portali - Autorizzazione preventiva per software demo e materiali multimediali;Clausole contrattuali su titolarità e cessione dei diritti -Verifica dei diritti di proprietà delle opere commissionate	A
Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-ter L. n. 633/1941)	duplicare abusivamente, riprodurre, trasmettere o diffondere in pubblico con qualsiasi procedimento, in tutto o in parte, opere dell'ingegno destinate al circuito televisivo, cinematografico, alla vendita o al noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riprodurre, duplicare, trasmettere o diffondere abusivamente, vendere o commerciare, cedere a qualsiasi titolo o importare abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immettere un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa	Uso non autorizzato di software o immagini in materiale commerciale; uso improprio o installazione non autorizzata di programmi informatici aziendali; diffusione non autorizzata di opere, mancata cessione dei diritti	Amministratore Unico, amministrazione, commerciale, Ufficio acquisti, Ufficio ce personale, Direttori Tecnic	fino 500 + interdittive		Inventario e gestione licenze software -Verifica legale licenze open-source (component compliance); - Audit periodici repository e codice sorgente; Registro licenze e contratti di manutenzione -Controlli IT sugli installati - Clausole di utilizzo nel regolamento informatico aziendale; Verifica delle fonti e licenze immagini/testi -Archivio proof-of-license; Policy copyright aziendale -Controllo IT sui file caricati nei portali - Autorizzazione preventiva per software demo e materiali multimediali;Clausole contrattuali su titolarità e cessione dei diritti -Verifica dei diritti di proprietà delle opere commissionate	A
Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-septies L. n. 633/1941)	In qualità di produttore o importatore di supporti non soggetti al contrassegno SIAE, omettere di comunicare alla SIAE i dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione	Uso non autorizzato di software o immagini in materiale commerciale; uso improprio o installazione non autorizzata di programmi informatici aziendali; diffusione non autorizzata di opere, mancata cessione dei diritti	Amministratore Unico, amministrazione, commerciale, Ufficio acquisti, Ufficio ce personale, Direttori Tecnic	fino 500 + interdittive		Inventario e gestione licenze software -Verifica legale licenze open-source (component compliance); - Audit periodici repository e codice sorgente; Registro licenze e contratti di manutenzione -Controlli IT sugli installati - Clausole di utilizzo nel regolamento informatico aziendale; Verifica delle fonti e licenze immagini/testi -Archivio proof-of-license; Policy copyright aziendale -Controllo IT sui file caricati nei portali - Autorizzazione preventiva per software demo e materiali multimediali;Clausole contrattuali su titolarità e cessione dei diritti -Verifica dei diritti di proprietà delle opere commissionate	A

5. Norme generali di comportamento

Con riguardo ai delitti in materia di violazione del diritto d'autore, tutti coloro che operano per conto della società debbono conformarsi ai seguenti principi:

1) Verifica della paternità autorale di ogni opera o sua parte (sia essa letteraria, fotografica, pittorica, filmica ecc…) che ADOPERA intende utilizzare nell'ambito della promozione della propria attività o delle proprie pubblicazioni e delle condizioni poste dall'autore per l'utilizzo dell'opera;
2) Ottenimento dell'autorizzazione da parte dell'autore o da chi ne detiene legittimamente il rispettivo diritto all'utilizzo;
3) Utilizzazione dell'opera nei limiti dell'autorizzazione concessa dall'autore o dal legittimo detentore dei diritti.
4) Verifica dei limiti della licenza di ogni software acquistato prima di effettuare copie ulteriori a quella di back-up;
5) Verifica dei limiti di licenza di ogni opera tutelata dal diritto d'autore e su qualsiasi supporto essa sia, prima del suo utilizzo.

Nell'ambito dei suddetti comportamenti è fatto divieto di:

a) Utilizzare per pubblicazioni aziendali (compreso il sito web) opere o parte di esse senza l'autorizzazione del loro autore o del legittimo detentore del corrispondente diritto;
b) duplicare abusivamente programmi per elaboratore contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (S.I.A.E.);
c) (importare, distribuire e, vendere, detenere a scopo commerciale o imprenditoriale programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (S.I.A.E.);
d) rimuovere arbitrariamente o eludere i dispositivi applicati a protezione di un programma;
e) trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in pubblico del contenuto di una banca di dati;
f) eseguire dell'estrazione o del reimpiego della banca di dati;
g) distribuire, vendere o concedere in locazione una banca di dati.

Nel caso in cui venga affidata a terzi l'elaborazione di materiale pubblicitario o divulgativo della Società, il relativo contratto dovrà espressamente contemplare una clausola che richiami al rispetto della presente parte speciale del Modello organizzativo e che preveda l'obbligo da parte del terzo di garantire (a pena della risoluzione del contratto e del risarcimento del danno) che i testi, immagini e altre opere utilizzate per il prodotto elaborato per il committente sono lecitamente utilizzabili per tale scopo ai sensi della legge sul diritto d'autore.

6. Protocolli preventivi

Oltre ai principi preventivi di carattere generale richiamati al punto 5.3.1 del presente Modello, sono adottate le seguenti prescrizioni:

Verifica periodica delle licenze software: controllo attivo degli installati, utilizzi, utenti, versioni, rispetto termini contrattuali

Audit interno annuale sull'utilizzo del software e sulla conformità alle licenze (open source, proprietarie).

Revisione contratti con fornitori, sviluppatori e designer esterni con clausole specifiche di cessione o licenza dei diritti d'autore del software, contenuti multimediali e documentazione tecnica.

Policy aziendale d'uso software e contenuti digitali: definizione chiara di cosa può essere utilizzato, da chi, come e con quali restrizioni – formazione interna mirata.

Controllo e validazione delle librerie open source e moduli di terze parti integrati nei prodotti: verifica compatibilità licenze, rischi copyleft, obblighi di attribuzione

Centralizzazione e archiviazione delle prove di licenza (accordi, fatture, certificati d'autenticità) per ogni software utilizzato o contenuto acquistato/licenziato.

Monitoraggio e limitazione delle condivisioni interne ed esterne di contenuti protetti da diritto d'autore (manuali, immagini, video, software demo) attraverso policy, controlli tecnici e restrizioni accesso.

Formazione periodica per il personale (soprattutto IT, R&D, marketing) sui rischi legati al diritto d'autore, licenze software e uso corretto dei materiali digitali.

Sistemi di controllo tecnico/rintracciabilità (es. logging, tracciamento versioni, controllo repository software) per verificare l'origine dei componenti software e dei contenuti digitali integrati nei prodotti.

Meccanismo di segnalazione e gestione delle violazioni delle licenze o del copyright: segnalazione interna, analisi, azioni correttive, aggiornamento della policy.

ESCLUSIONI

Adopera non ritiene, al momento, di inserire nel presente MOG i rischi legati agli altri reati presupposto di cui al D.lgs. 231/01 non direttamente affrontati nel presente elaborato assumendosi i conseguenti eventuali rischi ritenuti, comunque, gestiti (es. reati tributari, societari ecc. astrattamente applicabili).

Casalecchio di Reno, 28 dicembre 2025

IL DATORE DI LAVORO
Legale rappresentate di Adopera S.r.l