

UNIROCK SRL
MODELLO DI ORGANIZZAZIONE E DI GESTIONE

Ex D.lgs. 8 GIUGNO 2001 N. 231

Sommario:

1. MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO ai sensi del D. lgs. 8 giugno 2001 n. 231	5
1.1 Il contenuto del D.lgs.n.231/01	5
1.2 Le sanzioni	6
1.3 Esimenti della responsabilità amministrativa	8
2. Adozione del Modello di organizzazione, gestione e controllo di Unirock S.r.l.	8
2.1 Premessa: cenni sulla storia e sull'oggetto sociale di Unirock S.r.l.	8
2.2 Motivazioni e finalità nell'adozione del Modello	9
2.3 Elementi di predisposizione e struttura del Modello	11
2.4 Approvazione, modifiche ed integrazioni del modello	12
3. L'Organismo di Vigilanza	13
3.1. Costituzione, nomina, requisiti e funzionamento dell'Organismo di Vigilanza.....	13
3.2 Funzioni e poteri dell'Organismo di Vigilanza.....	14
3.3 Flussi informativi dell'Odv nei confronti dell'Amministratore Unico.....	16
3.4 Flussi informativi nei confronti dell'Organismo di Vigilanza	16
3.4.1 Obblighi di informativa periodica	17
3.4.2 Obblighi di informativa ad evento.....	17
3.4.3 Segnalazioni ai sensi della L. 30 novembre 2017 n. 179.....	17
3.4.4 Segnalazioni ai sensi del Decreto Legislativo n. 24 del 10 marzo 2023	18
4. Informazione, formazione dei dipendenti e diffusione del Modello.....	21
5. Sistema sanzionatorio, disciplinare e civilistico	21
5.1 Il sistema disciplinare.....	21
5.1.1 I principali riferimenti normativi nel sistema disciplinare	22
5.1.2 I principi del sistema disciplinare.....	22
5.1.3 Contenuto e destinatari del codice disciplinare	22

5.2 Misure applicabili	23
5.2.1 Lavoratori dipendenti	23
5.2.2 Amministratore Unico.....	24
5.2.3 Soggetti esterni (lavoratori autonomi, parasubordinati, fornitori)	24
6. Principi generali di comportamento	25
7. Principi generali del sistema di controllo	26
8. IL MODELLO 231 DI UNIROCK S.R.L. – LA PARTE SPECIALE	27
PARTE SPECIALE “A” REATI CONTRO LA PUBBLICA AMMINISTRAZIONE (artt. 24 e 25 D.lgs 231/2001).....	28
A.1 Descrizione delle fattispecie normative	28
A.2 Attività sensibili	36
A.3 Sistemi di controllo.....	38
A.3.1 Principi generali di comportamento	38
A.3.2 Regole specifiche di comportamento.....	39
PARTE SPECIALE “B” REATI SOCIETARI (art. 25 <i>ter</i> D.lgs. 231/2001)	43
B.1 Descrizione delle fattispecie normative.....	43
B.2 Attività sensibili	47
B.3 Sistema di controllo.....	49
B.3.1 Principi generali di comportamento	49
B.3.2 Regole specifiche di comportamento.....	50
PARTE SPECIALE “C” REATI TRIBUTARI (art. 25 <i>quindiesdecies</i> d.lgs. 231/2001)	52
C.1 Descrizione delle fattispecie normative.....	52
C.2 Attività sensibili	56
C.3 Sistema di controllo.....	58
C.3.1 Principi generali di comportamento	58
C.3.2 Regole specifiche di comportamento	58
PARTE “D” REATI IN MATERIA DI SICUREZZA E SALUTE SUL LAVORO (art. 25 <i>septies</i> d.lgs. 231/2001).....	60
D.1 Descrizione delle fattispecie normative.....	60
D.2 Attività sensibili	63
D.3 Sistema di controllo.....	65
D.3.1. Finalità della presente parte speciale	65
D.3.2 Principi generali di comportamento.....	65

D.3.3 Regole specifiche di comportamento	67
D.3.4 Aree di rischio	68
D.3.5 L'Organizzazione.....	68
D.3.6 I soggetti	68
D.3.7 Principi di comportamento e di attuazione del processo decisionale in conformità alle norme OHSAS 45001	70
PARTE "E" REATI AMBIENTALI (art. 25 <i>undecies</i> d.lgs. 231/2001)	81
E.1 Descrizione delle fattispecie normative.....	81
E.2 Attività sensibili	91
E.3 Sistema di controllo.....	93
E.3.1 Principi generali di comportamento	93
E.3.2 Regole specifiche di comportamento	93
PARTE SPECIALE "F" DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (art. 24 <i>bis</i> d.lgs. 231/2001).....	98
F.1 Descrizione delle fattispecie normative	98
F.2 Attività sensibili	106
F.3 Sistema di controllo	107
F.3.1 Principi generali di comportamento	107
F.3.2 Regole specifiche di comportamento	109
PARTE SPECIALE "G"	110
REATI DI RICETTAZIONE, RICICLAGGIO ED IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ' AUTORIZICICLAGGIO (art. 25 <i>octies</i> d.lgs. 231/2001)	110
REATI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (art. 25 <i>octies</i> 1 d.lgs. 231/2001).....	110
G.1 Descrizione delle fattispecie	110
G.2 Attività sensibili	115
G.3 Sistema di controllo.....	117
G.3.1 Principi generali di comportamento	117
G.3.2 Regole specifiche di comportamento	118
PARTE SPECIALE "H" REATI DI CRIMINALITÀ ORGANIZZATA (art. 24 <i>ter</i> d.lgs. 231/2001)	120
H.1 Descrizione delle fattispecie normative	120
H.2 Attività sensibili.....	122
H.3 Sistema di controllo	125
H.3.1 Principi generali di comportamento.....	125

H.3.2 Regole specifiche di comportamento	125
PARTE “I” REATI CONTRO L’ATTIVITA’ GIUDIZIARIA (art. 25 <i>decies</i> d.lgs. 231/2001)	127
I.1 Descrizione delle fattispecie normative	127
I.2 Attività sensibili	129
I.3 Sistema di controllo	130
I.3.1 Principi di comportamento	130
PARTE SPECIALE “L” DELITTI CONTRO LA FEDE PUBBLICA (art. 25 <i>bis</i> d.lgs. 231/2001)	132
L.1 Descrizione delle fattispecie normative	132
L.2 Attività sensibili.....	134
L.3 Sistema di controllo	135
L.3.1 Principi di comportamento	135
PARTE “M”	136
IMPIEGO DI CITTADINI TERZI IL CUI SOGGIORNO È IRREGOLARE (art. 25 <i>duodecies</i> d.lgs. 231/2001).....	136
RAZZISMO E XENOFOBIA (art. 25 <i>terdecies</i> d.lgs. 231/2001)	136
M.1 Descrizione delle fattispecie normative	136
M.2 Attività sensibili.....	138
M.3 Sistema di controllo	139
M.3.1 Principi generali di comportamento – Impiego di cittadini terzi il cui soggiorno è irregolare (art. 25 <i>duodecies</i> d.lgs. 231/2001)	139
M.3.2 Principi generali di comportamento – Razzismo e xenofobia (art. 25 <i>terdecies</i> d.lgs. 231/2001) .	139

1. MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO ai sensi del D. lgs. 8 giugno 2001 n. 231

1.1 Il contenuto del D.lgs.n.231/01

Il Decreto, recante “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica”, ha introdotto nell’ordinamento giuridico italiano un regime di responsabilità amministrativa (assimilabile sostanzialmente alla responsabilità penale) a carico degli enti (da intendersi come società, associazioni, consorzi, etc., di seguito denominati “Enti”) per reati tassativamente elencati e commessi nel loro interesse o vantaggio:

- Da persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi (c.d. soggetti “*apicali*”), ovvero
- Da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati (c.d. “*sottoposti all'altrui direzione*”).

La responsabilità dell’ente si aggiunge a quella della persona fisica, che ha commesso materialmente il reato e sono entrambe oggetto di accertamento nel corso del medesimo procedimento innanzi al giudice penale. La previsione della responsabilità amministrativa di cui al Decreto coinvolge, nella repressione degli illeciti penali ivi espressamente previsti, gli Enti che abbiano tratto interesse e/o vantaggio dalla commissione del reato.

In base al disposto del D.lgs.n.231/01 e successive integrazioni - la responsabilità amministrativa dell'ente si configura con riferimento alle seguenti fattispecie di reato:

- Reati contro la Pubblica Amministrazione (artt. 24 e 25 d.lgs. 231/2001);
- Delitti informatici e trattamento illecito di dati (art. 24-*bis* d.lgs. 231/2001);
- Delitti di criminalità organizzata (art.24-*ter* d.lgs. 231/2001);
- Delitti di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-*bis* d.lgs. 231/2001);
- Delitti contro l’industria e il commercio (art. 25-bis.1 d.lgs. 231/2001);
- Reati societari (art. 25-*ter* d.lgs. 231/2001);
- Delitti con finalità di terrorismo o di eversione dell’ordine democratico (art. 25-*quater* d.lgs. 231/2001);
- Pratiche di mutilazione degli organi genitali femminili (art. 25-*quater.1* d.lgs. 231/2001);
- Delitti contro la personalità individuale (art. 25-*quinquies* d.lgs. 231/2001);
- Reati di abuso di mercato (art. 25-*sexies* d.lgs.231/2001);
- Delitti di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-*septies* d.lgs. 231/2001);
- Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-*octies* d.lgs. 231/2001);
- Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-*octies.1* d.lgs. 231/2001);

- Delitti in materia di violazione del diritto d'autore (art. 25-*novies* d.lgs. 231/2001);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-*decies* d.lgs. 231/2001);
- Reati ambientali (art. 25-*undecies* d.lgs. 231/2001) nonché con riferimento alle sole sanzioni, "combustione illecita di rifiuti" (art. 256-*bis* D.lgs. 152/2006);
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-*duodecies* d.lgs. 231/2001);
- Razzismo e xenofobia (art. 25-*terdecies* d.lgs. 231/2001);
- Reati transnazionali (art. 10 L. 146/06);
- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-*quaterdecies* d.lgs. 231/2001);
- Reati tributari (art. 25-*quinqüesdecies* d.lgs. 231/2001);
- Reati di contrabbando (art. 25-*sexiesdecies* d.lgs. 231/2001);
- Delitti contro il patrimonio culturale (art. 25-*septiesdecies* d.lgs. 231/2001);
- Delitti di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-*duodevicies* d.lgs. 231/2001);
- False o omesse dichiarazioni per il rilascio del certificato preliminare previsto dalla normativa attuativa della direttiva (UE) 2019/2121 del 27 novembre 2019 (art. 25 ter- lett. s. Ter).
- Delitti contro gli animali (art. 25-*undevicies* d.lgs. 231/2001)
- Reati in materia di violazione di misure restrittive dell'Unione Europea (art. 25-*octies*.2)

L'Ente è soggetto alla responsabilità amministrativa anche per gli illeciti dipendenti da delitti tentati. Nell'ipotesi di commissione nella forma del tentativo dei delitti indicati nel Capo I del D. Lgs.231/08, le sanzioni previste sono ridotte di un terzo alla metà.

L'art. 4 del Decreto disciplina, inoltre, le condizioni per cui l'Ente può rispondere anche dei reati commessi all'estero.

1.2 Le sanzioni

Le sanzioni previste dal Decreto per gli illeciti amministrativi dipendenti da reato sono di differenti tipologie:

- sanzioni pecuniarie;
- sanzioni interdittive;
- confisca;
- pubblicazione della sentenza.

Le sanzioni interdittive, di durata non inferiore a tre mesi e non superiore a due anni, hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'Ente e sono costituite da:

- interdizione dall'esercizio delle attività;
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

- divieto di contrarre con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- esclusione da agevolazioni, finanziamenti, contributi e sussidi, nonché la revoca di quelli eventualmente già concessi;
- divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive sono applicate nelle ipotesi tassativamente indicate dal Decreto, solo se ricorre almeno una delle seguenti condizioni:

- 1) l'Ente ha tratto dal reato un profitto di rilevante entità ed il reato è stato commesso:
 - da soggetti in posizione apicale; ovvero
 - da soggetti sottoposti all'altrui direzione e vigilanza quando la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
- 2) in caso di reiterazione degli illeciti.

Il tipo e la durata delle sanzioni interdittive sono stabiliti dal giudice tenendo conto della gravità del fatto, del grado di responsabilità dell'Ente e dell'attività svolta dall'Ente per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. In luogo dell'applicazione della sanzione, il giudice può disporre la prosecuzione dell'attività dell'Ente da parte di un commissario giudiziale.

Le sanzioni interdittive possono essere applicate all'Ente in via cautelare, quando sussistono gravi indizi per ritenere l'esistenza della responsabilità dell'Ente nella commissione del reato e vi sono fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa natura di quello per cui si procede (art. 45). Anche in tale ipotesi, in luogo della misura cautelare interdittiva, il giudice può nominare un commissario giudiziale.

L'inosservanza delle sanzioni interdittive costituisce un reato autonomo previsto dal Decreto come fonte di possibile responsabilità amministrativa dell'Ente (art. 23).

Le sanzioni pecuniarie, applicabili a tutti gli illeciti, sono determinate attraverso un sistema basato su "quote" in numero non inferiore a cento e non superiore a mille e di importo variabile fra un minimo di euro 258,23 ed un massimo di euro 1.549,37. Il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'Ente nonché dell'attività svolta per eliminare od attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. L'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente, allo scopo di assicurare l'efficacia della sanzione (art. 11 del Decreto).

Oltre alle predette sanzioni, il Decreto prevede che venga sempre disposta la confisca del prezzo o del profitto del reato, che può avere ad oggetto anche beni o altre utilità dei valori equivalenti, nonché la pubblicazione della sentenza di condanna in presenza di una sanzione interdittiva.

Ferme restando le ipotesi di riduzione delle sanzioni pecuniarie di cui agli artt. 12 (casi di riduzione delle sanzioni pecuniarie) e 26 (delitti tentati), non insorge alcuna responsabilità in capo agli Enti qualora gli stessi abbiano volontariamente impedito il compimento dell'azione ovvero la realizzazione dell'evento.

1.3 Esimenti della responsabilità amministrativa

L'articolo 6 del Decreto stabilisce che l'ente non ne risponde nel caso in cui dimostri di aver adottato ed efficacemente attuato, prima della commissione del fatto, "modelli di organizzazione di gestione e controllo idonei a prevenire reati della specie di quello verificatosi"

La medesima norma prevede, inoltre, l'istituzione di un organo di controllo interno all'ente con il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei predetti modelli, nonché di curarne l'aggiornamento

Detti modelli di organizzazione, gestione e controllo (di seguito denominati i "Modelli"), ex Art. 6, commi 2 e 3, del D.lgs.n.231/01, devono rispondere alle seguenti esigenze:

- Individuare le attività nel cui ambito possano essere commessi i reati previsti dal Decreto
- Prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire
- Individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati
- Prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli
- Introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello

Ove il reato venga commesso da soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da soggetti che esercitano, anche di fatto, la gestione e il controllo. L'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi, l'ente non risponde se prova che:

- Il compito di vigilare sul funzionamento e l'osservanza del Modello e di curare il suo aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo
- I soggetti hanno commesso il reato eludendo fraudolentemente il Modello
- Non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di controllo in ordine al Modello

2. Adozione del Modello di organizzazione, gestione e controllo di Unirock S.r.l.

2.1 Premessa: cenni sulla storia e sull'oggetto sociale di Unirock S.r.l.

La società Unirock S.r.l. nasce nel 2010 con sede legale ed operativa in Bolzano (BZ), alla Via Degli Artigiani, 16/A – 39100 ed ha quale oggetto sociale la realizzazione di opere infrastrutturali, stradali ed idrauliche, manutenzione delle gallerie.

Fanno capo alla Società le Unità locali site in Marocco , Visso (MC) e Sospirolo (BL)

L'impegno serio e concreto profuso in oltre 25 anni di attività ha portato importanti riconoscimenti per la qualità dei lavori eseguiti dall'azienda, che oggi opera in ambito nazionale ed intercontinentale.

In particolare, UNIROCK S.r.l. come da ATTESTAZIONE SOA, opera nei settori:

- costruzione di strade, autostrade, ponti, viadotti, ferrovie, metropolitane (OG3),
- opere d'arte nel sottosuolo (OG4),
- opere fluviali, di difesa, di sistemazione idraulica e di bonifica (OG8),
- opere di ingegneria naturalistica (OG 13),
- lavori in terra (OS1),
- finiture di opere generali di natura edile e tecnica (OS7),
- apparecchiature strutturali speciali (OS11),
- opere strutturali speciali (OS21),
- barriere stradali di sicurezza (OS12A),
- produzione, montaggio e installazione di barriere paramassi e ferma neve (OS12B),
- demolizioni specializzate (OS23),
- sistemi antirumore per infrastrutture di mobilità (OS34).

2.2 Motivazioni e finalità nell'adozione del Modello

Unirock è una società consapevole della complessa realtà in cui si trova ad esercitare la propria attività, operando principalmente nel settore degli appalti, pubblici e privati, attraverso la partecipazione a gare d'appalto in Italia ed all'estero.

Tutto ciò rafforza l'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali.

Unirock nella sua attività si pone come obiettivi:

- la promozione della salute e della sicurezza e benessere sul posto di lavoro;
- la tutela dell'ambiente;
- l'adozione di principi di correttezza e trasparenza nei rapporti con le terze parti ed in particolar modo con la Pubblica Amministrazione;
- la trasparenza delle operazioni commerciali che devono essere improntate ad un Codice Etico scritto;
- il rispetto dei diritti umani e delle norme in materia di diritti sul posto di lavoro;
- un dialogo trasparente e costruttivo con i lavoratori di ogni livello.

A tal fine, sebbene l'adozione del Modello sia prevista dalla legge come facoltativa e non obbligatoria, l'azienda ha avviato un'analisi della propria organizzazione volta a verificare la rispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto.

Tale iniziativa è stata assunta nella convinzione che l'adozione del Modello – in linea con le indicazioni della Giurisprudenza in materia e con le Linee Guida emanate e successivamente aggiornate da Confindustria - possa costituire un valido strumento di sensibilizzazione di tutti coloro che operano in nome e per conto della società, affinché tengano comportamenti corretti e lineari nell'espletamento delle proprie attività, tali da prevenire il rischio di commissione dei reati previsti dal Decreto stesso.

In particolare, attraverso l'adozione del Modello, l'azienda si propone di perseguire le seguenti principali finalità:

- 1) Determinare, in tutti coloro che operano in nome e per conto dell'azienda nelle aree di attività a rischio, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, nella commissione di illeciti passibili di sanzioni penali comminabili nei loro stessi confronti e di sanzioni disciplinari direttamente irrogabili all'azienda.
- 2) Ribadire che tali forme di comportamento illecito sono fortemente condannate dall'azienda, in quanto le stesse sono comunque contrarie, oltre che alle disposizioni di legge, anche al "Codice Etico" al quale l'azienda intende attenersi nell'esercizio delle attività aziendale.
- 3) Consentire alla società, grazie ad un'azione di monitoraggio sulle aree di Attività a rischio, di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

Si considerano Destinatari del presente Modello:

- L'Amministratore Unico che per Statuto ha tutti i poteri per l'amministrazione e gestione ordinaria e straordinaria della Società;
- Tutti i dipendenti, i collaboratori ed i terzi che intrattengono rapporti contrattuali, a qualsiasi titolo, anche occasionale e temporaneo, con Unirock Srl;
- Revisori Legali che hanno il compito di effettuare controlli per verificare che la Società sia correttamente amministrata e la contabilità sia tenuta regolarmente.
- L'Organismo di Vigilanza che ha il compito di vigilare sul funzionamento e l'osservanza del Modello;

Tutti coloro che intrattengono rapporti commerciali e/o finanziari di qualsiasi natura con Unirock, sono tenuti al rispetto, attraverso apposite clausole contrattuali, del Modello e del Codice Etico che lo accompagna

L'attenzione sempre dimostrata dalla Società verso il rispetto della normativa vigente e le tematiche fondamentali quali la qualità, la sicurezza e l'ambiente hanno portato alla scelta conseguire le seguenti certificazioni:

UNI EN ISO 9001 N. IT 11/0538 del 24/12/2002 – Sistema di Gestione Qualità

UNI EN ISO 14001 N. IT 16/0763 del 09/09/2016 – Sistema di Gestione Ambientale

OHSAS 18001 N. IT11/0016 dal 22/12/2010 fino al 27/01/2021 SGSSL

UNI EN ISO 45001 N. IT 11/0016 del 27/01/2021 – Sistema di Gestione Salute Sicurezza sul Lavoro

UNI EN ISO 39001 N. IT 21/0401 del 02/05/2021 – Sistema di Gestione Sicurezza Stradale

UNI EN ISO 37001 N. IT 25/1094 del 08/10/2025 – Sistema di Gestione Anticorruzione

SOA ATTESTA S.P.A N.102091/7/00 del 25/09/2025 con scadenza 19/01/2030 Attestazione Qualificazione Esecuzione Lavori Pubblici

SA 8000:2014 N.IT 21/0593 del 16/06/2021 - Sistema di Gestione Responsabilità Sociale di Impresa

2.3 Elementi di predisposizione e struttura del Modello

Nella predisposizione del Modello, si è tenuto in debito conto dell'organizzazione e delle caratteristiche di Unirock, procedendo attraverso diverse fasi così riassunte:

- mappatura delle “attività a rischio” per individuare quelle nel cui ambito, per loro natura, possono essere commessi i reati di cui al Decreto e pertanto da sottoporre ad analisi e monitoraggio;
- analisi dei protocolli e procedure adottate da Unirock al fine di identificare e valutare i rischi che possa essere commesso uno dei reati presupposto nell'ambito delle diverse attività;
- definizione delle eventuali azioni di miglioramento da intraprendere finalizzate, ad integrare e garantire i principi di controllo;
- modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati.

L'attività sopra descritta è avvenuta nel concreto attraverso interviste con l'Amministratore Unico ed i dipendenti della Società, nonché l'esame e la raccolta di precise informazioni in ordine a:

- mappa delle attività aziendali “sensibili” ovvero di quelle nel cui ambito, per loro natura, possono essere commessi i reati di cui al Decreto e pertanto da sottoporre ad analisi e monitoraggio;
- analisi dei protocolli e delle procedure in essere e definizione delle eventuali implementazioni finalizzate, con riferimento alle attività aziendali “sensibili”, a presidiare in modo concreto le aree di rischio;
- tipologia dell'ente;
- quadro normativo applicabile all'ente;
- sistema organizzativo ed autorizzativo: attraverso principalmente l'analisi delle procure e deleghe esistenti per valutare la ripartizione dei poteri e delle competenze;
- gestione dei flussi finanziari: tenuto conto della struttura interna semplificata della Società, attraverso l'analisi dei presidi e delle cautele organizzative da essa adottate idonee a garantire, in modo effettivo, la tracciabilità, la trasparenza e la correttezza delle operazioni, anche attraverso i controlli e le verifiche di consulenti esterni ed indipendenti;
- esistenza di contributi pubblici e normativa ad essi applicabile;
- procedure esistenti o prassi consolidate;

- identificazione dell'Organismo di Vigilanza (di seguito anche "Organismo" o "Odv") e l'attribuzione di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
- definizione dei flussi informativi nei confronti dell'Organismo;
- attività di informazione, sensibilizzazione e diffusione a tutti i dipendenti delle regole comportamentali e delle procedure istituite;
- verifica del recepimento, dell'integrazione e implementazione del Modello all'interno dell'Azienda, e dei comportamenti aziendali, con relativo aggiornamento periodico (controllo ex post).

Il Modello è costituito da una "Parte Generale" ove si descrivono le componenti essenziali dello stesso con particolare riferimento all'Organismo di Vigilanza, la formazione del personale e la diffusione del Modello, il sistema disciplinare e le misure da adottare in caso di mancata osservanza delle prescrizioni contenute nello stesso e i principi generali di comportamento validi per tutte le aree di rischio.

Nelle "Parti Speciali" si fa esplicito riferimento ai soli reati contemplati dal D.lgs. 231/2001 ed alle relative aree funzionali che, all'esito dell'attività di mappatura dei rischi, si ritengono applicabili alla realtà di Unirock S.r.l.

Costituiscono, inoltre, parte integrante del Modello i seguenti documenti:

- Codice Etico (Allegato I), esplicita i valori a cui i Destinatari devono adeguarsi, accettando responsabilità, assetti, ruoli e regole;
- Dichiarazione annuale dell'Amministratore Unico quale responsabile amministrazione e finanza (All II)
- Documento di Valutazione dei rischi (All. III) predisposto in osservanza di quanto previsto dal D. Lgs. 81/08;

2.4 Approvazione, modifiche ed integrazioni del modello

Essendo il Modello un "atto di emanazione dell'organo dirigente" (in conformità alle prescrizioni dell'articolo 6, comma 1, lett. a del Decreto) la sua approvazione, adozione e recepimento sono rimesse alla competenza dell'Amministratore Unico.

Anche il Codice Etico viene approvato dall'Amministratore Unico in quanto parte integrante del Modello Organizzativo a cui è allegato.

Parimenti è compito della Società disporre e successivamente approvare l'aggiornamento del Modello in occasione di modifiche ed integrazioni ritenute sostanziali quali, tra le altre:

- novità legislative con introduzione di nuove figure di reato presupposto che richiedano un programma di aggiornamento e una nuova mappatura delle attività a rischio di commissione degli stessi nella realtà organizzativa di Unirock S.r.l.;
- revisione periodica del Modello anche in relazione a cambiamenti significativi della struttura organizzativa o dei settori di attività istituzionali;
- significative violazioni del Modello e/o esiti di verifiche sull'efficacia del medesimo.

Tuttavia, le modifiche ed integrazioni di carattere formale o che non incidono sull'assetto organizzativo vengono immediatamente recepite nello stesso, come negli allegati dello stesso, in maniera tempestiva su richiesta dell'Organismo di Vigilanza e recepimento della Società.

3. L'Organismo di Vigilanza

3.1. Costituzione, nomina, requisiti e funzionamento dell'Organismo di Vigilanza

L'articolo 6, comma 1, lett. b), del D.lgs.n.231/01 individua, come requisito affinché l'ente possa essere esonerato dalla responsabilità "amministrativa" dipendente dalla commissione dei reati specificati nel Decreto legislativo stesso, l'istituzione di un Organismo di Vigilanza *"dotato di autonomi poteri di iniziativa e di controllo"*.

L'Organismo di Vigilanza (di seguito Odv) può essere monocratico ovvero collegiale, ed i suoi componenti possono essere esterni alla Società.

Le caratteristiche previste dal Decreto, l'esperienza maturata nella prassi e le dimensioni di Unirock S.r.l., che è società medio-piccola, hanno portato alla nomina di un organismo composto da due membri, individuati in figure professionali esterne alla Società, esperti nell'ambito legale, tecnico ed economico .

In tal modo vengono soddisfatti i requisiti richiesti dalla normativa per l'efficace svolgimento dei propri compiti:

- **Autonomia e indipendenza:** l'Organismo di Vigilanza deve essere sprovvisto di compiti operativi, non può ricoprire incarichi di gestione, esecutivi o di controllo che creino situazioni di conflitto di interesse. È configurato in posizione di staff al vertice e riporta direttamente ed unicamente all'Amministratore Unico. Le attività poste in essere dall'Organismo di Vigilanza non possono essere sindacate. L'Organismo è inoltre autonomo nel senso regolamentare, ovvero ha la possibilità di determinare le proprie regole comportamentali e procedurali nell'ambito dei poteri e delle funzioni determinate dall'Amministratore Unico.
- **Professionalità:** l'Organismo di Vigilanza viene scelto tra professionisti affidabili con competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Deve, infatti, possedere capacità specifiche, in relazione a qualsiasi tecnica utile per prevenire la commissione di reati, per scoprire quelli già commessi e individuarne le cause, nonché per verificare il rispetto dei modelli da parte degli appartenenti all'organizzazione aziendale.
- **Continuità di azione:** al fine di garantire la costante attività di monitoraggio e di aggiornamento del Modello e la sua variazione al mutare delle condizioni aziendali di riferimento. L'Odv può avvalersi, nello svolgimento delle proprie funzioni, di consulenti esterni.

L'Organismo di Vigilanza è nominato dall'Amministratore Unico e rimane in carica per la durata indicata all'atto della nomina o, in mancanza di tale termine, fino alla decisione dell'Amministratore Unico che provvede alla nuova nomina / rinnovo. I membri possono ricoprire la carica per più mandati.

Costituiscono cause di ineleggibilità o di revoca quali componenti dell'Organismo di Vigilanza:

- l'aver riportato condanna penale anche con sentenza non definitiva o nella forma dell'applicazione della pena sull'accordo delle parti ex art. 444 C.p.p. per delitti di cui ai reati presupposto ex D.lgs. 231/01,

per i delitti puniti a titolo di dolo e le contravvenzioni che comportino l'applicazione di una pena accessoria di cui all'art. 19 c.p. o previste da specifiche disposizioni di legge;

- qualsiasi condanna, anche non definitiva, che comporti l'applicazione di una pena accessoria di cui all'art. 19 c.p. o previste da specifiche disposizioni di legge;
- l'applicazione di una misura di sicurezza, personale o patrimoniale, l'applicazione di una misura di prevenzione personale o patrimoniale o l'applicazione di una misura di prevenzione antimafia personale o patrimoniale;
- la dichiarazione di interdizione o di inabilità ai sensi del Codice Civile;
- una delle situazioni in cui risulta gravemente compromessa l'autonomia e l'indipendenza del singolo componente, come pure il conflitto di interessi con la Società Unirock.

Al verificarsi di alcune delle sopra indicate cause di ineleggibilità e/o revoca i titolari decadranno automaticamente.

Costituisce inoltre causa di sospensione dalla carica, per tutta la durata della misura, l'applicazione di una misura cautelare personale (custodia cautelare in carcere o in luogo di cura, arresti domiciliari, divieto e obbligo di dimora, obbligo di presentarsi alla Polizia Giudiziaria, divieto di espatrio) e l'applicazione di una misura interdittiva (sospensione dall'esercizio di un pubblico ufficio o servizio, divieto temporaneo di esercitare determinate attività professionali e imprenditoriali).

All'Organismo di Vigilanza ed ai suoi componenti si applicano le norme del Codice Civile in tema di mandato.

3.2 Funzioni e poteri dell'Organismo di Vigilanza

Le funzioni svolte dall'Organismo di Vigilanza possono essere così riassunte:

- Valutazione dell'adeguatezza del Modello e promozione del suo aggiornamento.
- Vigilanza sull'effettività del Modello ovvero della corrispondenza tra i comportamenti concreti dei destinatari ed il Modello istituito.
- Promozione e verifica dell'attività di informazione e formazione dei destinatari del Modello.
- Gestione dei flussi informativi.

In particolare, i compiti dell'Organismo di Vigilanza sono così definiti:

- Effettuare periodicamente ricognizioni sull'attività aziendale ai fini del controllo del mantenimento dei requisiti richiesti e dell'eventuale aggiornamento della mappatura delle aree a rischio di reato ai sensi del D.lgs. 231/01, proponendo all'Amministratore Unico le opportune modifiche ed integrazioni del Modello in relazione ai mutamenti dell'organizzazione aziendale e della normativa applicabile;
- Promuovere tutte le azioni necessarie per assicurare l'efficacia nel prevenire i comportamenti illeciti e la funzionalità nel tempo del Modello;
- Verificare periodicamente, nelle aree ritenute a rischio di reato, che l'attività venga svolta in conformità al Modello adottato anche attraverso:
 - ricognizioni mirate su determinate operazioni o specifici atti posti in essere da Unirock;

- attivazione e svolgimento di audit interni, raccordandosi con i dipendenti della Società;
- attuazione delle procedure previste dal Modello;
- Definire e curare, in attuazione del Modello, il flusso informativo che consenta all'Organismo di Vigilanza di essere periodicamente aggiornato sulle attività valutate a rischio di reato, nonché stabilire modalità di comunicazione per acquisire conoscenza delle eventuali violazioni del Modello;
- Promuovere adeguato processo formativo per il personale, finalizzato a fornire a tutti i dipendenti la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al D. Lgs. 231/2001, alla diffusione della conoscenza e della comprensione del Modello nonché alla predisposizione della documentazione interna necessaria al fine della sua efficace attuazione;
- Promuovere adeguate iniziative di informazione e conoscenza nei confronti di tutti i destinatari del Modello compresi tutti i soggetti con i quali Unirock intrattiene i rapporti commerciali;
- Segnalare eventuali violazioni del Modello all'Amministratore Unico che valuterà l'irrogazione dell'eventuale sanzione e monitorarne l'applicazione.

Ai fini dello svolgimento dei compiti assegnati, all'Organismo di Vigilanza spettano i poteri di seguito indicati:

- Accedere nei limiti posti dalla normativa sulla Privacy e dallo Statuto dei Lavoratori, a tutta la documentazione aziendale che ritiene rilevante nonché agli strumenti informatici e informativi relativi alle attività classificate o classificabili come a rischio di reato;
- Avvalersi dell'ausilio di tutti i dipendenti della Società, i quali hanno un correlativo obbligo di informazione nei confronti dell'Odv;
- Avvalersi di consulenti esterni con specifiche competenze professionali in materia, per l'esecuzione delle operazioni tecniche necessarie alla funzione di controllo. Tali consulenti dovranno sempre riferire i risultati del proprio operato all'Odv;
- Procedere, qualora si renda necessario, all'audizione diretta dei dipendenti;
- Richiedere informazioni a collaboratori, consulenti esterni, partners e fornitori di Unirock.

Le attività dell'Odv non devono essere preventivamente autorizzate da nessun organo; la mancata collaborazione con l'Odv costituisce un illecito disciplinare.

All'Odv è garantita la disponibilità di risorse finanziarie necessarie per lo svolgimento dell'attività di propria competenza tramite apposita previsione di un budget a sua disposizione .

L'Odv ha, come previsto dalla legge, autonomi poteri di iniziativa e controllo al fine di vigilare sul funzionamento e l'osservanza del Modello, ma non ha poteri coercitivi o di intervento modificativi della struttura aziendale o sanzionatori nei confronti di tutti i dipendenti, consulenti esterni, società di service, partner o fornitori; questi poteri sono demandati all'Amministratore Unico.

In ragione dei compiti affidati, l'Amministratore Unico è in ogni caso l'unico organo aziendale chiamato a svolgere un'attività di vigilanza sull'adeguatezza dell'intervento dell'Odv, in quanto all'organo dirigente compete comunque la responsabilità ultima del funzionamento e dell'efficacia del Modello.

3.3 Flussi informativi dell'Odv nei confronti dell'Amministratore Unico

In merito all'attività di *reporting*, l'Odv di Unirock provvede ad inviare all'Amministratore Unico una relazione annuale che avrà ad oggetto:

- l'attività complessivamente svolta nel corso del periodo;
- le criticità emerse sia in termini di comportamenti o eventi interni, sia in termini di efficacia del Modello;
- le segnalazioni ricevute nel corso del periodo di riferimento e le azioni intraprese dall'Odv stesso e dagli altri soggetti interessati a fronte delle stesse;
- le attività cui non si è potuto procedere per giustificate ragioni di tempo e/o risorse;
- lo stato dell'attuazione del Modello, con l'indicazione dei necessari e/o opportuni interventi correttivi dello stesso ed il loro livello di implementazione;
- il piano delle attività per l'anno successivo.

L'Organismo dovrà, invece, riferire tempestivamente all'Amministratore Unico in merito a:

- qualsiasi violazione del Modello ritenuta fondata, di cui sia venuto a conoscenza per segnalazione da parte dei dipendenti o che abbia accertato l'Organismo stesso;
- carenze organizzative o procedurali idonee a determinare il concreto pericolo di commissione di reati rilevanti ai fini del Decreto;
- modifiche normative rilevanti per l'attuazione ed efficacia del Modello;
- mancata collaborazione da parte dei dipendenti;
- esistenza di procedimenti penali nei confronti di soggetti che operano per conto di Unirock, ovvero di procedimenti a carico degli stessi in relazione a reati rilevanti ai sensi del Decreto;
- esito degli accertamenti disposti a seguito dell'avvio di indagini da parte dell'autorità giudiziaria in merito a reati rilevanti ai sensi del Decreto;
- ogni altra informazione ritenuta utile ai fini dell'assunzione di determinazioni urgenti da parte dell'Amministratore Unico.

3.4 Flussi informativi nei confronti dell'Organismo di Vigilanza

L'art. 6 lettera d) del D. Lgs. 231/01 riporta quale requisito esimente nell'adozione del Modello organizzativo *“prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli”*.

L'Obbligo di informazione nei confronti dell'Organismo di Vigilanza costituisce, dunque, uno strumento ulteriore per agevolare l'attività di vigilanza sull'efficacia del Modello e di accertamento a posteriori delle cause che hanno reso possibile il verificarsi dell'illecito.

L'obbligo di fornire informazioni all'Organismo di Vigilanza: Amministratore Unico, Responsabile Amministrazione, Responsabile Magazzino Manutenzione, Responsabile Ufficio Gare, Dirigenti ai sensi di delega ex art. 16 D.lgs. 81/08, Preposti di cantiere, RSPP.

3.4.1 Obblighi di informativa periodica

Tra i flussi informativi da trasmettere all'Organismo di Vigilanza con cadenza periodica si possono annoverare:

- Rapporto annuale relativo ad eventuali contenziosi penali, civili ed amministrativi in essere a cura del Responsabile Area Amministrativa;
- Rapporto annuale in materia di salute e sicurezza sui luoghi di lavoro a cura del Responsabile del Servizio di Prevenzione e Protezione;
- Annualmente elenco delle gare d'appalto e degli affidamenti ricevuti superiore ad 1.000.000,00 a cura del Resp. Ufficio Gare
- Dichiarazione annuale dell'Amministratore Unico quale responsabile amministrazione e finanza

3.4.2 Obblighi di informativa ad evento

Tra i flussi informativi da trasmettere all'Organismo di Vigilanza al verificarsi dell'evento si possono annoverare:

- i provvedimenti e/o notizie provenienti dall'autorità giudiziaria, o da qualsiasi altra autorità (es. Agenzia Entrate, GdF, INL) dai quali si evinca lo svolgimento di indagini/accertamenti, anche nei confronti di ignoti, per i reati o gli illeciti amministrativi di cui al Decreto;
- le richieste di assistenza legale inoltrate dai dipendenti o ex-dipendenti in caso, dei collaboratori esterni di Unirock in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto (per i collaboratori esterni se il procedimento si riferisce ad atti compiuti nello svolgimento dell'incarico a favore di Unirock);
- i procedimenti disciplinari svolti e le eventuali sanzioni irrogate quando riguardano fatti rilevanti ai sensi del Decreto 231 ovvero i provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- Segnalazione di Infortunio sul lavoro con indicazione della data, prognosi, causa, eventuali azioni correttive adottate e segnalazione di chiusura o proroga (con indicazione delle cause);
- Segnalazione di incidente ambientale con indicazione della causa ed eventuali azioni correttive adottate.

3.4.3 Segnalazioni ai sensi della L. 30 novembre 2017 n. 179

Tutti i Destinatari del Modello devono portare a conoscenza dell'Odv qualunque informazione, di qualsiasi tipo, proveniente anche da terzi, di cui siano venuti a diretta conoscenza, attinente alla violazione del Modello o ad eventuali altre irregolarità indirizzando le comunicazioni ad "Organismo di Vigilanza di Unirock S.r.l.", Via degli Artigiani 16/A , 39100 Bolzano.

In alternativa è stato istituito un indirizzo di posta elettronica dedicato: odvunirock231@gmail.com. Tale casella di posta elettronica è accessibile ai soli membri dell'Organismo di Vigilanza.

L'obbligo riguarda principalmente le risultanze delle attività poste in essere dalla Società, nonché le atipicità e le anomalie riscontrate.

A tale riguardo valgono le seguenti prescrizioni:

- Devono essere raccolte le segnalazioni relative a possibili ipotesi di commissione di reati previsti dal Decreto o, comunque, il compimento di atti idonei diretti alla realizzazione degli stessi; ed ancora comportamenti non in linea con le regole di condotta previste dal Modello e dalle relative procedure;
 - L'Odv valuterà le segnalazioni ricevute e adotterà i provvedimenti conseguenti, dopo aver ascoltato, se ritenuto opportuno, l'autore della segnalazione ed il responsabile della presunta violazione;
- Le segnalazioni di condotte illecite dovranno essere circostanziate e fondate su elementi di fatto precisi e concordanti, e potranno essere effettuate utilizzando gli appositi canali indicati.

L'Organismo di Vigilanza prenderà in considerazione tutte le segnalazioni ricevute valutando le eventuali conseguenti iniziative a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto ogni relativa decisione assunta.

La Società Unirock S.r.l.:

- richiede all'O.d.V. di gestire la segnalazione in modo confidenziale, così da assicurare la riservatezza dell'identità del segnalante e di altre persone coinvolte o a cui si fa riferimento nella segnalazione, fatti salvi gli obblighi di legge e la tutela dei diritti della società o delle persone accusate erroneamente e/o in mala fede;
- vieta rappresaglie e protegge coloro che fanno segnalazioni in buona fede da ritorsioni, discriminazioni o penalizzazioni, dirette o indirette, per motivi collegati alla segnalazione.

La Società provvederà, in caso di riscontrata violazione delle misure di tutela del segnalante anche da parte dell'O.d.V., nonché di riscontrate segnalazioni infondate effettuate con dolo o colpa grave, ad identificare ed applicare la sanzione ritenuta più adeguata alla circostanza.

3.4.4 Segnalazioni ai sensi del Decreto Legislativo n. 24 del 10 marzo 2023

Il D.lgs. n.24 del 10 marzo 2023 *“Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali”* disciplina la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato.

Con il termine <<whistleblowing>> s'intende la procedura di segnalazione spontanea da parte di un individuo interno o esterno all'azienda, detto “segnalante” (in inglese “whistleblower”) di un illecito o di un'irregolarità acquisite nell'ambito del proprio contesto lavorativo.

Attraverso i canali di segnalazione, possono essere segnalate violazioni delle norme ai sensi del d.lgs.231/2001 e violazioni del Modello 231 comprensivo del Codice Etico e di Condotta, violazioni della normativa europea in materia di sicurezza dei trasporti, tutela dell'ambiente, radioprotezione e sicurezza nucleare, sicurezza degli alimenti e dei mangimi e salute e benessere degli animali, salute pubblica, protezione dei consumatori, tutela

della vita privata e protezione dei dati personali, sicurezza delle reti e dei sistemi informativi, violazioni della normativa in materia di concorrenza e aiuti di Stato.

Pertanto, possono essere oggetto di segnalazione anche:

- gli elementi che riguardano condotte volte ad occultare le violazioni sopra indicate;
- le attività illecite non ancora compiute, ma che il segnalante ritenga ragionevolmente possano verificarsi in presenza di elementi concreti precisi e concordanti;
- le informazioni sulle violazioni, compresi i fondati sospetti.

Non sono ricomprese, tra le informazioni sulle violazioni segnalabili o denunciabili, le notizie palesemente prive di fondamento, le informazioni che sono già totalmente di dominio pubblico, nonché le informazioni acquisite sulla sola base di indiscrezioni o vociferazioni scarsamente attendibili (c.d. voci di corridoio).

Le disposizioni del decreto non si applicano, tra le altre, *“alle contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante che attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate”*.

In adempimento al Decreto Legislativo n. 24 /2023 la Società ha implementato i canali di segnalazione coerentemente alle previsioni ivi previste.

Pertanto, coloro che siano a conoscenza o che sospettino il verificarsi di violazioni, possono effettuare segnalazioni con le seguenti modalità:

a) attraverso il canale <https://whistleblowing.dataservices.it/UNIROCK>

b) attraverso il canale esterno attivato dall'ANAC, ovvero divulgata pubblicamente (rendendo di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone), solo quando, si verifichi anche una sola delle seguenti ipotesi:

- la segnalazione interna e/o esterna, già effettuata, non ha avuto seguito;
- il Segnalante ha fondati motivi di ritenere che, utilizzando il canale interno e/o esterno, non sarebbe dato efficace seguito alla segnalazione;
- il Segnalante ha il fondato timore di subire ritorsioni;
- la Violazione può costituire pericolo imminente o palese per l'interesse pubblico.

La gestione delle segnalazioni si attiene al sistema di protezione come previsto nel Decreto, secondo, tra gli altri, i seguenti principi:

- **tutela della riservatezza: L'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.**

Il divieto di rivelare l'identità del whistleblower è da riferirsi non solo al nominativo del segnalante ma anche a tutti gli elementi della segnalazione, dai quali si possa ricavare, anche indirettamente, l'identificazione del segnalante, inoltre la tutela dell'identità del segnalante si estende nel procedimento penale, contabile e disciplinare.

È tutelata anche l'identità delle persone coinvolte e delle persone menzionate nella segnalazione: *“I soggetti del settore pubblico e del settore privato, l'ANAC, nonché le autorità amministrative cui l'ANAC trasmette le segnalazioni esterne di loro competenza, tutelano l'identità delle persone coinvolte (segnalate) e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione nel rispetto delle medesime garanzie previste in favore della persona segnalante”*.

Peraltro, la segnalazione è sottratta all'accesso agli atti amministrativi e al diritto di accesso civico generalizzato;

- **protezione dalle ritorsioni:** È vietata ogni forma di ritorsione anche solo tentata o minacciata. Il Decreto, infatti, ha accolto una nozione ampia di ritorsione, *“qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto”*;
La gestione delle comunicazioni di ritorsioni nel settore pubblico e nel settore privato compete all'Anac;
- **rispetto delle limitazioni della responsabilità** per chi riveli o diffonda informazioni sulle violazioni coperte dall'obbligo di segreto o relative alla tutela del diritto d'autore o alla protezione dei dati personali ovvero che offendono la reputazione della persona coinvolta o denunciata.
La scriminante penale opera *“quando, al momento della rivelazione o diffusione, vi fossero fondati motivi per ritenere che la rivelazione o diffusione delle stesse informazioni fosse necessaria per svelare la violazione e la segnalazione, la divulgazione pubblica o la denuncia all'autorità giudiziaria o contabile è stata effettuata nelle modalità richieste”*;
- **tutela dell'integrità delle segnalazioni:** tutte le segnalazioni ricevute e la relativa documentazione sono adeguatamente archiviate per garantire che non vi siano dispersioni e/o trasmissioni di informazioni in contrasto con il principio di tutela della riservatezza del segnalante e del segnalato;
- **dovere di indipendenza e professionalità nella gestione delle segnalazioni:** i soggetti preposti alla gestione delle segnalazioni svolgono la propria attività assicurando le necessarie condizioni di obiettività ed indipendenza, competenza e diligenza professionale. Unirock ne cura la specifica formazione in tema di privacy e “whistleblowing”;
- **dovere di formazione ed informazione:** Unirock prevede adeguate iniziative di informazione e formazione del Personale sul tema e le misure, gli strumenti ed i canali di Segnalazioni adottati; assicura anche adeguata informativa nei confronti dei Terzi, anche tramite la pubblicazione sul sito internet istituzionale.

La Società assicura l'effettività del sistema di segnalazione attraverso la previsione di un sistema disciplinare idoneo a sanzionare le condotte che ne compromettano l'integrità o violino le tutele previste dalla normativa vigente, nel rispetto dei principi di proporzionalità e gradualità.

Si richiama specificatamente il “Regolamento per la gestione delle segnalazioni di condotte illecite e tutela del dipendente segnalante” adottato dalla Società.

4. Informazione, formazione dei dipendenti e diffusione del Modello

Unirock promuove la conoscenza dell'adozione del Modello, dei protocolli in esso contenuti e dei loro aggiornamenti tra tutti i dipendenti che sono pertanto tenuti a conoscerne il contenuto, ad osservarli e contribuire alla loro attuazione.

Il Modello viene messo a disposizione di ogni dipendente anche attraverso inserimento del Modello e del Codice Etico nel sito internet, la sua consegna ai nuovi assunti al momento dell'assunzione, e-mail o comunicazioni di aggiornamento sulle modifiche apportate al Modello o al Codice Etico.

Unirock promuove, altresì, la conoscenza e la divulgazione del Modello attraverso un'apposita attività di formazione ai propri dipendenti, differenziata in funzione della qualifica dei destinatari, sui contenuti del D.lgs. 231/01, del Modello e del Codice Etico.

Relativamente ai fornitori, consulenti, collaboratori e clienti, Unirock assicura un'adeguata informativa mediante l'inserimento del Modello e del Codice Etico sul sito internet e l'inserimento di apposita clausola nei contratti, ordini e convenzioni stipulate con i terzi, circa l'adozione da parte della Società del Modello e del Codice Etico e l'avvertenza che ogni comportamento posto in essere in contrasto con le linee di condotta indicate nel Modello stesso, tale da comportare il rischio di commissione di un reato sanzionato dal Decreto, potrà determinare, la risoluzione del rapporto contrattuale.

5. Sistema sanzionatorio, disciplinare e civilistico

La predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni contenute nel Modello è condizione essenziale per assicurare l'effettività del Modello stesso. Al riguardo, infatti, l'articolo 6, comma 2, lettera e) del Decreto prevede che i Modelli devono "introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello".

5.1 Il sistema disciplinare

Il Sistema Disciplinare idoneo a sanzionare il mancato rispetto del Modello di Organizzazione e gestione e del Codice Etico è da considerarsi elemento indispensabile del Modello stesso e strumento per garantirne la sua efficace attuazione.

Al riguardo l'art. 6, comma 2, lettera e) del D.lgs. 231/01 prevede che i Modelli di organizzazione e gestione debbano "introdurre un Sistema Disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello".

Anche l'art. 7, comma 4, lettera b) del Decreto stabilisce che l'efficace attuazione del Modello richiede anche "un Sistema Disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello".

Unirock S.r.l. ha costruito il proprio Sistema Disciplinare, riportato nel presente documento, basandosi sulla disciplina degli articoli sopra menzionati, delle pronunce giurisprudenziali e sulle indicazioni fornite dalle Linee Guida di Confindustria.

Il Sistema Disciplinare è diffuso a tutti i prestatori di lavoro ed è portato a conoscenza anche mediante affissione nelle bacheche aziendali.

5.1.1 I principali riferimenti normativi nel sistema disciplinare

- norme di legge in materia: in particolare l'art. 7 della Legge 300/70 (Statuto dei Lavoratori), l'art. 2104 del c.c. (diligenza del prestatore di lavoro), l'art. 2105 del c.c. (obbligo di fedeltà), l'art. 2106 c.c. (sanzioni disciplinari) l'art. 2118 c.c. (recesso dal contratto) e l'art. 2119 c.c. (recesso per giusta causa);
- disposizioni del contratto collettivo applicabile: C.C.N.L. Edilizia Industria;
- art. 1176 (diligenza nell'adempimento), 1218 c.c. (responsabilità del debitore) e 1453 c.c. e successivi (risoluzione del contratto);
- art. 1382 c.c. (effetti della clausola penale) e 1453 c.c. e successivi (risoluzione del contratto) e 1453 c.c. e successivi (risoluzione del contratto).

Le sanzioni previste nel Sistema Disciplinare, parte integrante del Modello di organizzazione gestione e controllo, hanno la stessa natura disciplinare delle disposizioni di cui all'art. 7 dello Statuto dei Lavoratori e sue successive modifiche e delle sanzioni disciplinari previste dall'art. 9 C.C.N.L. Edilizia Industria e sue successive modifiche.

5.1.2 I principi del sistema disciplinare

Il Sistema Disciplinare ha una funzione preventiva, l'inosservanza del Modello e del Codice Etico comporta l'attivazione di un meccanismo sanzionatorio interno, tempestivo ed immediato da parte della Società.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, al fine di contrastare gli eventuali comportamenti prodromici alla commissione dei reati ex decreto legislativo 231/01.

L'individuazione della sanzione avviene secondo il principio di adeguatezza e proporzionalità ed in relazione alla gravità del reato o, comunque, della violazione commessa ed assicurando, nei casi previsti dalla legge e dal CCNL, il coinvolgimento del soggetto interessato con la possibilità di giustificare il suo comportamento successivamente alla contestazione dell'addebito anche mediante la facoltà di farsi assistere da un rappresentante dell'associazione sindacale cui aderisce o conferisce mandato.

Il sistema disciplinare viene costantemente monitorato dall'Odv.

5.1.3 Contenuto e destinatari del codice disciplinare

Il Sistema Disciplinare di Unirock s.r.l. contiene:

- i fatti che sono considerati disciplinarmente rilevanti;
- le relative sanzioni in armonia con le norme di legge ed il CCNL;
- le procedure di contestazione e irrogazione delle sanzioni.

Le sanzioni individuate nel presente Sistema Disciplinare si applicano, con aspetti specifici, a:

- lavoratori dipendenti (che non rivestono la funzione di dirigente);
- lavoratori dirigenti ex art. 16 D.Lgs. 81/08;

- Amministratore Unico;
- soggetti esterni che agiscono per conto di Unirock S.r.L. (lavoratori autonomi, lavoratori parasubordinati, fornitori, professionisti, etc.).

5.2 Misure applicabili

Il procedimento di applicazione delle sanzioni nei confronti di tutti i dipendenti avviene nel rispetto delle disposizioni delle normative vigenti. Sarà cura dell'Odv trasmettere all'Amministratore Unico una nota contenente le generalità del soggetto responsabile della violazione, la descrizione della condotta contestata, l'indicazione delle previsioni del Modello che risultano essere violate e gli eventuali documenti a supporto della contestazione affinché si proceda con gli adempimenti previsti.

5.2.1 Lavoratori dipendenti

I comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali dedotte nel presente Modello costituiscono illeciti disciplinari.

Le sanzioni irrogabili nei riguardi dei lavoratori dipendenti (quadri, impiegati ed operai), nel rispetto delle norme del Codice Civile, delle procedure di cui all'articolo 7 della Legge 30 maggio 1970, n. 300 (Statuto Lavoratori) e dell'articolo 99 del CCNL e loro successive modifiche, potranno essere:

- rimprovero verbale;
- rimprovero scritto;
- multa non superiore a tre ore di retribuzione oraria calcolata sul minimo tabellare;
- sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni;
- licenziamento per mancanze ai sensi dell'art. 100 del CCNL.

Ad integrazione delle condotte già riportate nel CCNL si considerano sanzionabili, ai sensi del presente Sistema Disciplinare e nel rispetto delle norme del Codice Civile, delle procedure di cui all'articolo 7 della Legge 30 maggio 1970, n. 300 (Statuto Lavoratori) e dagli artt. 99 e 100 del CCNL e loro successive modifiche, le seguenti condotte:

- inosservanza delle procedure, dei protocolli (generali e specifici), dei regolamenti previsti e richiamati nel Modello diretti ad attuare le decisioni e la formazione della Società in relazione ai reati da prevenire;
- inosservanza dei principi e delle norme di comportamento presenti nel Codice Etico adottato dalla Società;
- omissione degli obblighi derivanti dall'art. 20 del D.lgs. 81/08 in materia di sicurezza e salute sui luoghi di lavoro;
- ostacolo o elusione dei controlli dell'organismo di Vigilanza, impedimento dell'accesso ad informazioni ed alla documentazione nei confronti dei soggetti incaricati ai controlli;
- omessa informativa all'organismo di Vigilanza nonché all'organo dirigente relativamente a flussi informativi specificati nel Modello;

- omessa segnalazione delle inosservanze o irregolarità commesse da altri lavoratori e da soggetti apicali;
- violazione delle misure adottate dalla Società a tutela del segnalante degli illeciti (whistleblower), che si sostanzia nella violazione delle misure di tutela garantite al segnalante, oppure nella proposizione (dolosa o gravemente colposa) di segnalazioni tendenziose, o che comunque si rivelino infondate.

La valutazione e la scelta della sanzione da irrogare tra quelle possibili previste deve tener conto della gravità delle condotte e della eventuale reiterazione del comportamento, in quanto reiterare un comportamento nel tempo costituisce sintomo di gravità della violazione.

Le contestazioni, che daranno luogo all'applicazione di sanzioni diverse dal semplice rimprovero verbale, devono essere necessariamente scritte, in modo da garantire la tracciabilità dell'applicazione nel sistema e i precedenti a carico del soggetto sanzionato.

5.2.2 Amministratore Unico

La Società valuta con rigore le infrazioni al presente Modello poste in essere da coloro che rappresentano il vertice della Società e ne manifestano l'immagine verso i dipendenti, il socio, i creditori e il pubblico.

In caso di violazione del Modello da parte dell'Amministratore Unico, l'OdV prenderà gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea soci al fine di adottare le misure più idonee previste dalla legge e/o la revoca di deleghe e/o incarichi eventualmente conferiti.

In ogni caso, è fatta salva la facoltà delle società di proporre azioni di responsabilità e risarcitorie.

5.2.3 Soggetti esterni (lavoratori autonomi, parasubordinati, fornitori)

Qualora i comportamenti in violazione del Modello o del Codice Etico fossero posti in essere da lavoratori autonomi, fornitori o altri soggetti che operano in forza di contratti per conto di Unirock s.r.l. si potrà procedere alla risoluzione del contratto ex articolo 1453 c.c. (risoluzione del contratto).

Nei confronti di tali soggetti non sussiste alcun potere disciplinare da parte dei vertici della società, salvo il potere di quest'ultima di intervenire sulla base del contratto attenendosi alla disciplina contrattuale prevista dal codice civile.

Le sanzioni dovranno corrispondere a quanto inserito nelle clausole contrattuali e alle norme di legge in materia specifica di ciascun rapporto (clausole risolutive espresse che facciano esplicito riferimento al rispetto delle disposizioni del Modello e del Codice etico).

6. Principi generali di comportamento

È fatto obbligo per tutti i destinatari del Modello di Organizzazione Gestione e Controllo di rispettare le regole, i principi e le procedure aziendali previste nel Modello stesso e nei documenti interni della Società ivi richiamati.

È fatto altresì divieto di:

- Porre in essere, dare causa o concorrere alla realizzazione di comportamenti che possano integrare, direttamente o indirettamente, qualsiasi fattispecie di reato disciplinata nella legislazione vigente e, in particolare, i reati di cui al Decreto;
- Porre in essere, dare causa o concorrere alla realizzazione di comportamenti tali da favorire qualsiasi situazione di conflitto di interessi nei confronti della P.A. o di un privato in relazione a quanto previsto dalle suddette ipotesi di reato;
- Porre in essere, dare causa o concorrere alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle considerate, possano potenzialmente diventarle;

Pertanto, è fatto obbligo ai Destinatari di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle normative nazionali ed internazionali vigenti, del Codice Etico, dei principi contenuti nel presente Modello e delle procedure societarie;
- osservare una condotta tesa a garantire il regolare funzionamento di Unirock s.r.l., assicurando ed agevolando ogni forma di controllo sulla gestione da parte dell'Odv.;
- applicare costantemente le regole del presente Modello e del Codice Etico;
- curare che nessun rapporto venga iniziato con persone o enti che non abbiano intenzione di adeguarsi ai principi etici di Unirock s.r.l.;
- accertarsi dell'identità delle controparti commerciali, siano esse persone fisiche che persone giuridiche e dei soggetti per conto dei quali esse eventualmente agiscono.

Ogni comportamento difforme da quanto previsto nel presente Modello ed ogni violazione dei divieti che comportino il rischio di commissione di un reato costituisce illecito disciplinare e avrà come conseguenza l'applicazione delle sanzioni secondo quanto previsto ai punti precedenti.

7. Principi generali del sistema di controllo

Unirock S.r.l., tenuto conto della dimensione organizzativa e del numero di dipendenti, stabilisce i propri presidi secondo i principi indicati:

- **Documentazione rigorosa:** ogni decisione relativa a spese, ordini, pagamenti e operazioni significative deve essere formalizzata per iscritto (ad esempio, con ordini di spesa, verbali, note interne, email ufficiali).
- **Tracciabilità:** tutte le operazioni devono essere registrate in modo da consentire la ricostruzione completa del processo decisionale e dell'esecuzione. Per ogni operazione vi deve essere un adeguato supporto documentale.
- **Controllo a posteriori:** le operazioni devono essere oggetto di verifica periodica, anche tramite la revisione contabile o la supervisione di un consulente esterno.
- **Accesso alle informazioni:** il sistema deve garantire che le informazioni siano disponibili e consultabili, anche da parte di soggetti terzi incaricati di vigilare sul funzionamento del modello

In particolare, ciascuna operazione/attività relativa ad ogni processo rilevante deve essere adeguatamente documentata. I documenti rilevanti devono:

- essere opportunamente formalizzati;
- riportare la data di compilazione e la firma del compilatore;
- essere archiviati, a cura del responsabile amministrativo e con modalità tali da non permettere la modifica successiva se non con apposita evidenza, in luoghi idonei alla conservazione, anche al fine di tutelare la riservatezza dei dati in essi contenuti e di evitare deterioramenti o smarrimenti.

Qualora sia previsto l'utilizzo di sistemi informatici per lo svolgimento delle attività sensibili, gli stessi assicurano:

- la corretta imputazione di ogni singola operazione ai soggetti che ne sono responsabili;
- la tracciabilità di ogni operazione effettuata (inserimento, modifica e cancellazione) dai soli utenti abilitati;
- l'archiviazione e conservazione delle registrazioni prodotte.

Le informazioni che confluiscono nella contabilità devono attenersi ai principi di chiarezza, trasparenza, correttezza, completezza ed accuratezza. Ogni alterazione, modifica che dovesse emergere rispetto a quanto una determinata funzione aziendale abbia in evidenza, va immediatamente segnalata all'Organismo di Vigilanza.

8. IL MODELLO 231 DI UNIROCK S.R.L. – LA PARTE SPECIALE

La Parte Speciale ha la finalità di definire linee, regole e principi di comportamento che tutti i destinatari del Modello 231 dovranno seguire al fine di prevenire, nell'ambito delle specifiche attività sensibili svolte nella società, la commissione di reati previsti dal Decreto e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Nello specifico, la Parte Speciale del Modello 231 ha lo scopo di:

- Indicare le modalità che gli esponenti aziendali sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- Fornire all'Odv ed alle altre funzioni di controlli gli strumenti per esercitare le attività di monitoraggio, controllo e verifica;

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi e rispettare:

- i principi contenuti nel Codice Etico;
- il Modello 231;
- le procedure aziendali e le istruzioni di servizio;
- Le procure, determinazioni di incarico;
- Le comunicazioni organizzative;
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto.

È inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge.

Nei paragrafi successivi verranno presi in esame i soli reati che, all'esito dell'analisi dei rischi, si ritiene potrebbero essere concretamente posti in essere da Unirock s.r.l. nell'esercizio della sua attività tipica.

Per i reati non ricompresi nelle singole parti speciali, Unirock richiama i principi espressi nel Codice Etico adottato ed il complesso dei protocolli e delle procedure dettate con riguardo alla prevenzione dei reati indicati per le Parti Speciali del Modello.

Ogni singola parte speciale illustra:

- le **singole fattispecie di reato** previste dal Decreto e ritenute realizzabili da Unirock s.r.l.;
- le **attività sensibili** e le relative funzioni coinvolte;
- il **sistema di controllo interno** inteso quali: principi etici; il sistema organizzativo formalizzato e chiaro; le regole di comportamento generali e specifiche da tenere nello svolgimento delle suddette attività; le procedure operative volte a regolamentare le attività; i poteri autorizzativi e di firma coerenti con le responsabilità organizzative.

PARTE SPECIALE “A” REATI CONTRO LA PUBBLICA AMMINISTRAZIONE (artt. 24 e 25 D.lgs 231/2001)

A.1 Descrizione delle fattispecie normative

Al fine di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili ai sensi del d.lgs. n. 231/2001, si riporta, qui di seguito, una breve descrizione dei reati richiamati dall’art. 24, dall’art. 25.

Preliminare, tuttavia, all’analisi delle fattispecie di reato contro la pubblica amministrazione è la delimitazione delle nozioni di pubblico ufficiale e incaricato di pubblico servizio, soggetti coinvolti di detti reati.

È importante sottolineare come la figura del pubblico ufficiale e dell’incaricato di pubblico servizio siano individuate dalla legge non sulla base del criterio della appartenenza o dipendenza da un ente pubblico, ma con riferimento alla natura dell’attività svolta in concreto dalla medesima, ovvero, rispettivamente, pubblica funzione e pubblico servizio.

Anche un soggetto estraneo alla Pubblica Amministrazione (di seguito anche PA) può, dunque, rivestire la qualifica di pubblico ufficiale o di incaricato di pubblico servizio, quando eserciti una delle attività definite come tali dagli artt. 357 e 358 c.p. (ad es. vedasi, dipendenti di istituti bancari ai quali siano affidate mansioni rientranti nel "pubblico servizio", ecc.).

Pubblici Ufficiali

Ai sensi dell’art. 357, primo comma, Codice penale, è considerato pubblico ufficiale agli effetti della legge penale colui il quale esercita *“una pubblica funzione legislativa, giudiziaria o amministrativa”*.

La norma definisce la nozione di “pubblica funzione amministrativa”, ma non le funzioni legislative e giudiziarie poiché meno problematiche nell’individuazione dei soggetti che le esercitano.

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”*.

Dunque, la definizione normativa fa riferimento innanzitutto alla natura della disciplina, per cui 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.

La norma, inoltre, definisce quali “funzioni pubbliche” quelle attività amministrative che rispettivamente ed alternativamente costituiscono esercizio di:

- poteri deliberativi;
- poteri autoritativi;
- poteri certificativi.

Secondo le definizioni sopra riportate, quindi, assumono la qualifica di pubblici ufficiali non solo i soggetti al vertice politico amministrativo dello Stato o di enti territoriali, ma anche – sempre riferendoci ad un’attività di altro ente pubblico retta da norme pubblicistiche – tutti coloro che, in base allo statuto nonché alle deleghe che esso consenta, ne formano legittimamente la volontà e/o la portino all’esterno in forza di un potere di rappresentanza.

Alla luce dei principi sopra enunciati, si può affermare che la categoria di soggetti più problematica è certamente quella che ricopre una “pubblica funzione amministrativa”

Incaricati di un pubblico servizio

L’art. 358 c. p. definisce *“incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio”*

Per pubblico servizio deve intendersi *“una 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 “pubblico servizio” viene individuato attraverso due criteri, uno positivo ed uno negativo. Il “servizio”, affinché possa definirsi pubblico, deve essere disciplinato da norme di diritto pubblico ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

Il legislatore ha inoltre precisato che non può mai costituire “servizio pubblico” lo svolgimento di “semplici mansioni di ordine” né la “prestazione di opera meramente materiale”. Con riferimento alle attività che vengono svolte da soggetti privati in base ad un rapporto concessorio con un soggetto pubblico, si ritiene che ai fini della definizione come pubblico servizio dell’intera attività svolta nell’ambito di tale rapporto concessorio non è sufficiente l’esistenza di un atto autoritativo di investitura soggettiva del pubblico servizio, ma è necessario accertare se le singole attività che vengono in questione siano a loro volta soggette a una disciplina di tipo pubblicistico.

La giurisprudenza ha individuato la categoria degli incaricati di un pubblico servizio, ponendo l’accento sul carattere della strumentalità ed accessorialità delle attività rispetto a quella pubblica in senso stretto.

Inoltre, l’art. 322-bis estende la punibilità di reati contro la Pubblica Amministrazione anche alle ipotesi in cui l’illecito coinvolga membri delle Corti Internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri.

A.1.1. Peculato (art. 314 c. 1 c.p.)

La norma punisce il comportamento del pubblico ufficiale o dell’incaricato di pubblico servizio che, avendo per ragioni del suo ufficio o servizio il possesso o la disponibilità di danaro o di altra cosa, se ne appropria e finisce per comportarsi nell’utilizzo della stessa come se ne fosse il proprietario, disponendo di quella res ben al di là di quelle che sono le corrispondenti destinazioni funzionali. Si tratta quindi di un reato cd “proprio”

previsto a carico del soggetto pubblico che può essere imputato al privato a titolo di concorso sulla base della consapevolezza della proprietà pubblica della res e della “conoscibilità della qualifica soggettiva del soggetto agente”.

Si sottolinea, inoltre, che ai sensi dell’art. 25, comma 1, D.lgs. 231/01 il reato rileva solo quando il fatto offende gli interessi finanziari dell’Unione europea.

A.1.2. Indebita destinazione di denaro o cose simili (art. 314 *bis* c.p.)

La norma punisce il pubblico ufficiale o l’incaricato di un pubblico servizio che, avendo per ragione del suo ufficio il possesso o la disponibilità di denaro o altra cosa mobile altrui, li destina ad un uso diverso da quello imposto da specifiche disposizioni di legge o da atti avente forza di legge che non lasciano margini di discrezionalità. È richiesto, inoltre, che l’agente procuri intenzionalmente a sé o ad altri un ingiusto vantaggio patrimoniale o arrechi ad altri un danno ingiusto.

Anche per questo reato l’art. 25, comma 1, D.lgs. 231/01 ne riconduce l’applicabilità esclusivamente al caso in cui l’offesa sia diretta agli interessi finanziari dell’Unione europea.

A.1.3 Peculato mediante profitto dell’errore altrui (art. 316 c.p.)

La norma punisce il pubblico ufficiale o l’incaricato di un pubblico servizio, nell’esercizio delle funzioni o del servizio, giovandosi dell’errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altre utilità. Anche in questo caso, come per il peculato “semplice”, si tratta di reato cd “proprio” previsto a carico del soggetto pubblico che può essere imputato al privato a titolo di concorso sulla base della consapevolezza della proprietà pubblica della res e della “conoscibilità della qualifica soggettiva del soggetto agente”.

La pena prevista per il reato in oggetto è la reclusione da sei mesi a tre anni, aggravata da sei mesi a quattro anni quando il fatto offende gli interessi finanziari dell’Unione europea e il danno o il profitto sono superiori a euro 100.000.

Anche per questo reato l’art. 25, comma 1, D.lgs. 231/01 ne riconduce l’applicabilità esclusivamente al caso in cui l’offesa sia diretta agli interessi finanziari dell’Unione europea.

A.1.4 Malversazione di erogazioni pubbliche (art. 316 *bis* c.p.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto dallo Stato o da altro ente pubblico o dall’Unione europea, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, non si proceda all’utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell’aver distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l’attività programmata si sia comunque svolta). La pena prevista per il reato in oggetto è la reclusione da sei mesi a quattro anni.

Si pensi alla richiesta ed all'ottenimento di un finanziamento pubblico erogato in vista dell'assunzione presso la Società di personale appartenente a categorie privilegiate, ovvero alla ristrutturazione di immobili danneggiati in occasione di calamità naturali che, una volta conseguito, non venga destinato a dette finalità.

Tenuto conto che il momento in cui il reato viene consumato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.

A.1.5 Indebita percezione di erogazioni pubbliche (art. 316 *ter* c.p.)

Il reato si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute - si conseguano 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 dall'Unione Europea.

In questo caso, contrariamente a quanto visto in merito al punto precedente (Art. 316-bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato si realizza nel momento dell'ottenimento dei finanziamenti.

Va evidenziato che tale reato, avendo natura residuale, si configura solo qualora la condotta non integri gli estremi del più grave delitto di truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis* c.p.).

A titolo esemplificativo, si citano, in particolare, le ipotesi di indebito ottenimento di un finanziamento pubblico finalizzato al sostegno delle attività imprenditoriali in determinati settori, mediante l'allegazione di false fatture attestanti prestazioni inesistenti; ovvero mediante la produzione di documentazione attestante la sussistenza dei requisiti per l'ottenimento del finanziamento.

A.1.6 Concussione (art. 317 c.p.)

Il reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio, abusando della sua qualità o del suo potere, costringa taluno a dare o promettere indebitamente, a sé o ad altri, denaro o altre utilità.

Trattandosi di un reato proprio di soggetti qualificati, la responsabilità della società potrà ravvisarsi nei casi in cui la stessa svolga attività di incaricato di pubblico servizio od anche qualora un dipendente, nell'interesse o a vantaggio della stessa, concorra nel reato del pubblico ufficiale o dell'incaricato di pubblico servizio, che, approfittando della sua posizione, esiga prestazioni non dovute.

A.1.7 Corruzione (artt. 318 – 319 – 319 bis – 319 *ter* - 320 – 321 c.p.)

Il reato si configura nel caso un pubblico ufficiale o un incaricato di pubblico servizio si faccia dare o promettere, per sé o per altri, denaro o altra utilità per esercitare le sue funzioni o i suoi poteri, omettere o ritardare atti del suo ufficio ovvero per compiere atti contrari ai suoi doveri di ufficio.

Il reato si configura altresì nel caso in cui l'indebita offerta o promessa sia formulata con riferimento ad atti – conformi o contrari ai doveri d'ufficio – già compiuti dal pubblico agente, allorché tali atti risultino comunque collegati all'accordo sinallagmatico corruttivo quale “prezzo” della condotta già posta in essere.

Il reato sussiste dunque sia nel caso in cui il pubblico ufficiale, dietro corrispettivo, compia un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia nel caso in cui compia un atto contrario ai suoi doveri (ad esempio: garantire l'illegittima aggiudicazione di un appalto), sia ancora nel caso in cui la dazione o promessa abbia ad oggetto la mera messa a disposizione, presente o futura, della funzione o dei poteri, senza riferimento ad uno specifico atto.

Nella forma della corruzione in atti giudiziari, il patto corruttivo è, inoltre, diretto a favorire o danneggiare una parte di un processo civile, penale o amministrativo, alterando il corretto svolgimento della giustizia e, nei casi più gravi, potendo determinare un'ingiusta condanna o un'ingiusta privazione della libertà personale, con conseguente aggravamento del trattamento sanzionatorio.

Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale.

A norma dell'art. 321 c.p., le pene previste per i pubblici ufficiali e gli incaricati di pubblico servizio si applicano anche ai privati che danno o promettono a quest'ultimi denaro o altra utilità.

A.1.8. Istigazione alla corruzione (art. 322 c.p.)

La pena prevista per tale reato si applica a chiunque offra o prometta denaro ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri o per omettere o ritardare un atto del suo ufficio oppure per compiere un atto contrario ai suoi doveri, qualora la promessa o l'offerta non vengano accettate. Parimenti, si sanziona la condotta del pubblico agente che solleciti una promessa o un'offerta da parte di un privato.

A.1.9. Induzione indebita a dare o promettere utilità (art. 319 *quater* c.p.)

Il reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induca taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altre utilità.

La norma sanziona non solo il pubblico ufficiale o incaricato di pubblico servizio, ma anche colui che dà o promette denaro o altre utilità.

Tale reato si differenzia da quello di concussione, in quanto il soggetto indotto non è più considerato come vittima, ma come coautore del reato che persegue un risultato illegittimo a lui favorevole.

A.1.10 Peculato, concussione, induzione a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzioni delle Comunità europee e di Stati esteri (art. 322 *bis* c.p.)

L'art. 322 *bis* c.p. estende l'applicabilità delle fattispecie corruttive (peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione) ai rapporti con pubblici ufficiali, incaricati di pubblico servizio o soggetti che esercitano funzioni equivalenti presso la Corte penale internazionale o gli organi delle Comunità europee e di Stati esteri.

A.1.11 Traffico di influenze illecite (art. 346 *bis* c.p.)

La norma punisce 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 altre 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. La stessa pena si applica a chi indebitamente dà o promette denaro o altre utilità. La pena è aumentata se il soggetto che indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità riveste la qualifica di pubblico ufficiale o di incaricato di un pubblico servizio.

A.1.12 Turbata libertà degli incanti (art. 353 c.p.)

Tale ipotesi di reato si configura quando nelle gare attivate dalla P.A. per arrivare alla scelta di un contraente - sia pubblici incanti (procedure aperte in cui ogni impresa interessata può presentare offerta) sia licitazioni private (destinate ad un numero ristretto di concorrenti) - con violenza o minaccia, doni o promesse, collusioni o altri mezzi fraudolenti si impedisce o turbi il regolare svolgimento della gara o si allontanano gli offerenti.

Si ricomprendono nella nozione di mezzi fraudolenti tutti i mezzi concretamente idonei a turbare la libertà degli incanti, alterando il regolare funzionamento e la libera partecipazione degli offerenti alla gara.

Le sanzioni sono innalzate se questi mezzi fraudolenti sono messi in atto da persona preposta dalla legge o dall'Autorità agli incanti.

Le sanzioni sono invece ridotte nel caso di licitazioni private per conto di privati, dirette da un pubblico ufficiale o da persona legalmente autorizzata.

A.1.13 Turbata libertà del procedimento di scelta del contraente (art. 353 *bis* c.p.)

Il reato si configura quando con violenza o minaccia, doni o promesse, collusioni o altri mezzi fraudolenti si interviene nel procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente con cui l'amministrazione deve stabilire le modalità per la scelta del contraente al fine di condizionare le modalità della stessa scelta.

Vengono incriminate le medesime condotte previste all'art. 353, con la differenza che la punibilità interviene già nella fase di predisposizione del bando.

Si tenta di porre rimedio a quelle situazioni in cui le scelte delle stazioni appaltanti vengono condizionate al momento dell'indizione della gara così da trarre un vantaggio a scapito di altre imprese.

A.1.14 Frode nelle pubbliche forniture (art. 356 c.p.)

Il reato punisce il fatto di chi commette frode nella esecuzione dei contratti di pubblica fornitura o nell'adempimento degli altri obblighi contrattuali che derivano da un contratto concluso con lo Stato o con un altro ente pubblico o con un'impresa esercente servizi pubblici o di pubblica necessità, anche in danno dell'Unione Europea.

Il reato è ravvisabile non solo nella fraudolenta esecuzione di un contratto di somministrazione (art. 1559 c.c.) ma anche di un contratto di appalto (art. 1655 c.c.) e, pertanto, ai fini della commissione del reato in esame rileva qualsiasi schema contrattuale con cui la pubblica amministrazione riceve cose od opere.

Per la configurabilità del reato, non rileva il mero inadempimento contrattuale ma occorre la malafede contrattuale e cioè la presenza di un espediente malizioso o di un inganno tale da far apparire l'esecuzione del contratto conforme agli obblighi assunti.

A titolo di esempio, integra il delitto di frode nelle pubbliche forniture la consegna di una cosa non conforme, per qualità, alle caratteristiche prestabilite nel capitolato di appalto.

A.1.15 Truffa in danno dello Stato o di enti pubblici o dell'Unione europea (art. 640, c. 2, n. 1 c.p.)

Il reato si configura qualora, utilizzando artifici o raggiri e in tal modo inducendo taluno in errore, si consegua un ingiusto profitto, in danno dello Stato, di altro ente pubblico o dell'Unione Europea.

Tale reato può realizzarsi quando, ad esempio, nella predisposizione di documenti o dati, per la partecipazione a procedure di gara, la società fornisce alla Pubblica Amministrazione informazioni non veritiere al fine di ottenere l'aggiudicazione. Si pensi, ancora, alla trasmissione all'amministrazione finanziaria di documentazione contenente false informazioni al fine di ottenere un rimborso fiscale non dovuto.

A.1.16 Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 *bis* c.p.)

Il reato si configura qualora la condotta di truffa sopra descritta abbia ad oggetto contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione Europea. La pena prevista per il reato in oggetto è la reclusione da due a sette anni.

Quanto all'oggetto materiale del reato, si precisa che i contributi e le sovvenzioni sono attribuzioni pecuniarie a fondo perduto, che possono avere carattere periodico o una tantum, in misura fissa o determinata in base a parametri variabili, natura vincolata all'*an* o al *quantum* o di pura discrezionalità; i finanziamenti sono atti negoziali caratterizzati dall'obbligo di destinazione delle somme o di restituzione o da ulteriori e diversi oneri; i mutui agevolati sono erogazioni di somme di denaro con obbligo di restituzione per il medesimo importo, ma con interessi in misura minore a quelli praticati sul mercato.

In ogni caso, le norme prendono in considerazione tutte le erogazioni di denaro caratterizzate da una vantaggiosità rispetto alle condizioni praticate dal mercato.

Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici, finalizzati, ad esempio alla ricerca o a sostenere l'occupazione, o ancora alla realizzazione di progetti di rilevanza pubblica.

A.1.17 Truffa informatica in danno dello Stato di altro ente pubblico (art. 640 *ter* c.p.)

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altro ente pubblico o dell'Unione Europea.

L'interferenza può realizzarsi in varie forme: in fase di raccolta ed inserimento dei dati, in fase di elaborazione, in fase di emissione. In tutti questi casi l'intervento avviene sulla memoria di un elaboratore sul cui corretto funzionamento l'autore materiale del reato interferisce in modo da ricavarne un indebito arricchimento in danno dello Stato o di altro ente pubblico.

Ad esempio, integra il reato la modificazione delle informazioni relative alla situazione contabile di un rapporto contrattuale in essere con un ente pubblico, ovvero l'alterazione dei dati fiscali e/o previdenziali contenuti in una banca dati facente capo alla Pubblica Amministrazione.

A.2 Attività sensibili

Il rischio di commissione di delitti contro la Pubblica Amministrazione è connaturato in ogni attività di impresa: qualsiasi società infatti si trova, nel corso della propria ordinaria attività, ad interfacciarsi in più di un'occasione con diversi enti pubblici e per le più disparate ragioni.

In particolare, Unirock S.r.l. intrattiene per la maggior parte rapporti commerciali con Enti Pubblici, sia nazionali che locali ed Enti pubblici economici : in ragione della sua attività può ritenersi a rischio di perpetrazione di reati contro la P.A.

Con riferimento ai reati contro la PA sopra evidenziati le principali attività sensibili ed il personale aziendale e consulenti maggiormente coinvolti che la Società ha rilevato al suo interno sono:

ATTIVITA' SENSIBILI	FASI	FUNZIONI INTERESSATE
Gestione partecipazione gare d'appalto ed affidamenti	Ricerca ed acquisizione informazioni gare d'appalto, bandi di gara per appalti di lavori, contratti	AU Resp. Uff. Gare
	Predisposizione, sottoscrizione, trasmissione offerte, tecniche ed amministrative	
	Predisposizione documentazione amministrativa richiesta	
	Aggiudicazione commessa	
Gestione ed esecuzione contratti con enti pubblici	Gestione operativa della commessa	AU Resp. Amm. Dirigenti del ex art. 16 Dlgs.81/08
	Controllo stato avanzamento lavori	
	Fornitura di beni o servizi	
	Rendicontazione	
Gestione rapporti con P.A.	Acquisizione informazioni per opportunità commerciali	AU Resp. Uff. Gare Dirigenti del ex art. 16 Dlgs.81/08
	Condivisione specifiche tecniche commerciali per presentazioni offerte	

	Esecuzione commessa, controllo operatività cantieri, SAL, fornitura servizi/rendicontazione	Delegati Ambiente e Sicurezza
	Interazioni con funzionari, dirigenti, RUP, membri commissione gare P.A.	
	Ispezioni e verifiche da parte della Pubblica Amministrazione	
	Richieste autorizzazioni/concessioni	
	Richiesta finanziamenti/agevolazioni	
	Sponsorizzazioni	
Gestione del personale	Ricerca e selezione del personale	AU Resp. amm. Consulente del lavoro incaricato
	Valutazione dei requisiti	
	Adempimenti in materia di assunzione/cessazione rapporto lavoro/retribuzioni/contributi previdenziali /ritenute fiscali	
Gestione attività amministrative, economiche e finanziarie	Gestione Ciclo attivo	AU Resp amm Dirigenti del ex art. 16 Dlgs.81/08 Commercialista incaricato
	Gestione Ciclo passivo	
	Gestioni conti correnti	
	Gestione Note spese	
	Scelta fornitori/consulenti	
	Predisposizione e redazione del Bilancio d'Esercizio	
Gestione degli affari legali	Predisposizione atti e contratti	AU Resp Amm Avv/ Consulente incaricato
	Gestione del contenzioso	
	Accordi transattivi	

A.3 Sistemi di controllo

A.3.1 Principi generali di comportamento

Vengono disciplinati nella presente parte speciale i principi e le regole di comportamento per i destinatari che operano nelle aree di attività a rischio.

In particolare, nell'ambito di tali attività è fatto divieto di:

- Offrire denaro, doni o altre utilità a dirigenti, funzionari o dipendenti sia della P.A. sia appartenenti ad interlocutori commerciali privati o a loro parenti sia italiani che di altri paesi, salvo che si tratti di doni o utilità di modica entità;
- Chiedere o accettare a qualsiasi titolo, compensi, regali, o altre utilità in connessione con l'espletamento delle proprie funzioni o dei compiti affidati, fatti salvi i regali d'uso purché di modico valore e nei limiti delle normali relazioni di cortesia;
- Cercare di influenzare le decisioni della controparte comprese quelle dei funzionari che trattano o prendono decisioni per conto della P.A., quando è in corso una qualsiasi trattativa di affari, richiesta o rapporto con la P.A.;
- Tenere una condotta ingannevole che possa indurre la PA in errore;
- Violare la legge e le corrette pratiche commerciali nel caso di effettuazione di una gara o di una diversa procedura ad evidenza pubblica;
- Nel corso di una trattativa di affari, richiesta o rapporto commerciale con la P.A. intraprendere direttamente o indirettamente le seguenti azioni:
 - Esaminare e/o proporre opportunità di impiego che possano avvantaggiare dipendenti della P.A. a titolo personale;
 - Sollecitare o ottenere informazioni riservate che possono compromettere l'integrità o la reputazione di entrambi;
- effettuare spese di rappresentanza arbitrarie che prescindono dagli obiettivi dell'Ente;
- esibire documenti, o divulgare informazioni riservate;
- esibire documenti che contengano informazioni mendaci o false;
- ammettere, per collaboratori esterni, compensi che non siano correlati al tipo di incarico da loro svolto su base contrattuale;
- danneggiare il funzionamento di reti informatiche, o di dati contenuti all'interno al fine di ottenere un ingiusto vantaggio.

Nel caso in cui Unirock utilizzi un consulente esterno o un soggetto terzo nei rapporti con la P.A. prevedere che nei confronti del consulente e del suo personale o del soggetto terzo siano applicate le stesse direttive valide anche per i suoi dipendenti;

Gestione della contabilità generale:

- gestione delle attività economiche e finanziarie attraverso Software gestionale “Sistemi” in modo da garantire la tracciabilità delle operazioni e fornire una rendicontazione a posteriori;
- accesso al sistema gestionale unicamente al personale autorizzato, Responsabile ed Addetta Amministrazione;
- specifica formazione ed informazione del personale addetto sui principi di trasparenza, integrità e chiarezza della documentazione contabile, nonché sulla necessità di segnalazione in presenza di anomalie;
- formazione e controllo di sussistenza adeguata documentazione a supporto di ogni operazione contabile/economica;
- Registrazione e controlli dei pagamenti e degli incassi con indicazione di data, importo, controparte, causale, riferimento documento, mezzo di pagamento
- tutti i rapporti con gli istituti di credito, inclusa l'esecuzione di pagamenti, l'apertura e chiusura dei conti correnti sono gestiti unicamente da soggetti con i poteri relativi : AU e Responsabile Amministrativa;
- Riconciliazioni periodiche tra estratti conto bancari, report POS, movimenti finanziari attivi e passivi, documenti contabili
- Adeguata conservazione ed archiviazione della documentazione contabile ed amministrativa a cura di Responsabile Amministrazione;
- Verifiche periodiche delle operazioni contabili ed amministrative da parte di soggetti terzi, quali Dottore commercialista , Consulente del lavoro incaricati e Revisori dei Conti
- Obbligo di segnalazione delle anomalie rilevate all'OdV nominato.

A.3.2 Regole specifiche di comportamento

Gestione delle attività amministrative, economiche e finanziarie:

La fatturazione attiva viene eseguita nel rispetto dei ruoli e delle responsabilità definiti dall'organizzazione interna e strettamente connessa alla formalizzazione di idonea documentazione giustificativa che ne attesti l'esistenza dei presupposti.

A tal fine Unirock ha predisposto un'apposita procedura che descrive l'oggetto, i soggetti coinvolti e le operazioni da effettuare nell'ambito del ciclo attivo.

In particolare:

- l'apertura della Cartella Commessa, dal momento dell'aggiudicazione della gara/ sottoscrizione contratto consente che tutta la documentazione amministrativa/contabile e di fatturazione ad essa relativa sia inserita digitalmente in modo da garantire la tracciabilità;
- le fatture elettroniche vengono emesse da Resp. Amm., previo controllo AU, solo al ricevimento del certificato di pagamento inoltrato via pec da Ente Appaltante, a seguito di verifica dello Stato Avanzamento Lavori;

- Resp. Amm. monitora e controlla l'avvenuta ricezione e corrispondenza dei pagamenti/incassi clienti sui conti correnti della Società;
- In caso di mancato incasso delle fatture attive, sono svolti controlli specifici e documentati sul mancato incasso e sono attivate adeguate procedure per recuperare il credito nei confronti del cliente, nel rispetto delle disposizioni normative di settore vigenti;
- Resp. Amm. provvede ad archiviazione delle fatture attive ed alla trasmissione al commercialista di prospetti periodici annui dei ricavi al fine della redazione del bilancio.

Per quanto attiene il ciclo passivo, il processo si svolge nel rispetto dei seguenti punti:

- analisi del fabbisogno di fornitura per ogni singola commessa da parte di delegati ex art. 16 D.Lgs. 81/08/, IT di cantiere con l'inserimento nella relativa Cartella nel software gestionale della parte relativa agli acquisti/forniture;
- redazione, emissione ed inoltro ordini di acquisto da IT di cantiere/Delegati ex art. 16 D.Lgs.81/08 ed approvazione da parte di AU;
- previsione della formalizzazione del contratto o incarico professionale con il fornitore di beni o prestatore di servizi;
- verifica di Resp. Amm dell'accettazione formale dell'ordine di acquisto/contratto da parte del fornitore, prima dell'esecuzione della prestazione o della consegna della fornitura;
- controlli di conformità delle forniture e dell'avvenuta esecuzione della prestazione di servizi da Dir Tecnici di cantiere
- monitoraggio di ricevimento fattura, stampa e registrazione a cura dell'Addetta Amm. sul gestionale "Sistemi";
- effettuazione controlli sulla corrispondenza tra fattura e documentazione a supporto a cura di Resp. Amm. In caso di disallineamento, svolgimento di opportune verifiche;
- documentazione di supporto di ogni operazione archiviata a cura di Resp. Amm.

Gestione pagamenti:

- predisposizione scadenziario attivo/passivo clienti e fornitori generato da programma software "Sistemi" e sottoposto ad AU;
- pagamenti disposti esclusivamente su conto corrente indicato dal terzo contraente al momento dell'accettazione ordine o successivamente solo tramite comunicazione scritta dello stesso;
- tutti i pagamenti sono disposti secondo la normativa vigente tramite bonifico bancario o modalità che ne prevede la tracciabilità ;
- rispetto della legislazione vigente in materia di limitazione all'utilizzo del contante;
- effettiva esecuzione pagamenti solo con autorizzazione e verifica della destinazione di pagamento solo per le finalità per le quali è intervenuta autorizzazione;
- verifica della corrispondenza tra beneficiario del pagamento e fornitore;
- utilizzo di sistemi informatici e di strumenti automatizzati per esecuzione pagamenti solo da parte delle figure autorizzate: AU e Resp. Amm.

- accesso al gestionale sistemi per verifiche e controlli da parte di consulente terzo incaricato, Dott. Commercialista al fine di predisporre scritture contabili e di bilancio;

Gestione note spese:

- limitazione/assenza di gestione contante nell'ambito dei cantieri allestiti: previsione acquisti solo di piccola entità da parte dei capisquadra con trasmissione fatture direttamente a Resp. Amm.;
- previsione di carta di credito per le spese correnti del cantiere solo in capo ai soggetti delegati ex art. 16 D. lgs. 81/08;
- limitazione del ricorso ad acquisti urgenti per le sole situazioni di reale gravità o non prevedibilità, mantenendo traccia scritta delle motivazioni;
- controllo e verifica dei documenti giustificativi (fatture/note spese/scontrini) dei pagamenti effettuati con carte di credito a cura di Resp. Amm.

Scelta fornitori:

- selezione dei fornitori di comprovata idoneità tecnica, qualità ed in possesso dei requisiti previsti dalla normativa vigente (Codice Appalti);
- verifica controllo requisiti del fornitore, delle certificazioni delle forniture del materiale e dichiarazioni di conformità da parte di IT di cantiere;
- inserimento negli ordini e contratti della specifica "clausola 231".

Gestione del personale:

La gestione del personale è improntata ai principi di legalità, trasparenza, correttezza e tracciabilità.

La Società riconosce la centralità delle risorse umane e l'importanza di stabilire e mantenere con esse relazioni basate sulla lealtà e sulla fiducia reciproca. Pertanto, la gestione dei rapporti di lavoro e di collaborazione si ispira al rispetto dei diritti dei lavoratori ed alla piena valorizzazione del loro apporto nell'ottica di favorirne lo sviluppo e la crescita professionale.

Nella selezione del personale la Società evita ogni discriminazione di trattamento a qualsiasi titolo, applicando in qualsiasi circostanza le prescrizioni del Codice Etico.

Le assunzioni, gli avanzamenti del personale sono autorizzati da AU previa verifica dei requisiti di competenza, idoneità ed onorabilità, secondo i principi e le regole stabiliti dalla normativa vigente.

Gli adempimenti in materia di assunzioni, cessazione del rapporto di lavoro, retribuzioni, ritenute fiscali e contributi previdenziali ed assistenziali sono predisposti da Consulente del Lavoro debitamente incaricati per la gestione; i consulenti sono tenuti al rigoroso rispetto dei presupposti e delle condizioni previste dalla legislazione vigente.

Ogni anomalia deve essere tempestivamente segnalata all'Organismo di Vigilanza.

Gestione degli affari legali / transazioni e gestione del contenzioso:

In relazione alla gestione del contenzioso, la Società assicura la tracciabilità del processo che ha dato origine al contenzioso e l'evoluzione del medesimo, mediante la conservazione della documentazione comprovante lo stato del contenzioso.

Assicura altresì che le rilevazioni contabili generate dal verificarsi di contenziosi si riferiscano a situazioni per le quali è presente per la società un rapporto diretto con la controparte e attinente alla sfera aziendale (es. ciclo passivo, ciclo attivo, gestione del personale, ecc....).

Con riferimento al contenzioso è previsto inoltre che venga assicurata la congruità dell'importo di eventuali transazioni anche attraverso specifico parere legale esterno.

Si richiama la procedura "Gestione Amministrativa" adottata dalla Società.

La violazione di tutti i principi di controllo, delle specifiche norme di comportamento indicate nonché delle procedure e/o istruzioni operative è da considerare violazione del Modello, per cui deve essere segnalata all'Odv affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

PARTE SPECIALE “B” REATI SOCIETARI (art. 25 *ter* D.lgs. 231/2001)

B.1 Descrizione delle fattispecie normative

Si riporta di seguito una breve descrizione dei reati, tra quelli contemplati negli artt. 25-*ter* del Decreto e degli illeciti amministrativi di abuso di mercato di cui al testo unico della finanza, considerati potenzialmente a rischio per la Società.

B.1.1 False comunicazioni sociali (art. 2621 – art. 2621 *bis* c.c.)

La falsità nelle comunicazioni sociali si realizza con la consapevole esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali rilevanti non rispondenti al vero, ovvero omissione di fatti materiali rilevanti la cui comunicazione è imposta dalla legge, sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo concretamente idoneo ad indurre altri in errore.

Si precisa che:

- nella nozione di “comunicazione sociale” rientrano tutte le comunicazioni previste dalla legge dirette ai soci o al pubblico, ivi compresi il progetto di bilancio, le relazioni, i documenti da pubblicare ai sensi degli artt. 2501-*ter* e 2504-*novies* c.c. in caso di fusione o scissione, ovvero in caso di acconti sui dividendi, a norma dell’art. 2433-*bis* c.c.;
- le informazioni false o omesse devono essere rilevanti;
- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto, realizzata consapevolmente e concretamente idonea a trarre in inganno;
- un bilancio falso, rilevante in sede penale, non significa necessariamente bilancio invalido in senso civilistico;
- si tratta di reato di pericolo e quindi perseguibile indipendentemente dal verificarsi di un danno; inoltre, la perseguibilità è d’ufficio;
- la Legge 69/2015 ha eliminato le soglie quantitative, precedentemente previste, di non punibilità rispetto a discostamenti contabili non tali da alterare significativamente la rappresentazione societaria;
- la Legge di cui al punto precedente ha comunque introdotto l’articolo 2621-*bis* relativo a fatti di lieve entità (ripreso dal D.lgs. 231/01 con l’introduzione, nell’art. 25-*ter* comma 1, della lettera a-*bis*), secondo cui le pene previste sono ridotte “se i fatti di cui all’art. 2621 sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta” nonché se “i fatti di cui all’articolo 2621 riguardano società che non superano i limiti indicati dal secondo comma dell’articolo 1 del regio decreto 16 marzo 1942, n. 267”. Nel secondo caso “il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale”;
- la responsabilità si estende anche all’ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Soggetti attivi del reato sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci ed i liquidatori (reato proprio).

B.1.2. Impedito controllo (art. 2625, comma 2, c.c.)

Il reato consiste nell'ostacolare o impedire lo svolgimento delle attività di controllo - legalmente attribuite ai soci o ad organi sociali - attraverso l'occultamento di documenti od altri idonei artifici.

Il reato, imputabile esclusivamente agli amministratori, può comportare la responsabilità dell'Ente soltanto nell'ipotesi in cui la condotta abbia causato un danno.

La fattispecie si configura non solo quando, attraverso l'occultamento di documenti o attraverso altri idonei artifici, siano impedito le predette attività, ma anche quando siano solamente ostacolate.

Si tratta, più precisamente, delle attività che influiscono:

- sulle iniziative di controllo dei soci previste dal codice civile e dagli altri atti normativi, quali ad esempio l'art. 2422 c.c. che prevede il diritto dei soci di ispezionare i libri sociali;
- sulle attività di controllo del collegio sindacale, previste dal codice civile e dalle altre norme, quali ad esempio gli artt. 2403 e 2403-bis che prevedono il potere dei membri del Collegio sindacale di procedere ad atti di ispezione e di controllo e di richiedere agli amministratori notizie sull'andamento delle operazioni sociali o di determinati affari.

B.1.3 Indebita restituzione dei conferimenti (art. 2626 c.c.)

La "condotta tipica" prevede, fuori dei casi di legittima riduzione del capitale sociale, la restituzione, anche simulata, dei conferimenti da parte degli amministratori ai soci o la liberazione degli stessi dall'obbligo di eseguirli

B.1.4 Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)

Anche tale condotta criminosa viene imputata esclusivamente agli amministratori e consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva; ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.

B.1.5 Illecite operazioni sulle quote sociali o della società controllante (art. 2628 c.c.)

La norma sanziona la condotta degli amministratori che, fuori dai casi consentiti dalla legge, acquistano o sottoscrivono quote della società, cagionando una lesione all'integrità delle riserve non distribuibili per legge.

B.1.6 Operazioni in pregiudizio ai creditori (art. 2629 c.c.)

La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altre società o scissioni, che cagionino danno ai creditori.

Si tratta quindi di un reato che può essere commesso con qualsiasi condotta che abbia come effetto quello di cagionare il danno ai creditori.

Con riferimento alle operazioni di riduzione del capitale sociale, si possono citare i seguenti esempi di condotte penalmente rilevanti: esecuzione della delibera di riduzione del capitale sociale nonostante l'opposizione dei creditori sociali o in mancanza della delibera da parte del Tribunale.

Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

B.1.7 Formazione fittizia del capitale sociale (art. 2632 c.c.)

Tale ipotesi si realizza quando viene formato o aumentato fittiziamente il capitale della società mediante attribuzione di quote sociali per somma inferiore al loro valore nominale; vengono sottoscritte reciprocamente quote; vengono sopravvalutati in modo rilevante i conferimenti dei beni in natura, i crediti ovvero il patrimonio della società nel caso di trasformazione.

B.1.8 Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)

Il reato previsto dall'art. 2633 c.c. sanziona la condotta dei liquidatori che cagionano danno ai creditori, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o prima dell'accantonamento delle somme necessarie a soddisfarli.

B.1.9 Corruzione tra privati e istigazione alla corruzione tra privati (art. 2635, comma 3, - art. 2635 *bis*, comma 1, c.c.)

Le norme sanzionano la condotta di chi, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuta agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, affinché compiano od omettano un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.

L' accettazione o meno dell'offerta o della promessa rappresenta il punto di differenziazione fra la fattispecie di istigazione alla corruzione e la fattispecie di corruzione vera e propria.

La norma non fa differenza fra corruzione attiva (promettere o dare) e corruzione passiva (sollecitare o accettare la promessa o ricevere). La fattispecie di corruzione passiva non è rilevante ai sensi delle sanzioni del Decreto, perché teoricamente non commessa nell'interesse della Società, ma la Società ha ritenuto di contemplare anche questa ipotesi, per creare un Sistema volto a presidiare tutti i fenomeni corruttivi, e di configurarla come una

violazione del Modello, anche in considerazione del fatto che trattasi di comportamento vietato dal Codice Etico, che può incidere gravemente sulla moralità generale dell'Azienda e foriera di pericoli di diffusione dei fenomeni corruttivi.

B.1.10 Illecita influenza dell'assemblea (art. 2636 c.c.)

Il reato si realizza quando con atti simulati o con frode si determina la maggioranza in assemblea, allo scopo conseguire, per sé o per altri, un ingiusto profitto; si tratta di un "reato comune", che può quindi essere commesso da chiunque.

La norma mira ad evitare che, attraverso condotte fraudolente si influisca illegittimamente sulla formazione della maggioranza assembleare.

Ai fini della norma in esame vengono in considerazione le condotte volte alla convocazione dell'assemblea, all'ammissione alla partecipazione all'assemblea e al computo dei voti per la deliberazione, nonché le relative attività di supporto.

B.1.11 Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2, c.c.)

La norma sanziona la condotta dolosa degli amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori di società o enti e altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazione alla predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero o occultano fraudolentemente informazioni sulla situazione economico-patrimoniale-finanziari (comma 1), ovvero in qualsiasi forma, anche omettendo comunicazioni obbligatorie, ne ostacolano consapevolmente le funzioni (comma 2).

Entrambe le fattispecie tutelano il regolare esercizio delle funzioni di vigilanza pubblica. Il primo comma è un reato di mera condotta, integrato sia dall'omessa comunicazione di informazioni dovute sia dal ricorso a mezzi fraudolenti volti ad occultare l'esistenza di fatti rilevanti per a situazione economica, patrimoniale o finanziaria della società, mentre il secondo comma richiede la causazione di un effettivo ostacolo alla funzione di vigilanza, quale conseguenza di una condotta che può assumere qualsiasi forma, ivi compresa l'omessa comunicazione di informazioni dovute.

B.1.12 False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D.lgs. 19/2023)

Il reato in oggetto è stato introdotto dal Decreto legislativo n. 19 del 02/03/2023, in attuazione della direttiva (UE) 2019/2121 del Parlamento europeo e del Consiglio, del 27/11/2019, che modifica la direttiva (UE) 2017/1332 per quanto riguarda le trasformazioni, le fusioni e le scissioni transfrontaliere.

La norma sanziona la condotta di chiunque, al fine di far apparire adempite le condizioni per il rilascio del certificato di cui all'art. 29 del medesimo decreto (attestante il regolare adempimento degli atti e delle formalità preliminari alle operazioni transfrontaliere di fusione, scissione o trasformazione societaria), formi documenti in tutto o in parte falsi, alteri documenti veri, renda dichiarazioni false oppure ometta informazioni rilevanti.

B.2 Attività sensibili

Con riferimento ai reati societari le principali attività sensibili e le funzioni aziendali maggiormente coinvolte che Unirock S.r.l. ha rilevato al suo interno sono:

ATTIVITA' SENSIBILI	FASI	FUNZIONI INTERESSATE
Redazione del bilancio	Redazione del progetto di bilancio	AU Assemblea Soci Dottore Commercialista Società di revisione
	Redazione della relazione sulla gestione	
	Consegna del progetto di bilancio e della relazione ai Revisori	
	Deposito del bilancio e dei suoi allegati e della relazione dell'AU	
	Approvazione del bilancio	
	Deposito del bilancio con gli allegati e del verbale di approvazione presso il registro delle imprese	
Rilevazione in contabilità dei fatti di gestione attività amministrative, economiche e finanziarie avvenuti nel corso dell'esercizio	Gestione Ciclo attivo	AU Resp. Amm. Resp. Ufficio Gare IT Cantiere Delegati ex art. 16 D.Lgs. 81/08 Dottore Commercialista Consulente del lavoro
	Gestione Ciclo passivo	
	Gestione Note spese	
Gestione dei rapporti con Socio e con i Revisori legali	Convocazione dell'Assemblea dei soci con le modalità ed entro i termini previsti dalla legge e dallo statuto	AU Dottore Commercialista Revisori legali

	Nomina di un segretario che cura la verbalizzazione	
	Archiviazione e conservazione presso la sede legale della società di tutta la documentazione rilevante	
	Trascrizione degli atti nei libri sociali e conservazione degli stessi	
	Comunicazione dell' AU di ogni interesse che il medesimo per conto proprio o terzi abbiano in una determinata operazione della società	
	Consegna del progetto di bilancio e della relazione al Revisore	
Operazioni relative al capitale sociale	In caso di operazione straordinarie approfondita valutazione contabile e fiscale con ausilio di esperti legali/tributari esterni	AU Consulenti esterni Assemblea dei soci Revisori legali
	Verifica della fattibilità finanziaria dell'operazione straordinaria	
	Controllo e approvazione della documentazione contrattuale relativa ad operazioni straordinarie da parte di AU	
	Fornire ai fini dell'approvazione dell'operazione straordinaria documentazione chiara, veritiera ed esaustiva	
	Adeguate conservazione e registrazione contabile	

B.3 Sistema di controllo

B.3.1 Principi generali di comportamento

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole individuate dal presente Modello i destinatari, per quanto di rispettiva competenza, sono tenuti a conoscere e a rispettare puntualmente oltre alle norme di legge e di regolamento di volta in volta applicabili, tutta la documentazione interna aziendale relativa al sistema amministrativo, finanziario e contabile.

È pur vero che il più delle volte tali reati vengono posti in essere da chi è formalmente responsabile di tali documenti (ai sensi dell'art. 2423 c.c.). Come già accennato, buona parte dei reati societari idonei a far scattare la responsabilità amministrativa dell'ente sono reati "propri", cioè puniti solo se commessi da soggetti che ricoprono la figura appunto di amministratore, direttore generale, liquidatore.

Tuttavia, può verificarsi l'ipotesi in cui tali fattispecie siano poste in essere, dolosamente, da personale non apicale, ad esempio da responsabili delle funzioni aziendali sia amministrative contabili che di cantiere come da consulenti esterni.

In tali casi, il reato sussiste solo se la falsità sia consapevolmente condivisa dai soggetti qualificati che, nel recepire il dato falso, lo fanno proprio, inserendolo nella comunicazione sociale. In mancanza di tale partecipazione cosciente e volontaria da parte dei soggetti qualificati il reato non si realizza.

Al fine di prevenire la commissione di tali reati è necessario che l'intero procedimento che porta alla formazione dei documenti deve essere improntato alla massima trasparenza e tracciabilità.

In tal senso, è fatto espresso obbligo a carico degli Organi Sociali di Unirock s.r.l., dei dipendenti, dei consulenti, dei partner di:

- tenere un comportamento improntato alla massima correttezza, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione dei bilanci e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria dell'Ente;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- assicurare il regolare funzionamento della Società e degli Organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge nonché la libera e corretta formazione della volontà assembleare;
- aver cura di effettuare, nella piena veridicità, con tempestività e correttezza, tutte le comunicazioni previste dalla disciplina applicabile nei confronti delle Autorità competenti, evitando di frapporre qualsivoglia ostacolo all'esercizio delle loro attività di controllo e verifica;
- Prevedere attività di formazione di base nei confronti di tutti i dipendenti coinvolti nell'attività di formazione del bilancio o di altri documenti similari, affinché conoscano almeno le principali nozioni sul bilancio;
- porre la massima attenzione e cautela, attraverso il rispetto delle norme di legge e delle procedure aziendali a essa indirizzate, alla tutela dell'integrità ed effettività del capitale e del patrimonio sociale, nel rispetto totale delle garanzie dei creditori e dei terzi in genere.

Nell'ambito dei suddetti comportamenti è fatto divieto in particolare di:

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci relazioni e prospetti o altre comunicazioni sociali, dati falsi e lacunosi o comunque non rispondenti alla realtà sulla situazione economica patrimoniale e finanziaria dell'Ente;
- omettere dati ed informazioni imposte dalla legge sulla situazione economica, patrimoniale e finanziaria dell'Ente;
- effettuare operazioni sull'utile non previste dalle leggi in vigore;
- determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere degli atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie dell'Ente;
- porre in essere qualsiasi comportamento che sia di **ostacolo** all'esercizio delle funzioni di **vigilanza** anche in sede di ispezione da parte delle autorità pubbliche di vigilanza;

B.3.2 Regole specifiche di comportamento

Gli adempimenti societari da parte di Unirock si svolgono nel rispetto dei principi sottoindicati e specifici presidi di controllo:

Formazione del bilancio:

Il bilancio deve essere completo sotto il profilo dell'informazione societaria e deve contenere tutti gli elementi richiesti dalla legge;

Tutte le operazioni sul capitale sociale che possano potenzialmente ledere l'integrità del capitale sociale devono essere assunte e deliberate dalle figure espressamente previste per compiti ruoli e responsabilità dalla normativa vigente e dall'organigramma aziendale

In particolare:

- Individuazione dei soggetti che nell'esercizio dell'attività di propria competenza a favore dell'ente intervengono nella gestione delle adeguate procedure amministrative, contabili e finanziarie per la formazione del bilancio. Tra le figure coinvolte la Società ha ricompreso, oltre agli organi amministrativi e i dipendenti facenti parte dell'Ufficio Amministrativo e Ufficio Gare ed i Direttori tecnici di Cantiere anche i consulenti esterni di cui si avvale quali il Dottore Commercialista, l'Assistente legale e il Consulente del Lavoro;
- invio dei dati utili alla redazione del bilancio da parte dei dipendenti interessati a Resp. Amm, per adeguata registrazione ed archiviazione nel Sistema Gestionale, in modo da consentire la tracciabilità del documento e l'identificazione del soggetto che lo trasmette;
- aggregazione dati contabili e trasmissione al Dottore Commercialista a cura di Resp. Amm., dopo verifica e controllo da parte di AU;
- Accesso ai sistemi di contabilità esclusivamente al personale autorizzato (AU , Resp. ed Add. Amm, Consulente Dottore Commercialista) mediante l'utilizzo di *user id e password*;

- Formazione del fascicolo di bilancio da parte del consulente esterno, Dottore Commercialista
- Approvazione del progetto di bilancio e della relazione sulla gestione da parte di AU
- Trasmissione del bilancio ai revisori legali nei termini previsti dalla normativa, per espressione del giudizio di competenza
- Approvazione del bilancio, da parte dell'Assemblea dei Soci
- Pubblicazione del bilancio e invio ai competenti registri a cura del Dottore Commercialista;
- Corretta archiviazione dei verbali delle riunioni degli organi sociali in Società

Operazioni Straordinarie:

La predisposizione delle situazioni patrimoniali in occasione di operazioni societarie straordinarie è svolta secondo i seguenti principi di controllo:

la gestione di operazioni straordinarie prevede il coinvolgimento dell'Amministratore Unico, del consulente esterno, Dottore Commercialista ed il controllo dei Revisori Legali

AU deve eseguire la verifica della fattibilità finanziaria dell'operazione straordinaria, con ausilio del consulente esterno, Dottore Commercialista, e della documentazione sulla situazione patrimoniale, economica e finanziaria

La documentazione fornita al Consulente Dottore Commercialista, ai Revisori Legali ed all'Assemblea dei Soci per l'approvazione deve essere adeguatamente conservata ed il suo contenuto deve essere chiaro, veritiero ed esaustivo

Le registrazioni contabili relative ad operazioni a carattere straordinario possono essere effettuate solo successivamente alla delibera favorevole da parte dell'Assemblea dei Soci ed in coerenza con i termini di efficacia dell'operazione stessa

Tutta la documentazione prodotta, inviata e ricevuta in merito ad operazioni straordinarie/modifiche societarie è archiviata presso la sede della Società;

Nello svolgimento delle attività in oggetto è inoltre fatto divieto di:

porre in essere attività e/o operazioni volte a creare disponibilità extracontabili (per esempio ricorrendo a fatture per operazioni inesistenti o alla sovrapproduzione) ovvero volte a creare fondi neri o contabilità parallele;

impedire od ostacolare le attività di controllo ai soci, ai consulenti esterni ai Revisori Legali, assicurando la trasparenza, chiarezza e tracciabilità di tutta la documentazione relativa alle attività in oggetto.

Si richiama la procedura Gestione Amministrativa adottata dalla Società.

La violazione di tutti i principi di controllo, delle specifiche norme di comportamento indicate nonché delle procedure e/o istruzioni operative è da considerare violazione del Modello, per cui deve essere segnalata all'Odv affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

PARTE SPECIALE “C” REATI TRIBUTARI (art. 25 *quinquiesdecies* d.lgs. 231/2001)

C.1 Descrizione delle fattispecie normative

I reati tributari sono stati introdotti dalla Legge 19 dicembre 2019 n. 157 “Conversione in legge, con modificazioni, del decreto-legge 26 ottobre 2019, n. 124, recante disposizioni urgenti in materia fiscale e per esigenze indifferibili”.

In particolare, il D. L. 124/2019, con l’art. 39, è intervenuto in materia penale-tributaria modificando molte delle fattispecie penali previste dal d.lgs. 74 del 2000 ed inserendo, nel novero dei reati presupposto della responsabilità degli enti, anche alcuni reati fiscali, aggiungendo al d.lgs. 231/2001 l’art. 25-*quinquiesdecies*.

Quest’ultimo è stato successivamente modificato dal d.lgs. 75/2020 che è andato ad estendere i reati tributari applicabili ai sensi del d.lgs. 231/01. Si precisa che i reati di cui alla cd. Direttiva PIF (i.e. reati di cui agli artt. 4, 5 e 10-quater del d. lgs. n. 74/2000) rientrano nell’ambito del d.lgs. n. 231/2001 solo se: i) commessi nell’ambito di sistemi fraudolenti transfrontalieri; ii) aventi il fine di evadere l’IVA; iii) per un importo complessivo (di IVA) non inferiore a 10 milioni di Euro;

C.1.1 Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 1 e 2 *bis* d.lgs. 74/2000)

L’art. 2 punisce chi al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi e così recita:

“1. È punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.”

2. Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell’amministrazione finanziaria.

2-bis. Se l’ammontare degli elementi passivi fittizi è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.”

C.1.2 Dichiarazione fraudolenta mediante altri artifici (art. 3 d.lgs. 74/2000)

Detto articolo punisce chi al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti tende ad ostacolare l’accertamento e ad indurre in errore l’amministrazione finanziaria.

“1. Fuori dai casi previsti dall’articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l’accertamento e ad indurre in errore l’amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente:

- a) *l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;*
- b) *l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.*
2. *Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.*
3. *Ai fini dell'applicazione della disposizione del comma 1, non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.”*

C.1.3 Dichiarazione infedele (art. 4 d.lgs. 74/2000)

L'art. 4 punisce chi al fine di evadere le imposte sui redditi o sul valore aggiunto, indica nella dichiarazione annuale elementi attivi o passivi diversi o inesistenti. Si riporta di seguito il testo.

“1. Fuori dei casi previsti dagli articoli 2 e 3, è punito con la reclusione da due anni a quattro anni e sei mesi chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:

- a) *l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a € 100.000,00;*
- b) *l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a € 2.000.000,00.*

1-bis. Ai fini dell'applicazione della disposizione del comma 1, non si tiene conto della non corretta classificazione, della valutazione di elementi attivi o passivi oggettivamente esistenti, rispetto ai quali i criteri concretamente applicati sono stati comunque indicati nel bilancio ovvero in altra documentazione rilevante ai fini fiscali, della violazione dei criteri di determinazione dell'esercizio di competenza, della non inerenza, della non deducibilità di elementi passivi reali.

1-ter. Fuori dei casi di cui al comma 1-bis, non danno luogo a fatti punibili le valutazioni che complessivamente considerate, differiscono in misura inferiore al 10 per cento da quelle corrette. Degli importi compresi in tale percentuale non si tiene conto nella verifica del superamento delle soglie di punibilità previste dal comma 1, lettere a) e b).”

C.1.4 Omessa dichiarazione (art. 5 d.lgs. 74/2000)

L'art. 5 punisce il soggetto obbligato o il sostituto di imposta che, al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta una delle dichiarazioni relative a dette imposte e così recita:

“1. È punito con la reclusione da due a cinque anni chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad € 50.000,00.

1-bis. È punito con la reclusione da due a cinque anni chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad € 50.000,00

2. Ai fini della disposizione prevista dai commi 1 e 1-bis non si considera omessa la dichiarazione presentata entro novanta giorni dalla scadenza del termine o non sottoscritta o non redatta su uno stampato conforme al modello prescritto.”

C.1.5 Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, comma 1 e 2 bis d.lgs. 74/2000)

L'art. 8 punisce chi emette fatture inesistenti per consentire evasione a terzi di imposte sui redditi o sul valore aggiunto. Si riporta il testo dell'articolo:

“1. È punito con la reclusione da quattro a otto anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

2. Ai fini dell'applicazione della disposizione prevista dal comma 1, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

2-bis. Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.”

C.1.6 Occultamento o distruzione di documenti contabili (art. 10 d.lgs. 74/2000)

L'art.10 punisce chi distrugge o occulta documentazione per evadere o far evadere imposte sui redditi o sul valore aggiunto e così dispone:

“1. Salvo che il fatto costituisca più grave reato, è punito con la reclusione da tre a sette anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.”

C.1.7 Indebita compensazione (art. 10 quater d.lgs. 74/2000)

L'art. 10 quater punisce chi vantando crediti non spettanti, li utilizza in compensazione su somme dovute:

“1. È punito con la reclusione da sei mesi a due anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, per un importo annuo superiore a € 50.000,00.

2. È punito con la reclusione da un anno e sei mesi a sei anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai € 50.000,00.”

C.1.8 Sottrazione fraudolenta al pagamento di imposte (art. 11 d.lgs. 74/2000)

L'art. 11 punisce chi, per non pagare imposte sui redditi o sul valore aggiunto o altro, si adopera per rendere inefficace la procedura di riscossione.

“1. È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

2. È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per se' o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.”

C.2 Attività sensibili

ATTIVITA' SENSIBILI	FASI	FUNZIONI INTERESSATE
Gestione attività amministrative, economiche e finanziarie per gli aspetti aventi valenza fiscale	Gestione Ciclo attivo	AU Resp. Amm. Resp. Ufficio Gare Delegati ex art. 16 D.Lgs. 81/08 IT Cantiere Dottore Commercialista Consulente del lavoro
	Gestione Ciclo passivo	
	Gestione conti correnti	
	Gestione Note spese	
	Scelta fornitori/consulenti	
	Predisposizione e redazione del Bilancio d'Esercizio	
Gestione adempimenti dichiarativi periodici, fiscali, tributari e calcolo imposte	Registrazioni informazioni contabili	AU Resp Amm Dottore Commercialista Revisori Legali
	Rilevazione, aggregazione e trasmissione dati fiscalmente rilevanti	
	Controlli revisori legali	
	Determinazione risultato fiscale e predisposizione dichiarazioni	
	Versamento imposte, trasmissione documentazione Amm. Finanziaria e conservazione documentale	
	Rapporti Amministrazione finanziaria	
Redazione del bilancio	Redazione del progetto di bilancio	AU Assemblea soci Dottore Commercialista Revisori Legali
	Redazione della relazione sulla gestione di AU	

	Consegna del progetto di bilancio e della relazione ai Revisori	
	Deposito del bilancio e dei suoi allegati e delle relazioni di AU	
	Approvazione del bilancio	
	Deposito del bilancio con gli allegati e del verbale di approvazione presso il registro delle imprese	
Operazioni relative al capitale sociale	In caso di operazione straordinarie approfondita valutazione contabile e fiscale con ausilio di esperti legali/tributari esterni	AU Consulenti esterni Assemblea dei soci Revisori legali
	Verifica della fattibilità finanziaria dell'operazione straordinaria	
	Controllo e approvazione della documentazione contrattuale relativa ad operazioni straordinarie da parte di AU	
	Fornire ai fini dell'approvazione dell'operazione straordinaria documentazione chiara, veritiera ed esaustiva	
	Adeguate conservazione e registrazione contabile	

C.3 Sistema di controllo

C.3.1 Principi generali di comportamento

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali aziendali e dei Destinatari, Dipendenti, e Consulenti/Partner nella misura necessaria alle funzioni dagli stessi svolte di:

- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- Violare i principi e le procedure esistenti in azienda e/o previste nella presente Parte Speciale.

La presente Parte Speciale prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

- Tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne e/o previste nella presente Parte Speciale in tutte le attività amministrative-contabile- finanziarie.
- Assicurare l'esistenza nell'impresa di un sistema sia organizzativo, sia amministrativo-contabile adeguati e che ricomprendano anche un sistema gestionale efficace.
- Assicurare la conduzione di corrette e tempestive determinazioni, dichiarazioni e liquidazioni delle imposte dovute per legge ed esecuzione dei connessi adempimenti.

C.3.2 Regole specifiche di comportamento

È fatto espresso obbligo a carico dei soggetti sopra indicati di:

- rispettare la normativa tributaria vigente, nonché le procedure ed i principi aziendali di comportamento, anche al fine di tutelare l'interesse finanziario dello Stato e dell'Unione Europea;
- presentare le dichiarazioni fiscali obbligatorie in ossequio ai principi di correttezza, veridicità e tempestività;
- utilizzare per tutte le attività amministrative/contabili il sistema informatico "Gestioni" per garantire la corretta e veridica imputazione di ogni operazione con fornitori, clienti, controparti o enti interessati, con la registrazione della causale dell'operazione attraverso modalità tali da consentire la tracciabilità dell'operazione e di eventuali variazioni successive nel Sistema;
- custodire in modo corretto e ordinato – anche approntando adeguate difese fisiche e/o informatiche – le scritture contabili e tutti gli atti e documenti di cui è obbligatoria la conservazione e metterli tempestivamente a disposizione dell'Amministrazione finanziaria che ne faccia richiesta;

- eseguire con correttezza e puntualità il pagamento delle imposte dovute ed il versamento delle somme dovute in qualità di sostituto di imposta;
- preservare l'integrità del patrimonio sociale da operazioni finalizzate ad eludere un'eventuale pretesa dell'Erario;
- Formazione adeguata, valutazione idoneità tecnica di tutti i soggetti coinvolti nelle attività considerate sensibili.

È fatto inoltre espresso divieto di:

- indicare, all'interno delle dichiarazioni fiscali obbligatorie, importi riferiti a documenti falsi o relativi a operazioni simulate, fraudolente o inesistenti;
- indicare nelle dichiarazioni fiscali elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi o inesistenti o crediti e ritenute fittizi, siano essi riferibili o meno alla documentazione di cui al punto precedente;
- emettere fatture o altri documenti aventi rilievo analogo a fronte di operazioni in tutto o in parte oggettivamente inesistenti o che indicano i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale;
- emettere fatture o altri documenti aventi rilievo analogo nei confronti di un soggetto diverso dal reale destinatario della prestazione;
- distruggere od occultare, anche parzialmente o temporaneamente, la documentazione contabile di cui è obbligatoria la conservazione;
- utilizzare in compensazione crediti non spettanti o inesistenti;
- porre in essere atti simulati o fraudolenti idonei a compromettere l'efficacia delle procedure di riscossione coattiva delle imposte.

Unirock S.r.l. si avvale di consulenti in materia fiscale, indipendenti e di comprovata professionalità, per la predisposizione delle dichiarazioni fiscali e per l'espletamento di tutti gli adempimenti richiesti dalla vigente normativa fiscale sotto il profilo amministrativo e contabile.

Tutte le attività sensibili delineate e le relative aree di rischio sono presidiate da procedure e/o istruzioni operative la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'OdV affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si richiama la procedura aziendale Gestione Amministrativa.

PARTE “D” REATI IN MATERIA DI SICUREZZA E SALUTE SUL LAVORO (art. 25 *septies* d.lgs. 231/2001)**D.1 Descrizione delle fattispecie normative**

Il rischio – reato connesso all’area di attività indicata (ossia quella più propriamente consistente nella realizzazione di opere infrastrutturali, stradali ed idrauliche e la manutenzione delle gallerie) sorge a seguito della violazione delle norme in materia di salute e sicurezza sul lavoro.

L’art. 25 *septies* del Decreto legislativo 231/2001, infatti, nella attuale formulazione, prevede sanzioni amministrative per le persone giuridiche nel caso di omicidio o lesioni colpose commessi con violazione delle norme in materia di sicurezza e salute nel lavoro.

L’elemento comune alle tre fattispecie di reato è la colpa, così definita dall’art. 43 del c.p.:

"Il delitto:

è doloso, o secondo l'intenzione, quando l'evento dannoso o pericoloso, che è il risultato dell'azione od omissione e da cui la legge fa dipendere l'esistenza del delitto, è dall'agente preveduto e voluto come conseguenza della propria azione od omissione;

è preterintenzionale, o oltre l'intenzione, quando dall'azione od omissione deriva un evento dannoso o pericoloso più grave di quello voluto dall'agente;

è colposo, o contro l'intenzione, quando l'evento, anche se preveduto, non è voluto dall'agente e si verifica a causa di negligenza o imprudenza o imperizia, ovvero per inosservanza di leggi, regolamenti, ordini o discipline [...]".

L’individuazione della responsabilità dell’ente richiede la verifica della condotta che ha concorso a determinare l’evento e la valutazione della stessa, al fine di verificare se essa sia stata caratterizzata dalla violazione di una regola cautelare e se l’autore della stessa potesse prevedere, con giudizio ex ante, quello specifico sviluppo causale e attivarsi per evitarlo.

Nell’ambito degli infortuni sul lavoro, il requisito dell’interesse si ravvisa qualora la persona fisica, pur non volendo il verificarsi dell’evento morte o lesioni del lavoratore, agisce consapevolmente allo scopo di conseguire un’utilità per la persona giuridica. Tale circostanza si ravvisa, ad esempio, quando la mancata adozione delle cautele infortunistiche risulta essere l’esito di una scelta finalisticamente orientata ad ottenere un risparmio sui costi d’impresa.

Le fattispecie delittuose in oggetto assumono rilevanza in questa sede in quanto siano conseguenze di violazioni alle norme di prevenzione degli infortuni e delle malattie nei luoghi di lavoro, norme contenute nel decreto legislativo 81/08 (e sue modificazioni) che, quindi, costituisce il riferimento per la valutazione della colpa. In particolare, per fissare obblighi e responsabilità dal momento che nella maggior parte dei casi la colpa viene individuata nella omissione di un comportamento doveroso proprio sulla base di quelle norme.

Poiché l’interesse o il vantaggio della Società rappresentano il fondamento della sua responsabilità, la contraddizione fra l’involontarietà dell’evento infortunistico e la necessità dell’interesse è stata risolta dalla giurisprudenza ravvisando l’interesse o il vantaggio per la Società non nell’evento ma nella condotta colposa del responsabile, individuando di volta in volta il vantaggio nel risparmio di tempi o di risorse nel corso dell’esecuzione del lavoro.

Particolare rilevanza assume la irrogazione di sanzioni interdittive sempre disposta in caso di condanna.

Si riporta di seguito una breve descrizione dei reati richiamati dall'art. 25 *septies* del D.lgs. 231/2001.

D.1.1 Omicidio colposo (art. 589 c.p.)

L'art. 589 c.p. sanziona la condotta di chi *“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 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”.

D.1.2 Lesioni personali colpose (art. 590, comma 3, 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 euro 309.

Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da euro 123 a euro 619; se è gravissima, della reclusione da tre mesi a due anni o della multa da euro 309 a euro 1239.

Se i fatti di cui al secondo comma sono commessi con violazione delle norme 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 2000 e la pena per 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”.

La lesione è considerata grave (art. 583, comma 1, c.p.) nei seguenti casi:

"1) se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;

2) se il fatto produce l'indebolimento permanente di un senso o di un organo."

La lesione è considerata, invece, gravissima se dal fatto deriva (art. 583 comma 2, c.p.):

"1) una malattia certamente o probabilmente insanabile;

2) la perdita di un senso;

3) la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella;

4) la deformazione, ovvero lo sfregio permanente del viso".

D.2 Attività sensibili

ATTIVITA' SENSIBILI	FASI	FUNZIONI INTERESSATE
Definizione organizzativa	Identificazione ruoli e funzioni rilevanti ex D.lgs. n. 81/2008	Datore di lavoro Delegati ex art. 16 D.lgs. 81/08
Identificazione competenze	Ricognizione ruoli e competenze interne ex D.lgs. n. 81/2008	Datore di lavoro Delegati ex art. 16 D.lgs. 81/08 Preposti
Informazione, formazione personale dipendente	Programmazione, erogazione e verifica dell'apprendimento delle attività formative e informative	Datore di Lavoro Delegati ex art. 16 D.lgs. 81/08 Preposti RSPP
Predisposizione, adozione, aggiornamento documentazione ex D.lgs. 81/08	DVR	Datore di Lavoro
	POS specifico per ciascun cantiere	Delegati ex art. 16 D.lgs. 81/08 RSPP
	DUVRI ex art. 26 D.lgs. 81/08	Consulente incaricato
Gestione sicurezza cantieri temporanei mobili	Controllo osservanza obblighi titolo IV D.lgs. 81/08	Datore di Lavoro Delegati ex art. 16 D.lgs. 81/08 Preposti RSPP Consulente incaricato
	Redazione / Congruenza POS cantiere / PSC / PO subappaltatori	
	Rispetto standard strutturali DPI / Attrezzature / Luoghi di lavoro	
	Predisposizione misure di prevenzione e protezione	
	Riunioni coordinamento / Cooperazione	

	Riunioni periodiche	
Affidamento lavori, servizi e forniture ad imprese appaltatrici o lavoratori autonomi	Verifica idoneità tecnico-professionale del fornitore	Datore di Lavoro Delegati ex art. 16 D.lgs. 81/08 Preposti Resp. Amm. RSPP
	Acquisizione documentazione certificazioni, autocertificazioni richieste dalla legge	
	Consegna POS / DUVRI	
	Riunione operativa di coordinamento e verbalizzazione	
Consultazione /partecipazione	Consultazione e partecipazione dei lavoratori o RLS	Datore di Lavoro Delegati ex art. 16 D.lgs. 81/08 RSPP

D.3 Sistema di controllo

D.3.1. Finalità della presente parte speciale

Si deve anzitutto evidenziare che i delitti di cui alla presente Parte Speciale, a differenza di tutti gli altri previsti dal Decreto, non consistono in condotte illecite volontarie; essi sono integrati da condotte meramente colpose, e quindi involontarie.

Nel caso di omicidio o lesioni colpose nessuno vuole la realizzazione dell'evento lesivo: esso avviene a causa di un'omissione del rispetto delle norme antinfortunistiche determinata da colpa (ossia da negligenza o imprudenza o imperizia), e non dalla volontà di cagionare quell'evento.

La presente Parte Speciale ha quindi la finalità di evidenziare le norme che la Società ha adottato con finalità di prevenzione, attraverso misure tecniche ed organizzative finalizzate all'assunzione puntuale ed esaustiva di tutti i rimedi e di tutte le misure imposte dalla legge e dai regolamenti e suggerite dalla miglior tecnologia, per la piena tutela della sicurezza del lavoro e la riduzione al minimo del rischio.

Il proposito di Unirock Srl nell'adottare la presente Parte Speciale, quindi, non è tanto quello di dettare una serie di norme di condotta volte alla prevenzione di infortuni ed incidenti, e ciò in considerazione del fatto che la Società è già dotata di un adeguato sistema di procedure in materia di tutela della salute e della sicurezza nei luoghi di lavoro, corrispondenti alla normativa di cui al Testo Unico ed alle successive integrazioni e modifiche, bensì quello di richiamare la documentazione, le procedure e l'organizzazione esistente in forza di quanto disposto dall'art. 30 del D.Lgs. 81/08 s.m.i.. In effetti Unirock Srl è dotata di una organizzazione che, considerata la natura e il tipo di attività che viene svolta, assicura attraverso una articolazione di funzioni con competenze tecniche e poteri necessari la verifica, valutazione, gestione e controllo del rischio.

D.3.2 Principi generali di comportamento

Unirock Srl ha da tempo codificato i principi generali cui intende conformarsi nell'affrontare la questione della tutela della sicurezza e della salute del lavoro.

La Società considera la tutela della salute e della sicurezza non semplicemente un obbligo di Legge, ma un dovere morale. La Società ritiene, infatti, che la tutela della salute e della sicurezza dei lavoratori rappresenti una concreta possibilità di crescita per l'impresa stessa e per i suoi lavoratori. In tal senso si impegna da sempre a garantire ai propri dipendenti condizioni di lavoro rispettose della dignità delle persone ed ambienti di lavoro sicuri, sviluppando tra i lavoratori la consapevolezza dei rischi legati all'esercizio dell'Attività, e promuovendo l'adozione di comportamenti responsabili e conformi alle disposizioni normative da parte di tutti, dipendenti e collaboratori.

Unirock Srl svolge quindi la propria attività di impresa nel pieno rispetto dei principi di salvaguardia dell'integrità psico-fisica dei propri lavoratori e fonda la propria politica aziendale per la tutela della salute e della sicurezza dei lavoratori sui seguenti obiettivi:

- la diminuzione nel tempo della frequenza e della gravità dei fenomeni infortunistici e delle malattie professionali, al minimo livello tecnicamente raggiungibile;

- l'adozione, in ogni scelta tecnica ed organizzativa, delle misure di prevenzione e protezione necessarie per eliminare i rischi, o per ridurli per quanto possibile tecnicamente;
- il mantenimento nel tempo dei livelli di sicurezza desiderati, compatibilmente con la gestione ottimale dei costi della sicurezza, anche attraverso l'impiego efficiente e pianificato delle risorse umane, tecnologiche e materiali in possesso dell'impresa.

A tal fine, Unirock Srl ha fatto del costante aggiornamento degli strumenti e delle tecnologie messe a disposizione dei propri dipendenti per l'esercizio delle attività aziendali uno dei principi cardine della propria attività d'impresa.

Per perseguire gli obiettivi che caratterizzano la propria politica aziendale, Unirock Srl è impegnata:

- a rispettare la normativa vigente e quella che entrerà in vigore in futuro, in materia di tutela della salute e della sicurezza;
- ad assicurare comprensione, attuazione e sostegno della propria politica a tutti i livelli aziendali al fine di garantire la partecipazione al sistema in funzione delle competenze e delle responsabilità di ciascuno, nella consapevolezza che per il raggiungimento degli obiettivi indicati è necessario l'impegno di tutti;
- a valorizzare la formazione e l'opera di tutte le persone direttamente impegnate nella tutela della salute e della sicurezza dei lavoratori, conferendo alla specifica funzione aziendale l'importanza che merita, con la consapevolezza che il perseguimento degli obiettivi indicati necessita di idonee competenze tecniche e gestionali;
- a valorizzare le competenze specifiche di tutti i lavoratori, fornendo ad essi la necessaria informazione e formazione sui rischi e sulle misure di eliminazione o riduzione degli stessi, riconoscendo che i principali artefici del miglioramento dei livelli di sicurezza in azienda sono i lavoratori stessi;
- a pretendere da parte di tutto il personale che opera in azienda, interno ed esterno, il rispetto della vigente normativa in materia di salute e sicurezza sul lavoro, nonché di tutte le disposizioni interne che l'azienda ha stabilito o stabilirà, con l'obiettivo di migliorare e mantenere i livelli di sicurezza;
- a garantire ai propri dipendenti il costante adeguamento delle attrezzature, dei macchinari e dei dispositivi di protezione individuale, con la consapevolezza che l'aggiornamento delle apparecchiature in uso ai dipendenti per l'esercizio delle attività, sulla base degli adeguamenti tecnico scientifici, contribuisce al raggiungimento degli obiettivi perseguiti in materia dalla Società;
- a promuovere l'applicazione delle norme di tutela della salute e della sicurezza anche mediante richiesta che ogni dipendente segnali eventuali carenze o anomalie di funzionamento di macchine, attrezzature di lavoro o dispositivi di sicurezza, che possano causare dei danni alla

salute ed alla sicurezza dei lavoratori, nonché eventuali violazioni alle vigenti disposizioni normative ed alle disposizioni interne.

D.3.3 Regole specifiche di comportamento

Il sistema di gestione della sicurezza ai sensi del D.lgs. 30 aprile 2008 n. 81

Per l'applicazione della politica aziendale di sicurezza e salute e il raggiungimento dei fini, che si propone in questo settore, Unirock S.r.l. opera con un consolidato sistema interno di gestione della prevenzione e protezione dei lavoratori sui luoghi di lavoro, conforme alla vigente normativa in materia e rispettoso di quanto è previsto dal già citato art. 30 del decreto 81/08 per il quale il Datore di Lavoro è stato individuato nell'Amministratore Unico, ai dirigenti e preposti a mezzo delega ai sensi dell'art. 16 e lettere di incarico sono stati ricordati i loro obblighi e i loro poteri, i lavoratori sono stati informati e formati secondo le necessità richieste dall'attività che viene loro affidata.

In particolare, la Società ha adempiuto alle disposizioni di cui al Testo Unico della sicurezza individuando le funzioni ed i soggetti deputati alla gestione delle singole aree, nonché le metodologie e gli strumenti di prevenzione.

Gli elementi del sistema di gestione della sicurezza tengono conto della specificità della società che, nell'ambito dell'Unità Produttiva principale e delle Unità locali, attraverso un'organizzazione di Dirigenti e di Preposti, svolge attività:

- negli uffici, che comprendono anche il magazzino, siti in Bolzano;
- nelle Unità locali site in Marocco, Sospirolo (magazzino) e Visso;
- nei cantieri esterni in Italia o all'estero di varia complessità e durata.

Il sistema di gestione della sicurezza, in conformità alle norme vigenti e alla giurisprudenza, si articola sui seguenti elementi:

- un sistema organizzativo formalizzato con il quale la Società con deleghe ex art. 16 e con nomine specifiche indica la suddivisione dei poteri, compiti e responsabilità in tema di tutela della salute e sicurezza nei luoghi di lavoro che coincide con il sistema di poteri, compiti e responsabilità a fini produttivi in modo che effettivamente Dirigenti e Preposti siano responsabili delle attività che dirigono o a cui sovrintendono;
- un Documento di Valutazione dei Rischi (DVR) attraverso il quale per ciascuna area di lavoro e per ciascun gruppo omogeneo di lavoratori vengono individuate le idonee misure di prevenzione e protezione collettive ed individuali;
- procedure finalizzate alla regolamentazione delle attività potenzialmente pericolose o che necessitano di specifica disciplina;

- sistema di formazione, informazione ed addestramento per il personale dipendente dalla Società in conformità alla normativa vigente;
- DVRS e/o POS specifici per ciascun cantiere.
- DVRS e/o POS specifici per ciascun cantiere.

D.3.4 Aree di rischio

Il Documento di Valutazione dei Rischi redatto ex D.lgs. 81/08 dettaglia le singole aree dove vengono sviluppate le attività rilevanti ai fini della prevenzione antinfortunistica e della tutela della salute dei lavoratori.

Il “livello di rischio” dei dipendenti chiamati ad operare nell’una o nell’altra area/attività indicate è diverso, così come è evidente che possono coesistere diverse mansioni con altrettante diversità anche nel “livello di rischio”. Su tali basi è stato sviluppato il Documento di Valutazione dei Rischi.

Nel caso in cui il personale aziendale sia impegnato in attività ricadenti nell’ambito del Titolo IV del D.Lgs. 81/08 (cantieri temporanei e mobili) è prevista la redazione del Piano Operativo di Sicurezza (POS) in coerenza con quanto definito dal Piano di Sicurezza e Coordinamento (PSC) predisposto dalla Committenza.

Per la gestione, invece, dei lavori che ricadono nei contratti d’appalto, d’opera o di somministrazione di cui all’art. 26 del D.Lgs. 81/08 è prevista la predisposizione del Documento Unico di Valutazione dei Rischi (DUVRI) che fornisce informazioni in merito ai luoghi di lavoro del committente, agli obblighi e divieti per gli appaltatori e alle misure da adottare per garantire l’eliminazione o riduzione dei rischi da interferenza.

Ai fini della disciplina della presente sezione del Modello vengono pertanto assunte quali “aree a rischio” quelle indicate nei Documenti di Valutazione dei Rischi (DVR, POS, DUVRI).

D.3.5 L’Organizzazione

Il “Datore di Lavoro” in materia di prevenzione degli infortuni e tutela della salute e sicurezza dei lavoratori coincide con l’Amministratore Unico in quanto soggetto che esercita i poteri decisionali e di spesa.

Il Datore di Lavoro ha formalizzato attraverso deleghe ex art. 16 ai dirigenti le responsabilità che discendono dal D.lgs 81/08 secondo il principio legislativo e giurisprudenziale della responsabilità connessa alle attività da ciascuno dirette, controllate o eseguite e per l’area di lavoro di competenza. La linea operativa si avvale per le attività di sicurezza e protezione, del supporto tecnico delle altre competenze aziendali e specificatamente del Servizio di Prevenzione e Protezione e del Medico Competente per la sorveglianza sanitaria. Nei cantieri esterni vengono specificatamente nominati i Capi Cantiere e i preposti incaricati della vigilanza.

D.3.6 I soggetti

Secondo quanto dispongono gli articoli 2, 16, 17, 18, 19, 20, 22, 23, 24 e 25 del D.lgs. 81/08 i soggetti interessati dalla presente parte speciale sono:

- il datore di lavoro è il soggetto che, in base al tipo e l'assetto dell'organizzazione, ne ha la responsabilità in quanto esercita i poteri decisionali e di spesa;
- i dirigenti, che esercitano le funzioni ad essi attribuite secondo le competenze assegnate in conformità di quanto stabilito dagli artt. 16 e 18 del D.lgs. 81/08;
- i preposti, che secondo le loro attribuzioni e competenze hanno gli obblighi previsti dall'art. 19 del D.lgs. 81/08;
- i lavoratori, cui spetta adempiere agli obblighi di cui all'art. 20 del D.lgs. 81/08;
- il medico competente, cui spetta adempiere agli obblighi di cui all'art. 25 del D.lgs. 81/08;
- gli addetti alle emergenze, incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza;

La Società, in conformità a quanto previsto dal D.Lgs. 81/08 ha provveduto ad affidare lo svolgimento di compiti del Servizio di Prevenzione e Protezione (RSPP) ad un soggetto esterno di comprovata esperienza, in possesso dei requisiti di professionalità e competenza richiesti dalla normativa vigente, con i compiti previsti dalla legge in particolare dall'art. 33 del D.lgs. 81/08.

Tale scelta è stata effettuata a seguito di adeguata valutazione delle esigenze organizzative e dei profili di rischio aziendale, garantendo in ogni caso l'efficace svolgimento delle funzioni di prevenzione e protezione e il pieno rispetto degli obblighi di legge in materia di salute e sicurezza sul lavoro.

Il medico competente, sulla base dell'esito della valutazione dei rischi, ha elaborato un programma di sorveglianza sanitaria che aggiorna in ragione di eventuali modificazioni dei cicli produttivi ed esprime i giudizi di idoneità o meno alla mansione specifica. Il medico competente sulla base dei fattori di rischio per la salute stabilisce la periodicità e la tipologia degli accertamenti clinici, strumentali e di laboratorio che devono essere svolti.

D.3.6.1 La formazione

La Società assicura che ciascun lavoratore riceva adeguata formazione, informazione e addestramento, secondo quanto disposto dalle norme in materia (artt. 36 e 37 D.Lgs. 81/08), in particolare:

- al momento dell'assunzione;
- in occasione del trasferimento o di un cambio di mansioni;
- in occasione della messa in esercizio di nuove attrezzature, macchinari o impianti o dell'utilizzo di nuove sostanze.

Il sistema di formazione, informazione e addestramento del personale dipendente della Società, in materia di prevenzione e protezione in merito ai rischi ed alle modalità sicure di svolgimento della mansione assegnata, è attuato in collaborazione con il Responsabile del Servizio di Prevenzione e Protezione e di consulenti esterni di comprovata professionalità e competenza.

Le attività di aggiornamento formativo sono oggetto di una specifica pianificazione periodica, in funzione dello sviluppo o del quadro normativo di riferimento e/o delle attrezzature, materiali e tecnologie impiegate nel processo industriale.

D.3.7 Principi di comportamento e di attuazione del processo decisionale in conformità alle norme OHSAS 45001

Unirock S.r.l. opera con un sistema interno di gestione della prevenzione e protezione dei lavoratori sui luoghi di lavoro, conforme alle vigenti norme OHSAS 45001.

Gli elementi del sistema di gestione della sicurezza tengono conto della specificità della Società che attraverso un'organizzazione complessa ed articolata di dirigenti di vario livello e di preposti, svolge attività:

- nella Sede di Bolzano e nelle Unità locali;
- nei cantieri esterni in Italia e all'estero di varia complessità e durata.

Poiché il principio ispiratore del D.Lgs. 81/08 si può sintetizzare attraverso la convinzione che la sicurezza sul lavoro si ottiene responsabilizzando tutti coloro (dipendenti e non) che operano all'interno delle aree aziendali e/o delle aree all'interno delle quali prestano la loro opera lavorativa, destinatari della presente Parte Speciale sono tutti i lavoratori della Società, ciascuno in base alle proprie attribuzioni e competenze, nonché tutti i soggetti terzi a vario titolo coinvolti dall'attività aziendale.

La presente Parte Speciale prevede l'espresso divieto a tutti i lavoratori di porre in essere, o anche tollerare che altri pongano in essere, comportamenti:

- tali da integrare le fattispecie di reato considerate dal D. Lgs. 81/08;
- che possano compromettere i presidi di sicurezza adottati dalla società favorendo potenzialmente la commissione dei reati di omicidio colposo e lesioni personali colpose;
- non conformi alle procedure aziendali o, comunque, non in linea con i principi espressi dal presente Modello in materia di sicurezza e igiene dei luoghi di lavoro.

Ai collaboratori esterni ed appaltatori sono stati estesi obblighi e divieti, per quanto di loro competenza, attraverso apposite clausole contrattuali.

Nell'ambito del sistema interno di gestione della prevenzione e protezione dei lavoratori sui luoghi di lavoro, come da disposizioni di legge e norma tecnica di settore, spetta al datore di lavoro:

- organizzare e gestire la Società secondo principi e criteri conformi alle norme di legge, ai principi del presente documento e del codice etico;

- valutare i rischi per la sicurezza e salute dei lavoratori ed elaborare il “Documento sulla valutazione dei rischi” previsto dal T.U. con le modalità ivi prescritte;
- designare il responsabile del servizio di prevenzione e protezione dai rischi;
- affidare ai lavoratori i compiti e le responsabilità in relazione alle loro aree di competenza, munendoli di tutti i poteri di organizzazione, gestione e controllo richiesti dalle funzioni delegate o assegnate.

È fatto obbligo al datore di lavoro, ai dirigenti, in base alle funzioni conferite, nell’ambito delle loro aree di competenza e avvalendosi dei soggetti loro subordinati, nonché delle altre strutture o risorse aziendali per loro disponibili, di:

- nominare il medico competente per l’effettuazione della sorveglianza sanitaria e, ove previsti, il medico autorizzato e l’esperto qualificato;
- designare preventivamente i lavoratori incaricati dell’attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell’emergenza;
- designare i preposti;
- nell’affidare i compiti ai lavoratori, tenere conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute ed alla sicurezza;
- fornire ai lavoratori i necessari ed idonei dispositivi di protezione individuale, sentito il responsabile del servizio di prevenzione e protezione ed il medico competente;
- prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico;
- richiedere l’osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione;
- richiedere al medico competente l’osservanza degli obblighi a loro carico, rispettivamente nel D.Lgs. 81/08 e s.m.i.;
- adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
- informare prima possibile i lavoratori esposti al rischio di un pericolo grave ed immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
- adempiere agli obblighi di informazione, formazione e addestramento di cui agli articoli 36 e 37 del T.U.;

- impedire ai lavoratori di proseguire la loro attività in una situazione di lavoro in cui sussiste un pericolo grave e immediato;
- consentire ai lavoratori di verificare, mediante il rappresentante dei lavoratori per la sicurezza, l'applicazione delle misure di sicurezza e di protezione della salute;
- consegnare tempestivamente al rappresentante dei lavoratori per la sicurezza, su richiesta di questi e per l'espletamento della sua funzione, copia del documento di cui all'articolo 17, comma 1, lettera a), nonché consentire al medesimo rappresentante di accedere ai dati di cui alla lettera q) del D.lgs. 81/08 e s.m.i.;
- elaborare il documento di cui all'articolo 26, comma 3 del D.lgs. 81/08 e s.m.i e, su richiesta di questi e per l'espletamento della sua funzione, consegnarne tempestivamente copia ai rappresentanti dei lavoratori per la sicurezza;
- prendere appropriati provvedimenti per evitare che le misure tecniche adottate possano causare rischi per la salute della popolazione o deteriorare l'ambiente esterno verificando periodicamente la perdurante assenza di rischio;
- comunicare in via telematica all'INAIL, nonché per suo tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro di cui all'articolo 8, entro 48 ore dalla ricezione del certificato medico, a fini statistici e informativi, i dati e le informazioni relativi agli infortuni sul lavoro che comportino l'assenza dal lavoro di almeno un giorno, escluso quello dell'evento e, a fini assicurativi, quelli relativi agli infortuni sul lavoro che comportino un'assenza al lavoro superiore a tre giorni;
- consultare il rappresentante dei lavoratori per la sicurezza nelle ipotesi di cui all'articolo 50 del D.lgs. 81/08 e s.m.i.;
- adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro, adeguate alla natura dell'attività, alle dimensioni dell'azienda o dell'unità produttiva, e al numero delle persone presenti;
- nell'ambito dello svolgimento di attività in regime di appalto e di subappalto, munire i lavoratori di apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore, l'indicazione del datore di lavoro;
- in caso di affidamento di lavori, servizi e forniture all'impresa appaltatrice o a lavoratori autonomi verificare l'idoneità tecnico professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori, ai servizi e alle forniture da affidare in appalto o mediante contratto d'opera o di somministrazione;
- garantire, nell'ambito dei cantieri temporanei o mobili, il rispetto delle prescrizioni applicabili di cui al titolo IV del D.lgs. 81/08 e s.m.i.;
- convocare la riunione periodica di cui all'articolo 35 del D.lgs. 81/08 e s.m.i.;

- aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;
- vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità.

Ai preposti, nell'ambito delle loro attribuzioni e competenze, è fatto obbligo di:

- sovrintendere e vigilare sulla osservanza da parte dei singoli lavoratori dei loro obblighi di legge, nonché delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messa a loro disposizione e, in caso di persistenza della inosservanza, fermare il lavoratore o l'attività lavorativa;
- verificare affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;
- richiedere l'osservanza delle misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato e inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
- informare prima possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
- impedire ai lavoratori, di proseguire la loro attività in una situazione di lavoro in cui sussiste un pericolo grave ed immediato;
- segnalare tempestivamente al delegato sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro, delle quali venga a conoscenza sulla base della formazione ricevuta;
- frequentare appositi corsi di formazione, secondo quanto previsto dall'articolo 37 del D.lgs. 81/08 e s.m.i..
- in caso di rilevazione di deficienze dei mezzi e delle attrezzature di lavoro e di ogni condizione di pericolo rilevata durante la vigilanza, se necessario, interrompere temporaneamente l'attività e, comunque, segnalare tempestivamente al datore di lavoro e al dirigente le non conformità rilevate;

Ai singoli lavoratori è fatto obbligo di:

- contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;
- osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;

- utilizzare correttamente i macchinari, le apparecchiature, gli utensili, le sostanze ed i preparati pericolosi, i mezzi di trasporto, le altre attrezzature di lavoro, nonché i dispositivi di sicurezza e di protezione (DPI) messi a loro disposizione conformemente all'informazione e formazione ricevute e all'addestramento eventualmente organizzato;
- aver cura delle attrezzature di lavoro e dei DPI messi a loro disposizione, non apportando modifiche di loro iniziativa e segnalando immediatamente al datore, all'RSPP o al preposto qualsiasi difetto od inconveniente rilevato;
- segnalare immediatamente al delegato o al subdelegato al dirigente, al preposto o al servizio di prevenzione e protezione le deficienze dei mezzi e dei dispositivi citati in precedenza, nonché le altre eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze e pericoli, dandone notizia al rappresentante dei lavoratori per la sicurezza;
- non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza, ovvero che possono compromettere la sicurezza propria e di altri lavoratori;
- partecipare ai programmi di formazione e di addestramento organizzati dal datore di lavoro;
- sottoporsi ai controlli sanitari previsti dal D.lgs. 81/08 e s.m.i. o comunque disposti dal medico competente.

Al servizio di prevenzione e protezione, utilizzato dal datore di lavoro, dai dirigenti dai preposti e dai lavoratori è fatto espresso obbligo di attuare i compiti indicati all'art. 33 del T.U. e quindi, con la collaborazione del datore di lavoro dei dirigenti e dei preposti, provvedere:

- all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto delle norme vigenti sulla base della specifica conoscenza dell'organizzazione aziendale;
- ad elaborare, per quanto di competenza, le misure preventive e protettive di cui all'articolo 28, comma 2 del T.U., ed i sistemi di controllo di tali misure;
- ad elaborare le procedure di sicurezza per le varie attività aziendali;
- a proporre i programmi di informazione e formazione dei lavoratori;
- a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonché alla riunione periodica di cui all'articolo 35 del T.U.;
- a fornire ai lavoratori le informazioni di cui all'articolo 36 del T.U.

Al medico competente e, ove previsto, al medico autorizzato è fatto obbligo di:

- collaborare con il datore di lavoro e con il servizio di prevenzione e protezione alla valutazione dei rischi, anche ai fini della programmazione, ove necessario, della sorveglianza sanitaria, alla predisposizione della attuazione delle misure per la tutela della salute e della integrità psico-fisica dei lavoratori, all'attività di formazione e informazione nei confronti dei lavoratori, per la parte di competenza, e alla organizzazione del servizio di primo soccorso considerando i particolari tipi di lavorazione ed esposizione e le peculiari modalità organizzative del lavoro;
- programmare ed effettuare la sorveglianza sanitaria di cui all'articolo 41 D.lgs. 81/08 e dell'articolo 83 D.lgs. 230/1995, attraverso protocolli sanitari definiti in funzione dei rischi specifici e tenendo in considerazione gli indirizzi scientifici più avanzati. Emettere, sulla base dei risultati della sorveglianza sanitaria, il giudizio di idoneità del lavoratore alla mansione specifica (con o senza prescrizione) stabilendo, laddove necessario e tecnicamente possibile, i limiti di esposizione;
- istituire, aggiornare e custodire, sotto la propria responsabilità, una cartella sanitaria e di rischio per ogni lavoratore sottoposto a sorveglianza sanitaria che provvederà a consegnare al datore di lavoro in caso di cessazione dall'incarico e al lavoratore alla cessazione del rapporto di lavoro;
- fornire informazioni ai lavoratori sul significato della sorveglianza sanitaria cui sono sottoposti e, nel caso di esposizione ad agenti con effetti a lungo termine, sulla necessità di sottoporsi ad accertamenti sanitari anche dopo la cessazione dell'attività che comporta l'esposizione a tali agenti. A richiesta, ha l'obbligo di fornire informazioni analoghe ai rappresentanti dei lavoratori per la sicurezza;
- comunicare per iscritto, in occasione delle riunioni periodiche, al datore di lavoro, al responsabile del servizio di prevenzione protezione dai rischi, ai rappresentanti dei lavoratori per la sicurezza, i risultati anonimi collettivi della sorveglianza sanitaria effettuata e fornire indicazioni sul significato di detti risultati ai fini della attuazione delle misure per la tutela della salute e della integrità psico-fisica dei lavoratori;
- visitare gli ambienti di lavoro almeno una volta all'anno o a cadenza diversa che stabilisce in base alla valutazione dei rischi; l'indicazione di una periodicità diversa dall'annuale deve essere comunicata al datore di lavoro ai fini della sua annotazione nel documento di valutazione dei rischi;
- partecipare alla programmazione del controllo dell'esposizione dei lavoratori i cui risultati gli sono forniti con tempestività ai fini della valutazione del rischio e della sorveglianza sanitaria.

I Destinatari della presente sezione devono esercitare un controllo continuo e puntuale teso ad evidenziare rischi che potrebbero comportare la realizzazione dei reati indicati nell'art. 25-*septies* ed in generale qualunque situazione che possa comportare un pericolo per l'igiene e la salute dei lavoratori e di tutti i soggetti comunque presenti nelle aree della Società.

Le attività connesse con il presente profilo di rischio devono essere gestite nel rispetto delle norme applicabili e del sistema normativo aziendale che, prevede quanto segue:

- nomine/designazioni delle funzioni rilevanti per la sicurezza. In tema di deleghe di responsabilità e nomine/designazioni delle funzioni rilevanti per la sicurezza viene garantito che:
 - le nomine e le designazioni dei soggetti responsabili in materia di salute e sicurezza sul lavoro sono adeguatamente formalizzate, con firma da parte dei soggetti incaricati, e pubblicizzate all'interno della Società e all'esterno;
 - il sistema delle nomine e designazioni è coerente con l'evoluzione dell'organizzazione societaria;
 - le Funzioni incaricate di compiti rilevanti per la sicurezza sono dotate dei poteri di organizzazione, gestione e controllo, ed eventualmente di spesa, adeguati alla struttura e alla dimensione dell'organizzazione e alla natura dei compiti assegnati in considerazione anche della possibilità del verificarsi di casi di urgenze non prevedibili né rinviabili;
 - sono definite le responsabilità e le modalità operative atte ad assicurare la verifica del possesso e del mantenimento dei requisiti di competenza e professionalità richiesti per le figure rilevanti per la sicurezza, con particolare riferimento ai requisiti di aggiornamento periodico obbligatori;
- rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici. Sono formalizzati ruoli, responsabilità e modalità operative atte a garantire:
 - idonei flussi informativi tra il servizio SPP e le Funzioni a vario titolo coinvolte nel processo di approvvigionamento di beni e servizi, al fine di assicurare una gestione degli acquisti che tenga conto dell'esigenza di valutare preliminarmente i rischi che possono essere introdotti nella Società in fase di approvvigionamento;
 - il rispetto dei principi generali di prevenzione in materia di salute e sicurezza sul lavoro al momento delle scelte progettuali e tecniche, nella scelta di attrezzature, componenti e dispositivi di protezione e nella gestione di sostanze e preparati pericolosi;
 - il mantenimento nel tempo degli standard tecnico-strutturali di legge, di attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici tramite adeguanti interventi di manutenzione ordinaria e straordinaria e verifiche periodiche che tengano conto di quanto previsto dalla norma tecnica di settore, nonché delle informazioni contenute nei libretti d'uso e manutenzione delle singole apparecchiature, attrezzature, impianti;
- valutazione dei rischi (DVR) e predisposizione delle misure di prevenzione e protezione;
- gestione della sicurezza nei cantieri temporanei o mobili: sono formalizzati ruoli, responsabilità e modalità operative atte ad assicurare:
 - l'assolvimento di tutti gli obblighi di cui al titolo IV° del D.lgs. 81/08 e s.m.i. (cantieri temporanei o mobili). In particolare, viene garantita l'osservanza degli obblighi previsti dalla legge in materia attraverso la redazione dei Piani Operativi per la Sicurezza di competenza, verificando la congruenza dei Piani Operativi dei subappaltatori con il Piano Operativo di Unirock e con il Piano di Sicurezza del Committente.

Prima dell'inizio dei lavori e nel corso di essi, sono previste apposite riunioni di coordinamento e cooperazione condotte eventualmente anche con la partecipazione degli appaltatori e fornitori.

Appaltatori, fornitori e lavoratori autonomi hanno l'obbligo, sotto pena di sanzioni disciplinari, di osservare le regole operative afferenti la salute e la sicurezza nei luoghi di lavoro stabilite nel presente Modello, nelle clausole contrattuali, nei documenti di sicurezza, nelle disposizioni relative ai rischi **interferenziali**. **Viene richiesto** agli appaltatori di assumere analoghe iniziative volte a trasmettere tutta la documentazione, le informazioni e gli obblighi relativi, verso i subappaltatori;

- riunioni periodiche della sicurezza e consultazione dei RLS: sono formalizzati ruoli, responsabilità e modalità operative atte ad assicurare:
 - la consultazione dei RLS in tutti i casi previsti dall'art. 50 del D.Lgs. 81/08 garantendone adeguata tracciabilità;
 - lo svolgimento con periodicità almeno annuale di una riunione cui partecipano il datore di lavoro o un suo rappresentante, il responsabile del servizio di prevenzione e protezione, il medico competente, il medico autorizzato (ove previsto), i rappresentanti dei lavoratori per la sicurezza. Nel corso della riunione, di cui si conserva adeguata tracciabilità, vengono trattati almeno i seguenti argomenti:
 - il documento di valutazione dei rischi;
 - l'andamento degli infortuni e delle malattie professionali e della sorveglianza sanitaria;
 - i criteri di scelta, le caratteristiche tecniche e l'efficacia dei dispositivi di protezione individuale;
 - i programmi di informazione e formazione di dirigenti, preposti, lavoratori ai fini della sicurezza e della protezione della loro salute.

La riunione ha altresì luogo 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.

- formazione, informazione e addestramento di dirigenti, preposti, lavoratori e particolari categorie di lavoratori: sono formalizzati ruoli, responsabilità e modalità operative atte ad assicurare:
 - un'adeguata formazione, informazione, addestramento dei lavoratori in conformità a quanto stabilito dagli artt. 36 e 37 del D.lgs. 81/08 e s.m.i. e dall'Accordo in sede di Conferenza permanente per i rapporti tra lo Stato e le Regioni;
 - il possesso dei necessari requisiti da parte dei formatori della sicurezza in accordo a quanto definito dal citato Accordo Stato Regioni;
 - la tracciabilità dei processi di formazione, informazione, addestramento e verifica periodica dell'apprendimento;

Nello specifico è previsto che ciascun lavoratore riceva una adeguata informazione:

- sui rischi per la salute e sicurezza sul lavoro connessi alla attività della impresa in generale;
- sulle procedure che riguardano il primo soccorso, la lotta antincendio, l'evacuazione dei luoghi di lavoro;
- sui nominativi dei lavoratori incaricati di applicare le misure di primo soccorso e antincendio;
- sui nominativi del responsabile del servizio di prevenzione e protezione e del medico competente;
- sui rischi specifici cui è esposto in relazione all'attività svolta, sulle norme di sicurezza e le disposizioni aziendali in materia;
- sui pericoli connessi all'uso delle sostanze e dei preparati pericolosi sulla base delle schede dei dati di sicurezza previste dalle norme vigenti e dalle norme di buona tecnica;
- sulle misure e le attività di protezione e prevenzione adottate.

Nello specifico è previsto che ciascun lavoratore riceva una formazione sufficiente ed adeguata in merito ai rischi specifici di cui al D.lgs. 81/08. La formazione e, ove previsto, l'addestramento specifico avviene in occasione:

- della costituzione del rapporto di lavoro o dell'inizio dell'utilizzazione qualora si tratti di somministrazione di lavoro e/o di prestazioni occasionali di tipo accessorio;
- del trasferimento o cambiamento di mansioni;
- dell'evoluzione dei rischi, dell'insorgenza di nuovi rischi o di modifiche legislative.

L'azienda definisce ruoli, responsabilità e modalità operative per assicurare adeguata formazione, e i necessari aggiornamenti periodici, a particolari categorie di lavoratori, quali:

- dirigenti e preposti;
- lavoratori incaricati dell'attività di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave ed immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza.
- sorveglianza sanitaria e gestione degli infortuni: la sorveglianza sanitaria viene garantita attraverso protocolli sanitari definiti dal medico competente e, ove ne ricorra l'obbligo, dal medico autorizzato e dall'esperto qualificato sulla base dei rischi specifici. Nel pianificare le attività di sorveglianza sanitaria è fatto obbligo di considerare l'eventuale presenza di lavoratori in distacco o distaccati, personale interinale, personale che effettua prestazioni occasionali di tipo accessorio. La periodicità dei controlli tiene conto delle norme applicabili, nonché del livello dei rischi. Sono formalizzati ruoli, responsabilità e modalità operative atte ad assicurare:

- la visita medica preventiva intesa a constatare l'assenza di controindicazioni al lavoro cui il lavoratore è destinato al fine di valutare la sua idoneità alla mansione specifica;
- la visita medica periodica per controllare lo stato di salute dei lavoratori ed esprimere il giudizio di idoneità alla mansione specifica;
- la visita medica su richiesta del lavoratore, qualora sia ritenuta dal medico competente correlata ai rischi professionali o alle sue condizioni di salute, suscettibili di peggioramento a causa dell'attività lavorativa svolta, al fine di esprimere il giudizio di idoneità alla mansione specifica;
- la visita medica in occasione del cambio della mansione onde verificare l'idoneità alla mansione specifica;
- la visita medica alla cessazione del rapporto di lavoro nei casi previsti dalle norme vigenti;
- la visita medica preventiva in fase pre-assuntiva;
- la visita medica precedente alla ripresa del lavoro, a seguito di assenza per motivi di salute di durata superiore ai sessanta giorni continuativi, al fine di verificare l'idoneità alla mansione;
- l'aggiornamento tempestivo del protocollo sanitario in relazione all'evolversi dell'organizzazione aziendale;
- l'istituzione e aggiornamento, ove ne ricorra l'obbligo, dei documenti sanitari personali e loro consegna all'ISPESL con le modalità previste all'art. 90 del D.lgs. 230/95 e s.m.i..

È fatto divieto di effettuare visite mediche per accertare stati di gravidanza e negli altri casi vietati dalle norme vigenti.

La cartella sanitaria e di rischio, istituita e mantenuta aggiornata per ogni lavoratore sottoposto a sorveglianza sanitaria a cura del medico competente e, ove previsto, del medico autorizzato, è custodita con salvaguardia del segreto professionale e della privacy presso il luogo concordato con il datore di lavoro o suo delegato al momento della nomina.

L'azienda definisce, inoltre, ruoli, responsabilità e modalità operative per garantire:

- una tempestiva comunicazione al medico competente, al medico autorizzato (ove previsto) e all'esperto qualificato (ove previsto) in merito alle variazioni relative all'organico aziendale (es. assunzioni, cambio mansioni, cessazioni, rientri dopo malattie con assenze superiori ai 60 gg, ecc.) affinché questi possano assicurare l'aggiornamento del calendario delle visite di idoneità e sorveglianza sanitaria;
- la vigilanza sull'assolvimento degli obblighi previsti per il medico competente e l'esperto qualificato compresa la visita degli ambienti di lavoro da parte del medico competente/medico autorizzato almeno una volta all'anno o con cadenza differente, stabilita in funzione dei risultati della Valutazione dei Rischi;
- l'assolvimento degli obblighi di registrazione e comunicazione in caso di infortuni;
- l'analisi e monitoraggio degli infortuni compresi i *near miss*.

- vigilanza e verifiche periodiche in merito al rispetto delle procedure e delle istruzioni di lavoro in sicurezza e all'efficacia delle procedure adottate: sono definiti ruoli, responsabilità e modalità operative atte ad assicurare:
 - la vigilanza sul rispetto delle procedure e delle istruzioni di sicurezza da parte del personale aziendale;
 - la segnalazione dei rischi rilevati e dell'eventuale mancato rispetto delle norme di sicurezza da parte del personale aziendale;
 - l'applicazione del sistema disciplinare in caso di violazioni riscontrate;
 - la definizione e implementazione di adeguati piani di azione per sanare eventuali difformità e/o carenze riscontrate nel corso delle verifiche.

Il personale della società, a qualsiasi titolo coinvolto nelle attività di gestione degli aspetti in materia antinfortunistica e di tutela dell'igiene e della sicurezza sul lavoro, è tenuto ad osservare le modalità esposte nel presente documento, le previsioni di legge esistenti in materia nonché le norme comportamentali richiamate anche nel Codice Etico.

Le violazioni di procedure o altre disposizioni contenute nei documenti di sicurezza che comportino il pericolo per la sicurezza o salute delle persone sono considerate violazioni disciplinari gravi anche quando il pericolo si determina per la persona cui è addebitabile la violazione e anche se nessun danno alla persona si verifica.

Ogni violazione deve essere tempestivamente segnalata all'OdV.

PARTE “E” REATI AMBIENTALI (art. 25 *undecies* d.lgs. 231/2001)

E.1 Descrizione delle fattispecie normative

Si definiscono reati ambientali tutte le attività che danneggiano l'ambiente, le quali generalmente provocano o possono provocare un deterioramento significativo della qualità dell'aria, compresa la stratosfera, del suolo, dell'acqua, della fauna e della flora, compresa la conservazione delle specie.

L'esigenza di una tutela penale dell'ambiente è avvertita sia a livello comunitario che nazionale. A livello comunitario tale esigenza è stata recepita nella Direttiva del Parlamento europeo e del Consiglio n° 99, del 19 novembre 2008, sulla tutela penale dell'ambiente, secondo la quale ciascuno Stato membro deve adottare le misure necessarie affinché siano perseguibili penalmente una serie di attività «illecite e poste in essere intenzionalmente o quanto meno per grave negligenza».

Il 7 luglio 2011 è stato approvato il Decreto legislativo n. 121 di attuazione delle Direttive comunitarie in tema di reati ambientali, denominato “Attuazione della Direttiva 2008/99/C sulla tutela penale dell'ambiente, nonché della direttiva 2009/123/CE che modifica la direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni”. In particolare, il D.lgs. 121/11 prevede l'introduzione nel D.lgs. 231/2001 del nuovo art. 25 *undecies* che estende la responsabilità dell'ente ai reati ambientali.

Nell'introdurre l'art. 25 *undecies* il legislatore ha operato un rimando solo “parziale” alle norme vigenti in materia di tutela dell'ambiente, selezionando solo specifiche ipotesi di reato ed introducendo ex novo le fattispecie di cui agli articoli 727-bis e 733-bis del Codice penale.

La Legge 22 maggio 2015 n. 68 ha introdotto nuovi delitti ambientali nel Codice penale e, quindi, ampliato anche il novero di quelli contemplati dal D.lgs. 231/01.

Da ultimo, il D. L. 116/2025 (noto come D. L. «Terra dei Fuochi») è intervenuto apportando significative modifiche al D.lgs. 152/2006 (Testo Unico Ambientale – T.U.A.), al Codice penale e al Codice di procedura penale e al Codice antimafia. Elemento centrale della riforma è altresì l'ampliamento della responsabilità degli enti, con effetti diretti sulla compliance aziendale e sui modelli organizzativi che le imprese devono adottare per prevenire il rischio di illeciti ambientali. Il decreto inasprisce sensibilmente il regime sanzionatorio, innalzando le soglie delle sanzioni pecuniarie a livelli molto elevati e ampliando l'elenco dei reati che possono costituire presupposto di responsabilità per le imprese. Tra questi figurano nuove fattispecie penali come l'impedimento del controllo, l'omessa bonifica, l'organizzazione di traffici illeciti di rifiuti e l'abbandono o combustione illegale di rifiuti.

Con riferimento ai criteri di imputazione della responsabilità dell'ente trovano applicazione i seguenti criteri:

- criteri oggettivi di imputazione della responsabilità all'ente, definiti all'art. 5 del d.lgs. 231/01, laddove stabilisce che i reati-presupposto sono riferibili all'ente solo se commessi (da soggetti apicali o da persone a questi sottoposte) nel suo interesse o a suo vantaggio;
- criterio di imputazione soggettiva, per cui l'adozione del Modello di organizzazione, gestione e controllo mantiene una decisiva funzione esimente della responsabilità dell'ente.

Va tuttavia precisato che nel caso dei reati ambientali l'art. 25-*undecies* non riconosce efficacia esimente ai modelli organizzativi di gestione definiti conformemente a standard e Regolamenti internazionali, come è invece avvenuto con l'introduzione della responsabilità dell'ente per i reati commessi in violazione della normativa sulla sicurezza e prevenzione degli infortuni sul lavoro. Inoltre, a differenza della normativa sulla sicurezza, la normativa ambientale non individua preliminarmente l'organizzazione aziendale ma si limita a definire, nell'ambito di normative specifiche, le figure responsabili dell'Ente di fronte alle autorità, ad es. la figura del Titolare dell'autorizzazione agli scarichi idrici o alle emissioni in atmosfera.

Si riporta di seguito una breve descrizione dei reati, tra quelli contemplati nell'art. 25 *undecies* del Decreto, considerati potenzialmente a rischio per la Società.

E.1.1. Inquinamento ambientale (art. 452 *bis* c.p.)

Questo reato si verifica allorché abusivamente si cagioni un inquinamento (deterioramento o compromissione) significativo e misurabile del suolo, delle acque, dell'aria, della flora, della fauna e dell'agricoltura.

La pena prevista è la reclusione da due a sei anni e la multa da 10.000 a 100.000 Euro

Quando il reato è commesso in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie di animali o vegetali protette, la pena viene aumentata da un terzo alla metà.

Nel caso, inoltre, in cui l'inquinamento causi un deterioramento, compromissione o distruzione di un habitat all'interno di un'area naturale protetta o sottoposta a vincoli la pena è aumentata da un terzo a due terzi.

E.1.2 Disastro ambientale (art. 452 *quater* c.p.)

Questo reato si verifica allorché abusivamente vengano cagionati uno dei tre eventi alternativi del disastro:

- alterazione irreversibile dell'equilibrio di un ecosistema;
- alterazione eliminabile solo con provvedimenti eccezionali ed onerosi;
- offesa alla pubblica incolumità per estensione della compromissione o per il numero di persone offese o esposte al pericolo.

Quando il reato è commesso in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette, la pena viene aumentata.

Perché si realizzi un disastro ambientale non basta l'inquinamento ordinario di cui all'art. 452 *bis* c.p., ma l'evento danno o pericoloso deve avere carattere di grave diffusione e prorompente impatto sull'ambiente e sulla salute pubblica e il danneggiamento deve essere irreversibile o eccezionalmente costoso da rimuovere.

E.1.3 Delitti colposi contro l'ambiente (art. 452 *quinquies* c.p.)

Questo reato si verifica quando uno dei fatti contemplati negli articoli precedenti 452- bis c.p. e 452-quater c.p. è commesso per colpa ovvero manca la volontà di determinare un qualsiasi evento costituente reato, ma l'evento si verifica ugualmente per negligenza, imprudenza, imperizia o per inosservanza di leggi, regolamenti, ordini o discipline (art. 43 c.p.).

Le pene previste dai medesimi articoli sono ridotte da un terzo a due terzi e diminuite ulteriormente di un terzo se c'è solo il pericolo di inquinamento o disastro ambientale.

E.1.4 Traffico e abbandono di materiale ad alta radioattività (art. 452 *sexies* c.p.)

Questo reato si verifica quando chiunque abusivamente cede, acquista, riceve, trasporta, importa, esporta, procura ad altri, detiene, trasferisce, abbandona o si disfa illegittimamente di materiale ad alta radioattività.

La pena è aumentata se dal fatto deriva il pericolo di compromissione o deterioramento del suolo, delle acque, dell'aria, di un ecosistema, dell'agricoltura, della flora e della fauna

Se dal fatto deriva poi pericolo per la vita o per l'incolumità delle persone, la pena è aumentata fino alla metà.

E.1.5 Impedimento del controllo (art. 452 *septies* c.p.)

Questo reato sanziona *“chiunque, negando l'accesso, predisponendo ostacoli o mutando artificiosamente lo stato dei luoghi, impedisce, intralcia o elude l'attività di vigilanza e controllo ambientali e di sicurezza e igiene del lavoro, ovvero ne compromette gli esiti”*.

Tale previsione tutela l'esercizio delle funzioni di vigilanza ambientale e di sicurezza sul lavoro, colpendo le condotte che ne ostacolano il regolare svolgimento.

E.1.6 Circostanze aggravanti (art. 452 *octies* c.p.)

L'art. 452 *octies* viene applicato quando a commettere i reati ambientali in oggetto, sia una associazione di tre o più persone; le pene previste dall'art 416 c.p. (associazione per delinquere) sono aumentate.

Quando il fine è l'acquisizione, la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, di appalti o di servizi pubblici in materia ambientale le pene previste dal medesimo articolo 416-bis c.p. (associazione di tipo mafioso) sono aumentate.

Le pene di cui al primo e secondo punto sono aumentate da un terzo alla metà se dell'associazione fanno parte pubblici ufficiali o incaricati di un pubblico servizio che esercitano funzioni o svolgono materia ambientale.

E.1.7 Omessa bonifica (art. 452 *terdecies* c.p.)

L'art. 452 *terdecies* punisce l'omessa bonifica, ovvero la mancata esecuzione di interventi obbligatori per disposizione di legge o per ordine di un'autorità pubblica o giudiziaria, volti a bonificare, ripristinare o recuperare lo stato dei luoghi.

E.1.8 Attività organizzate per il traffico illecito di rifiuti (art. 452 *quaterdecies* c.p.)

La norma punisce 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.

La pena è aumentata se si tratta di rifiuti ad alta radioattività.

Il giudice, con la sentenza di condanna o con quella emessa ai sensi dell'articolo 444 del codice di procedura penale, ordina il ripristino dello stato dell'ambiente e può subordinare la concessione della sospensione condizionale della pena all'eliminazione del danno o del pericolo per l'ambiente.

È sempre ordinata la confisca delle cose che servirono a commettere il reato o che costituiscono il prodotto o il profitto del reato, salvo che appartengano a persone estranee al reato.

Quando essa non sia possibile, il giudice individua beni di valore equivalente di cui il condannato abbia anche indirettamente o per interposta persona la disponibilità e ne ordina la confisca.

E.1.9 Uccisione, distruzione, cattura, prelievo, detenzione e commercio di esemplari di specie animali o vegetali selvatiche protette (art. 727 *bis* c.p.)

Questo reato sanziona chi, fuori dai casi previsti dalla legge, uccide, cattura, detiene o commercia esemplari di specie selvatiche protette, animali o vegetali.

Il reato richiede la lesione di esemplari protetti, la cui elencazione viene disposta da parte di Direttive dell'UE.

La *deminutio* per "quantità e impatto trascurabili" esclude la punibilità solo se entrambe le condizioni sussistono cumulativamente.

E.1.10 Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733 *bis* c.p.)

La norma punisce la condotta di chiunque, fuori dai casi consentiti, distrugge un habitat all'interno di un sito protetto o comunque lo deteriora compromettendone lo stato di conservazione.

La fattispecie sanzionata consiste nella distruzione di un habitat all'interno di un sito protetto ovvero al suo deterioramento che ne comprometta lo stato di conservazione ed è ipotizzabile che si verifichi in azienda.

In caso di violazioni costituenti ipotesi di reati perseguiti ai sensi del titolo VIII *bis* del libro secondo (aggiunto dalla Legge n. 22/2022 "Disposizioni in materia di reati contro il patrimonio culturale") o dell'articolo 733 *bis* del codice penale, il sequestro di quanto adoperato per commettere gli illeciti ad essi relativi può essere disposto, in caso di flagranza, anche dagli addetti alla sorveglianza dell'area protetta, al fine di evitare l'aggravamento o la continuazione del reato.

Il responsabile è obbligato a provvedere alla riduzione in pristino dell'area danneggiata, ove possibile, e comunque è tenuto al risarcimento del danno.

E.1.11 Norme previste dal Testo Unico Ambientale (d.lgs. n. 152/2006)

Inquinamento idrico (art. 137)

- a) Scarico non autorizzato di acque reflue industriali (comma 1):
Fuori dai casi sanzionati ai sensi dell'art. 29 *quattordices*, comma 1, chiunque apra o comunque effettui nuovi scarichi di acque reflue industriali, senza autorizzazione, oppure continui ad effettuare o mantenere detti scarichi dopo che l'autorizzazione sia stata sospesa o revocata, è punito con l'arresto da due mesi a due anni o con l'ammenda da millecinquecento euro a diecimila euro.
- b) Scarico non autorizzato di acque reflue industriali contenenti sostanze pericolose (comma 2):
Quando le condotte di scarico non autorizzato di acque reflue industriali contengono le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del presente decreto, la pena è aumentata (comma 2).
- c) Scarico di acque reflue industriali contenenti sostanze pericolose in violazione delle prescrizioni imposte con l'autorizzazione o da autorità competenti (comma 3):
La norma punisce chiunque, al di fuori delle ipotesi di cui al comma 5, effettui uno scarico di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del presente decreto senza osservare le prescrizioni dell'autorizzazione, o le altre prescrizioni dell'autorità competente a norma delle disposizioni inerenti gli scarichi in reti fognarie (art. 107, comma 1) e gli scarichi di sostanze pericolose (art. 108, comma 4).
- d) Scarico di acque reflue industriali contenenti sostanze pericolose in violazione dei limiti tabellari o dei limiti più restrittivi fissati da Regioni o dall'Autorità competente (comma 5):
È punito chiunque, in relazione alle sostanze indicate nella tabella 5 dell'Allegato 5 alla parte terza del presente decreto, nell'effettuazione di uno scarico di acque reflue industriali, superi i valori limite fissati nella tabella 3 o, nel caso di scarico sul suolo, nella tabella 4 dell'Allegato 5 alla parte terza del presente

decreto, oppure i limiti più restrittivi fissati dalle Regioni o dalle Province autonome o dall'Autorità competente a norma dell'articolo 107, comma 1.

Se sono superati anche i valori limite fissati per le sostanze contenute nella tabella 3/A del medesimo Allegato 5, si applica [...]”.

e) Scarico sul suolo, nel sottosuolo o nelle acque sotterranee (comma 11):

Chiunque non osservi i divieti di scarico previsti dalla normativa inerente agli scarichi sul suolo (art. 103) e agli scarichi nel sottosuolo e nelle acque sotterranee (art. 104) è punito con l'arresto sino a tre anni.

Abbandono di rifiuti pericolosi e di rifiuti non pericolosi con rischi per l'ambiente o la salute (art. 255 bis e 255 ter):

a) Abbandono di rifiuti non pericolosi in casi particolari (art. 255 bis):

È punito chiunque, in violazione delle disposizioni sulla gestione dei rifiuti (art. 192, comma 1 e 2), degli imballaggi (art. 226, comma 2) e di particolari categorie di rifiuti come i veicoli fuori uso (art. 231, comma 1 e 2) abbandona o deposita rifiuti non pericolosi ovvero li immette nelle acque superficiali o sotterranee.

La pena è aumentata se:

- a) dal fatto deriva pericolo per la vita o l'incolumità delle persone ovvero pericolo di compromissione o deterioramento dell'ambiente naturale;
- b) il fatto è commesso in siti contaminati o potenzialmente contaminati o comunque sulle strade di accesso ai predetti siti e relative pertinenze

b) Abbandono di rifiuti pericolosi

È punito chiunque, in violazione delle medesime disposizioni per i rifiuti non pericolosi, abbandona o deposita rifiuti pericolosi ovvero li immette nelle acque superficiali o sotterranee.

La pena è aumentata se:

- a) dal fatto deriva pericolo per la vita o l'incolumità delle persone ovvero pericolo di compromissione o deterioramento dell'ambiente naturale;
- b) il fatto è commesso in siti contaminati o potenzialmente contaminati o comunque sulle strade di accesso ai predetti siti e relative pertinenze

Attività di gestione non autorizzata di rifiuti (art. 256) e combustione illecita di rifiuti (art. 256 bis)

a) Attività di gestione rifiuti non autorizzata (art. 256, comma 1):

Fuori dai casi sanzionati ai sensi dell'art. 29 *quattordices*, comma 1, è punito chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212, 214, 215 e 216 D. lgs. 152/2006.

La pena è aumentata quando:

- c) dal fatto deriva pericolo per la vita o l'incolumità delle persone ovvero pericolo di compromissione o deterioramento dell'ambiente naturale;
- d) il fatto è commesso in siti contaminati o potenzialmente contaminati o comunque sulle strade di accesso ai predetti siti e relative pertinenze

b) Realizzazione o gestione di una discarica non autorizzata (art. 256, comma 3):

Viene punita la condotta di chi realizza o gestisce una discarica non autorizzata e se la discarica è destinata, anche in parte, allo smaltimento di rifiuti pericolosi la pena è aumentata.

Il trattamento sanzionatorio si aggrava, ulteriormente, se:

- dal fatto deriva pericolo per la vita o l'incolumità delle persone ovvero pericolo di compromissione o deterioramento dell'ambiente naturale (acque, aria, porzioni estese o significative del suolo/sottosuolo, ecosistema, biodiversità, flora, fauna);
- il fatto è commesso in siti contaminati o potenzialmente contaminati o comunque sulle strade di accesso ai predetti siti e relative pertinenze.

Alla sentenza di condanna o alla sentenza emessa ai sensi dell'articolo 444 del codice di procedura penale, consegue la confisca dell'area sulla quale è realizzata la discarica abusiva se di proprietà dell'autore o del compartecipe al reato, fatti salvi gli obblighi di bonifica o di ripristino dello stato dei luoghi.

c) Attività non consentite di miscelazione di rifiuti (art. 256, comma 5):

È punito chiunque, in violazione del divieto di cui all'articolo 187, effettua attività non consentite di miscelazione di rifiuti.

d) Deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi (art. 256, comma 6, primo periodo):

E' punito chiunque effettua 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).

e) Combustione illecita di rifiuti (art. 256 *bis*, comma 1 e 3 *bis*):

È punito chiunque appicca il fuoco a rifiuti abbandonati ovvero depositati in maniera incontrollata. Nel caso in cui sia appiccato il fuoco a rifiuti pericolosi, la pena è aumentata. Il responsabile è tenuto al ripristino dello stato dei luoghi, al risarcimento del danno ambientale ed al pagamento, anche in via di regresso, delle spese per la bonifica.

La pena è aumentata inoltre quando dalla combustione di rifiuti non pericolosi:

- a) dal fatto deriva pericolo per la vita o l'incolumità delle persone ovvero pericolo di compromissione o deterioramento dell'ambiente naturale (acque, aria, porzioni estese o significative del suolo/sottosuolo, ecosistema, biodiversità, flora, fauna);
- b) il fatto è commesso in siti contaminati o potenzialmente contaminati o comunque sulle strade di accesso ai predetti siti e relative pertinenze.

Bonifica dei siti (art. 257, comma 1 e 2):

L'articolo 257, Codice dell'Ambiente, obbliga chi cagiona un inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee, determinando il superamento delle concentrazioni soglia di rischio (CSR), a procedere alla bonifica dei siti inquinati in conformità al progetto approvato secondo il procedimento previsto dall'articolo 242 del Codice dell'Ambiente.

La pena è aumentata se l'inquinamento è provocato da "sostanze pericolose".

Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258, comma 4, secondo periodo):

La norma sanziona la condotta di chi effettua il trasporto di rifiuti pericolosi senza il formulario di identificazione (FIR) di cui all'art. 193 o senza i documenti sostitutivi ivi previsti.

Spedizione illegale di rifiuti (art. 259, comma 1):

È punito chiunque effettua una spedizione di rifiuti costituente traffico illecito ai sensi dell'art. 2, punto 35 del regolamento CE n. 1013/2006 del Parlamento europeo e del Consiglio, del 14 giugno 2006 (abrogato) e dell'art. 3, punto 26 del regolamento UE 2024/1157 del Parlamento europeo e del Consiglio dell'11 aprile 2024, il quale definisce «spedizione illegale» la spedizione effettuata:

- “a) senza notifica alle autorità competenti interessate a norma del presente regolamento;*
- b) senza l'autorizzazione delle autorità competenti interessate a norma del presente regolamento;*
- c) con l'autorizzazione delle autorità competenti interessate ottenuta ai sensi del presente regolamento mediante falsificazioni, false dichiarazioni o frodi;*
- d) in un modo non conforme alle informazioni contenute nel documento di notifica o contenute nel documento di movimento o da fornire nel medesimo, fatta eccezione per gli errori materiali di minore entità nel documento di notifica o nel documento di movimento;*
- e) in un modo che il recupero o lo smaltimento risulti in contrasto con il diritto dell'Unione o internazionale;*
- f) in contrasto con l'articolo 4, paragrafi 1 e 3, o con gli articoli 37, 39, 40, 45, 46, 48, 49, 50 o 52;*
- g) in un modo che, in relazione alle spedizioni di rifiuti di cui all'articolo 4, paragrafi 4 e 5, non è conforme agli obblighi di cui all'articolo 18, paragrafi 2, 4, 6 e 10, o alle informazioni contenute o da fornire nel documento di cui all'allegato VII, fatta eccezione per gli errori materiali di minore entità nel documento di cui all'allegato VII”.*

Delitti colposi in materia di rifiuti (art. 259 ter):

La norma viola la condotta di taluno che commette per colpa i fatti di cui agli artt. 255 *bis* (abbandono di rifiuti non pericolosi in casi particolari), 255 *ter* (abbandono di rifiuti pericolosi), 256 (attività di gestione di rifiuti non autorizzata) e 259 (spedizione illegale di rifiuti).

Sistema informativo di controllo della tracciabilità dei rifiuti (art. 260 *bis*, commi 6,7, secondo e terzo periodo e 8):

- a) È punito colui che, nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi inserisce un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti.
- b) È punito colui che, durante il trasporto anche di rifiuti pericolosi fa uso di un certificato di analisi di rifiuti contenente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati.
- c) È punito il trasportatore che accompagna il trasporto di rifiuti con una copia cartacea della scheda SISTRI – AREA Movimentazione fraudolentemente alterata. La pena è aumentata nel caso di rifiuti pericolosi.

Inquinamento atmosferico (art. 279, comma 5):

Viene sanzionata la condotta di chi, nell'esercizio di uno stabilimento, viola i valori limiti di emissione stabiliti dalla normativa vigente.

E.1.12 Cessazione e riduzione dell'impiego delle sostanze lesive (art. 3, comma 6, L. n. 549/1993)

In particolare, i comportamenti disciplinati dall'articolo 3 della Legge n. 549/1993 hanno ad oggetto una serie di condotte che trovano la loro disciplina (ed il regime delle eventuali esenzioni o deroghe applicabili) nel Regolamento (CE) n. 1005/2010, in tema di:

- Produzione, consumo, importazione, esportazione, detenzione e commercializzazione di sostanze lesive di cui alla Tabella A alla Legge n. 549/1993.
- Autorizzazione di impianti che prevedano l'utilizzazione delle sostanze lesive di cui alla Tabella A alla Legge n. 549/1993.
- Utilizzazione delle sostanze di cui alla Tabella A alla Legge n. 549/1993 per la manutenzione di apparecchi ed impianti già venduti ed installati, nonché tempi e modalità per la cessazione dell'utilizzazione delle sostanze di cui alla Tabella B alla Legge n. 549/1993.

È punito con sanzione penale chiunque viola le disposizioni dell'art. 3 sopra indicato. Nei casi più gravi, alla condanna consegue la revoca dell'autorizzazione o della licenza in base alla quale viene svolta l'attività costituente illecito.

E.2 Attività sensibili

ATTIVITA' SENSIBILI	FASI	FUNZIONI INTERESSATE
Gestione degli aspetti tecnico-amministrativi		
Pianificazione	Identificazione e valutazione degli aspetti ambientali	Datore di lavoro Delegato ambiente Consulente incaricato
	Individuazione prescrizioni di legge e regolamentari	
	Definizione obiettivi programmi miglioramento prevenzione e protezione ambientale	
Attuazione	Identificazione ruoli e funzioni rilevanti ex D.lgs. n. 152/2006	Datore di lavoro Delegato ambiente Consulente incaricato
	Formazione / Informazione adeguate	
	Individuazione e gestione potenziali emergenze ambientali	
Verifica	Monitoraggio e sorveglianza operazioni con impatto ambientale / Raggiungimento obiettivi prefissati	Datore di lavoro Delegato ambiente Consulente incaricato
	Periodica e sistematica rispetto prescrizioni di legge / regolamentari / piano ambientale	
Affidamento lavori, servizi e forniture ad imprese appaltatrici o lavoratori autonomi	Verifica idoneità tecnico-professionale del fornitore	Datore di lavoro Delegato ambiente Resp. Amm. Consulente incaricato
	Acquisizione documentazione certificazioni, autocertificazioni richieste dalla legge	
	Informazioni adeguate	

	Vigilanza operatività fornitori	
	Tracciabilità monitoraggio prestazioni fornitori	

Aree a rischio

Le attività a rischio individuate, in riferimento ai reati ambientali ritenuti applicabili, coinvolgono particolarmente le attività nei cantieri esterni e sono le seguenti:

1. gestione degli aspetti tecnici amministrativi legati all'esitazione e smaltimento rifiuti (campionamenti, caratterizzazione);
2. vigilanza su eventuali appaltatori, sub – appaltatori, terzi che operano all'interno delle aree di lavoro di Unirock;
3. gestione dei processi che comportano impatti ambientali (es. emissioni, reflui, inquinamento suolo);
4. gestione del presidio normativo, dei provvedimenti autorizzativi (comunicazioni alle autorità competenti; richieste, modifiche, integrazioni, cessazioni, di provvedimenti autorizzativi; attuazione piani di monitoraggio, ecc)) e delle verifiche periodiche in merito alla conformità normativa.

E.3 Sistema di controllo

E.3.1 Principi generali di comportamento

Unirock S.r.l. pone la massima attenzione nello sviluppare e tenere sotto controllo gli impatti ambientali delle proprie attività ricercandone sistematicamente il miglioramento.

I requisiti cui si ispira la Società riguardano:

- per la fase di pianificazione, le attività relative a:
 - identificazione e valutazione degli aspetti ambientali;
 - individuazione delle Prescrizioni ex lege e delle altre prescrizioni applicabili;
 - definizione di politiche ambientali, di obiettivi con riferimento agli aspetti ambientali e di programmi di miglioramento, di prevenzione e protezione ambientale;
- per la fase di attuazione, le attività relative a:
 - definizione di «risorse, ruoli, responsabilità ed autorità»
 - formazione/informazione, ovvero quelle attività volte a fare sì che la «competenza, formazione e consapevolezza» delle persone (sia di quelle che lavorano per l'organizzazione sia di quelle che lavorano per conto di essa) le cui attività hanno impatti ambientali, siano sempre adeguate alle esigenze e congrue rispetto al perseguimento della politica ambientale;
 - l'individuazione e la gestione delle potenziali emergenze ambientali.
- per la fase di verifica, le attività relative a:
 - monitoraggio, sorveglianza e misurazione (i) delle operazioni che possono avere impatti ambientali significativi, (ii) del raggiungimento degli obiettivi prefissati e (iii) della corretta taratura della strumentazione di monitoraggio ambientale;
 - verifica periodica e sistematica del rispetto delle prescrizioni previste dalla legge e delle altre eventuali prescrizioni (es. procedure ed istruzioni operative aziendali) sottoscritte dall'organizzazione.

E.3.2 Regole specifiche di comportamento

La presente Parte Speciale prevede l'espresso divieto – a carico degli Esponenti Aziendali, in via diretta, ed a carico dei Collaboratori esterni e Partner, di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che considerati individualmente o collettivamente:

- integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-*undecies* del D.lgs. 231/2001);
- possano compromettere i presidi di tutela ambientale adottati dalla Società favorendo potenzialmente la commissione dei reati ambientali di cui all'art. 25-*undecies* del D. Lgs. 231/2001;

- di tenere comportamenti in violazione alle procedure aziendali o, comunque, non in linea con i principi espressi dal presente Modello e del Codice Etico.

È fatto, inoltre, obbligo di:

- osservare tutti i dettami previsti dal D.lgs. 152/06 e s.m.i. o da altre leggi e regolamenti che tutelano l'ambiente;
- osservare i protocolli e le procedure che disciplinano l'attività aziendale.

In tema di deleghe di responsabilità e nomine/designazioni delle funzioni rilevanti per la tutela dell'ambiente viene garantito che:

- le deleghe in materia ambientale, che coincidono con le deleghe in materia di salute e sicurezza sul lavoro, siano adeguatamente formalizzate, con la specifica indicazione dei poteri delegati, la firma da parte dei soggetti incaricati, e pubblicizzate;
- il delegato possenga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;
- il sistema delle deleghe, nomine e designazioni sia coerente con l'evoluzione dell'organizzazione societaria;
- le Funzioni incaricate di compiti rilevanti per la tutela ambientale siano dotate dei poteri di organizzazione, gestione e controllo, ed eventualmente di spesa, adeguati alla struttura e alla dimensione dell'organizzazione e alla natura dei compiti assegnati in considerazione anche della possibilità del verificarsi di casi di urgenze non prevedibili né rinviabili.

I Destinatari della presente sezione devono esercitare un controllo continuo e puntuale teso ad evidenziare i rischi che potrebbero comportare la realizzazione dei reati indicati nell'art. 25-*undecies* ed in generale qualunque situazione che possa comportare un pericolo per la tutela ambientale.

I principi di controllo specifici definiti per disciplinare le attività di gestione dei rifiuti prodotti dall'organizzazione affinché le stesse siano svolte in conformità ai requisiti normativi e autorizzativi vigenti prevedono la definizione di ruoli, responsabilità e modalità operative contenute principalmente nei documenti di sicurezza del cantiere, per garantire:

- il rispetto di tutti gli adempimenti previsti dalla normativa in capo al produttore del rifiuto;
- il rispetto dei termini temporali per le annotazioni sul registro di carico e scarico dei rifiuti;
- il rispetto del divieto di combustione dei rifiuti;
- l'adeguatezza delle aree di deposito, anche con riferimento a particolari tipologie di rifiuti speciali (es. oli esausti), ed il rispetto dei requisiti previsti per il deposito temporaneo (limiti quantitativi, qualitativi e temporali);

- l'identificazione dei rifiuti e l'attribuzione del codice CER e delle eventuali caratteristiche di pericolosità;
- il ricorso, ove necessario, ad analisi di caratterizzazione dei rifiuti effettuate da laboratori qualificati previa individuazione della frequenza di caratterizzazione, delle modalità di campionamento e di adeguati flussi informativi verso i laboratori di analisi in merito alla provenienza e composizione dei campioni da analizzare;
- la vigilanza sulla correttezza/esaustività delle informazioni contenute nei certificati di analisi sui rifiuti forniti dai laboratori terzi;
- il rispetto del divieto di miscelazione dei rifiuti pericolosi con i rifiuti non pericolosi e di rifiuti pericolosi che abbiano caratteristiche di pericolosità differenti;
- la qualifica iniziale e la verifica periodica del possesso e della validità delle iscrizioni/comunicazioni/autorizzazioni previste dalla normativa per la gestione dei rifiuti da parte dei soggetti terzi a cui vengono conferiti i rifiuti prodotti (inclusa la permanenza della validità delle fidejussioni prestate, ove previste, ed eventuali altre prescrizioni contenute nelle specifiche autorizzazioni);
- la verifica della correttezza e completezza della documentazione di trasporto (formulari di identificazione dei rifiuti), inclusa la verifica delle targhe dei mezzi utilizzati ed il possesso dei requisiti previsti dalla normativa ADR, ove applicabile (cartellonistica, equipaggiamenti, documenti di trasporto);
- la verifica del rientro della IV° copia del formulario entro i tempi previsti dalla normativa applicabile e l'adozione dei provvedimenti di legge in caso di mancato rientro;
- la tracciabilità di tutte le attività relative alla gestione dei rifiuti.

La nozione di produttore di rifiuto sopra richiamata è quella indicata alla lett. f) dell'art.183 del decreto legislativo 3 aprile 2006, n. 152 modificato dalla legge 6 agosto 2015, n.125 che individua come produttore non solo il soggetto la cui attività produce rifiuti o chiunque effettui operazioni di pretrattamento, di miscelazione o altre operazioni che hanno modificato la natura o la composizione di detti rifiuti ma anche "il soggetto al quale sia giuridicamente riferibile detta produzione".

I principi di controllo specifici definiti per prevenire la contaminazione del suolo, sottosuolo, acque superficiali e sotterranee prevedono la definizione di ruoli, responsabilità e modalità operative per garantire:

- un adeguato e tempestivo intervento in caso di eventi accidentali che possano comportare fenomeni di inquinamento del suolo e/o sottosuolo;
- la comunicazione ex art. 242 del D.lgs. 152/06 e s.m.i. al verificarsi di un evento che sia potenzialmente in grado di contaminare il sito;
- ove necessario, la bonifica dei siti inquinati in conformità a progetti approvati dall'Autorità competente nell'ambito del procedimento di cui agli articoli 242 e seguenti del D.lgs. 152/06 e s.m.i..

Con riferimento ai reati di inquinamento ambientale, disastro ambientale e delitti colposi contro l'ambiente ai sensi degli artt. 452 *bis*, 452 *quater* e 452 *quinqüies* c.p., nonché ai reati di carattere associativo che determinano "circostanze aggravanti" ai sensi dell'art. 452 *octies* del c.p., si pone in rilievo come i relativi rischi appaiano già presidiati dai principi di controllo specifici sopra definiti, dalle regole previste nelle procedure, nel Codice Etico e nelle altre Parti del Modello cui si rimanda.

Oltre a quanto sopra è prevista la definizione di ruoli, responsabilità e modalità operative volte a pianificare ed attuare verifiche di conformità normativa periodiche e sistematiche comprensive degli aspetti previsti nel titolo VI *bis* del Codice penale.

Poiché, inoltre, nell'ambito delle aree a rischio assumono rilevanza i comportamenti di terzi cui l'organizzazione può affidare lo svolgimento di parte delle attività, i principi di controllo specifici prevedono l'esistenza di una normativa aziendale che disciplini le attività di selezione dei fornitori, successivo affidamento dei contratti e monitoraggio delle prestazioni, tesa a garantire che i fornitori a cui vengono affidate attività rilevanti da un punto di vista ambientale siano idonei da un punto di vista tecnico, professionale e autorizzativo e siano vincolati contrattualmente al rispetto delle norme ambientali vigenti e ai requisiti specifici stabiliti dall'organizzazione. L'obiettivo è inoltre quello di garantire che le attività siano svolte in conformità a quanto previsto dalle norme ambientali vigenti e dai requisiti specifici stabiliti dall'organizzazione. In particolare, tale normativa aziendale definisce ruoli, responsabilità e modalità operative per garantire:

- la definizione delle informazioni che devono essere date ai fornitori riguardo le norme e prescrizioni da rispettarsi nell'ambito dello svolgimento della loro attività per conto della Società;
- la vigilanza sull'operatività dei fornitori anche con particolare riferimento alla combustione illecita dei rifiuti;
- la segnalazione di scostamenti rispetto a quanto previsto dalle norme ambientali vigenti e ai requisiti specifici stabiliti dall'organizzazione e la definizione di azioni correttive atte a evitare il ripetersi degli scostamenti individuati;
- la tracciabilità di tutte le attività relative al processo di selezione e affidamento a terzi di attività rilevanti da un punto di vista ambientale e di tutte le attività relative al processo di monitoraggio delle prestazioni dei fornitori.

Il personale della società, a qualsiasi titolo coinvolto in attività che comportino impatti ambientali, è tenuto ad osservare le modalità esposte nel presente documento, le previsioni di legge esistenti in materia.

Dal punto di vista documentale, per le attività che ricadono sotto l'applicazione del Titolo IV del Dlgs 81/08 s.m.i. il Piano Operativo di Sicurezza (POS) contiene anche una parte dedicata nello specifico alla tutela ambientale con riferimento alle attività svolte da Unirock all'interno del cantiere di riferimento.

Il personale della società, a qualsiasi titolo coinvolto nelle attività di gestione degli aspetti in materia di tutela ambientale, è tenuto ad osservare le modalità esposte nel presente documento, le previsioni di legge esistenti in materia nonché le norme comportamentali richiamate anche nel Codice Etico.

Le violazioni di procedure o altre disposizioni contenute nel Modello Organizzativo sono considerate violazioni disciplinari.

Ogni violazione deve essere tempestivamente segnalata all'OdV.

PARTE SPECIALE “F” DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI **(art. 24 *bis* d.lgs. 231/2001)**

F.1 Descrizione delle fattispecie normative

La legge 18 marzo 2008 n. 48 ha ratificato la Convenzione di Budapest del 23 novembre 2001, promossa dal Consiglio d'Europa in tema di criminalità informatica e riguardante i reati commessi avvalendosi in qualsiasi modo di un sistema informatico o in suo danno.

L'art. 24 *bis* del d.lgs. 231/2001 contempla la responsabilità degli enti con riguardo alle categorie di reati informatici e di trattamento illecito di dati.

Inoltre, il D. L. 105 del 21 settembre 2019, convertito in L. 18 novembre 2019, n. 133 ha istituito il c.d. “*perimetro di sicurezza nazionale cibernetica*”, volto ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle Amministrazioni Pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale (art. 1, comma 1, del D. L. sopra citato). In ragione di quanto sopra è stato introdotto nel Codice penale il nuovo reato presupposto di cui all'art. 640 *quinqüies* c.p. (*Frode informatica del certificatore di firma elettronica*), che però non risulta rilevante ai fini della presente Parte Speciale in quanto Unirock S.r.l. non rientra nel perimetro di sicurezza cibernetica di cui alla normativa in esame.

L'art. 19 della Legge n. 238 del 23 dicembre 2021, avente ad oggetto “*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea - Legge Europea 2019-2020*” ha comportato modifiche al Codice penale che hanno interessato anche i delitti informatici ricompresi nell'art. 24 *bis* del d.lgs. n. 231/01.

Infine, ulteriori modifiche all'art. 24 *bis* del Decreto sono state introdotte dalla legge 90/2024 recante “*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*”: Con tale intervento il Legislatore inasprisce la sanzione pecuniaria applicata all'ente che commette i delitti di cui agli artt. 615 *ter*, 617 *quater*, 617 *quinqüies*, 635 *bis*, 635 *ter*, 635 *quater* e 635 *quinqüies* del codice penale, e introduce quale nuovo reato presupposto, il delitto di estorsione, di cui all'art. 629 terzo comma del codice penale, commesso mediante le condotte di cui agli articoli 615 *ter*, 617 *quater*, 617 *sexies*, 635 *bis*, 635 *quater* e 635 *quinqüies*.

Prima di passare all'analisi delle singole fattispecie criminose è opportuno fornire alcune definizioni come sono state acquisite nella giurisprudenza.

L'espressione «sistema informatico» esprime il concetto di una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche. Queste ultime, come si è rilevato in dottrina, sono caratterizzate dalla registrazione (o “memorizzazione”), per mezzo di impulsi elettronici, su supporti adeguati, di “dati”, cioè di rappresentazione elementari di un fatto, effettuate attraverso simboli numerici (“codice”) in combinazioni diverse; tali “dati”, elaborati automaticamente dalla macchina, generano le “informazioni” costituite “da un insieme più o meno vasto di dati organizzati secondo una logica che consente loro di attribuire un particolare significato per l'utente”.

Con l'espressione «sistema telematico» le disposizioni sui crimini informatici rinviano invece ad un insieme combinato di apparecchiature idoneo alla trasmissione a distanza di dati e di informazioni, attraverso l'impiego di tecnologie dedicate alle telecomunicazioni.

La qualifica di operatore del sistema, che può essere rivestita tanto da una persona fisica quanto da una impresa, nella pratica si attribuisce a chiunque può usufruire delle prestazioni e delle risorse di un elaboratore elettronico. Ad esempio:

- il soggetto preposto alle operazioni di «input» e di «output», di avviamento o di arresto dell'elaboratore elettronico;
- il programmatore che scrive, con appositi linguaggi, le istruzioni e le operazioni che il computer è chiamato ad effettuare;
- il sistemista, che studia le possibili evoluzioni di un sistema per ottimizzarlo ed implementarlo;
- l'analista che sviluppa gli algoritmi per soddisfare specifiche esigenze tecniche;
- il singolo utente dei sistemi informatici.

F.1.1 Accesso abusivo a un sistema informatico o telematico (art. 615 *ter* c.p.)

Tale reato si realizza quando un soggetto "*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 diritto ad escluderlo*". Si considera misura di sicurezza anche la protezione del sistema rappresentata da una semplice chiave di accesso (password).

Le pene sono aumentate:

- 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
- Se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato
- 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 il delitto in oggetto riguardi 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

Il delitto di accesso abusivo al sistema informatico rientra tra i delitti contro la libertà individuale. Il bene che viene protetto dalla norma è il domicilio informatico seppur vi sia chi sostiene che il bene tutelato è, invece,

l'integrità dei dati e dei programmi contenuti nel sistema informatico. L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato

Il delitto di accesso abusivo a sistema informatico si integra, ad esempio, nel caso in cui un soggetto accede abusivamente ad un sistema informatico e procede alla stampa di un documento contenuto nell'archivio del PC altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura)

Il delitto potrebbe essere astrattamente commesso da parte di qualunque dipendente della società accedendo abusivamente ai sistemi informatici di proprietà di terzi (outsider hacking), ad esempio, per prendere cognizione di dati riservati di un'impresa concorrente, ovvero tramite la manipolazione di dati presenti sui propri sistemi come risultato dei processi di business allo scopo di produrre un bilancio falso o, infine, mediante l'accesso abusivo a sistemi aziendali protetti da misure di sicurezza, da parte di utenti dei sistemi stessi, per attivare servizi non richiesti dalla clientela.

È prevista un'aggravante speciale, comune anche ad altre fattispecie di crimini informatici, nel caso in cui il reato sia commesso con abuso della qualità di operatore del sistema.

F.1.2 Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 *quater*)

Questo reato punisce le condotte prodromiche all'accesso abusivo ad un sistema informatico o telematico.

La norma sanziona “*chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, 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*”.

La fattispecie svolge, dunque, una funzione “anticipatoria” rispetto all'accesso abusivo ex art. 615 *ter* c.p., costituendone un possibile antefatto naturalistico, tanto che in talune ipotesi gli interpreti ravvisano un assorbimento nel più grave accesso abusivo contestato nello stesso contesto spazio-temporale.

F.1.3 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* c.p.)

Tale reato si integra qualora un soggetto “*fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe*”, nonché nel caso in cui un soggetto riveli,

parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione al pubblico.

La pena base è aumentata se il fatto è commesso:

- 1) in danno di un sistema informatico o telematico di interesse militare o relativo all'ordine pubblico o alla sicurezza o alla sanità o alla protezione civile o comunque di interesse pubblico;
- 2) in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o 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 un investigatore privato, o con abuso della qualità di operatore del sistema.

Per «comunicazioni informatiche o telematiche» si intendono le trasmissioni di dati, suoni, immagini, simboli, programmi ed ogni altra informazione trasportata attraverso sistemi di elaborazione automatizzati.

“Per intercettazione” deve intendersi l'effettiva cognizione del contenuto dell'altrui comunicazione, non importa se sia stata registrata o meno, mentre non è tale la verifica della durata della comunicazione, o la registrazione dei numeri chiamati, a fine di documentazione, controllo e contabilizzazione del traffico telefonico.

L'intercettazione deve essere fraudolenta e, pertanto, deve essere attuata con l'impiego di mezzi ingannevoli o idonei a aggirare il sistema o il gestore.

Oltre all'intercettazione fraudolenta sono sanzionati «l'impedimento» e «l'interruzione» delle comunicazioni che si verificano quando l'agente, con qualunque accorgimento tecnico, utilizzi o inserisca ostacoli fisici o programmi in grado di inibire, arrestare o rendere difficoltoso il normale esercizio del servizio.

Il secondo comma punisce anche chi divulga il contenuto delle comunicazioni fraudolentemente intercettate. Per l'integrazione del reato è necessario che la rivelazione sia rivolta ad un numero indeterminato di persone e che avvenga con un mezzo di informazione al pubblico; non è, pertanto, punibile la condotta di chi riveli il contenuto delle comunicazioni ad un individuo specifico.

F.1.4 Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi e intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinques* c.p.)

Il reato si realizza quando qualcuno, *"fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi"*.

La condotta vietata dall'art. 617 *quinques* è, pertanto, costituita non solo dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, ma anche se le si detiene solamente o vengono diffuse. Si tratta di un reato che mira a prevenire quello precedente di intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche

Anche la semplice installazione di apparecchiature idonee all'intercettazione viene punita dato che tale condotta rende probabile la commissione del reato di intercettazione. Ai fini della condanna il giudice dovrà, però, limitarsi ad accertare se l'apparecchiatura installata abbia, obiettivamente, una potenzialità lesiva.

Qualora all'installazione faccia seguito anche l'utilizzo delle apparecchiature per l'intercettazione, interruzione, impedimento o rivelazione delle comunicazioni, si applicheranno nei confronti del soggetto agente, qualora ricorrano i presupposti, più fattispecie criminose.

F.1.5 Danneggiamento

Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)

Tale fattispecie reato si realizza quando un soggetto *"distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui"*.

Secondo il D.lgs. n. 7 del 15 gennaio 2016 la pena base è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di pubblico ufficiale/incaricato di pubblico servizio o di operatore del sistema.

Il reato, ad esempio, si integra nel caso in cui il soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.

Il danneggiamento potrebbe essere commesso a vantaggio dell'ente laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte del fornitore dell'ente o al fine di contestare il corretto adempimento delle obbligazioni da parte del fornitore.

Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (art. 635 ter c.p.)

Tale reato si realizza quando un soggetto *"commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici 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 base è aumentata se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

Secondo il D.lgs. n. 7 del 15 gennaio 2016 la pena base è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di pubblico ufficiale/incaricato di pubblico servizio o di operatore del sistema.

Questo delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati alla soddisfazione di un interesse di natura pubblica.

Perché il reato si integri è, inoltre, sufficiente che si tenga una condotta finalizzata al deterioramento o alla soppressione del dato.

Danneggiamento di sistemi informatici o telematici (art. 635 *quater* c.p.)

Questo reato si realizza quando un soggetto mediante le condotte di cui all'art. 635-bis (danneggiamento di dati, informazioni e programmi informatici), 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.

La pena prevista per il reato base, ovvero la reclusione da due a sei anni, è aumentata in due casi:

- 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;
- se il colpevole per commettere il fatto usa minaccia o violazione ovvero se è palesemente armato.

Si tenga conto che qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635 *bis* c.p.

Il reato si integra in caso di danneggiamento o cancellazione dei dati o dei programmi contenuti nel sistema, effettuati direttamente o indirettamente (per esempio, attraverso l'inserimento nel sistema di un virus).

Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635 *quinques* c.p.)

Questo reato sanziona chi, mediante le condotte di cui all'art. 635 *quater* (danneggiamento di informazioni, dati e programmi informatici), ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento". Tale reato è punito con la pena della reclusione da due a sei anni

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di informazioni, dati e programmi informatici pubblici o di pubblico interesse (art. 635 *ter* c.p.), quel che rileva è che il sistema sia utilizzato per il perseguimento di un pubblico interesse indipendentemente dalla proprietà privata o pubblica del sistema stesso.

Il reato si può configurare nel caso in cui un dipendente cancelli file o dati, relativi ad un'area per cui sia stato abilitato ad operare, per conseguire vantaggi interni (ad esempio, far venire meno la prova del credito da parte di un ente o di un fornitore) ovvero che l'amministratore di sistema, abusando della sua qualità, ponga in essere i comportamenti illeciti in oggetto per le medesime finalità già descritte.

F.1.6 Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635 *quater*. 1. c.p.)

Questa fattispecie di reato è stata anch'essa inserita dall'art. 16 della l. 28 giugno 2024, n. 90 per incriminare la fase "preparatoria" dei reati sopra descritti. Viene, infatti, punito chi *"allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero 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, abusivamente si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici"*.

Si tratta di un reato di pericolo, che anticipa la soglia di tutela alla mera disponibilità e circolazione di strumenti potenzialmente dannosi, senza richiedere un effettivo danneggiamento del sistema.

F.1.7 Estorsione (art. 629, comma 3, c.p.)

Il comma 3 dell'art. 629 è stato aggiunto dall'art. 16 della l. 28 giugno 2024, n. 90 e introduce una forma di estorsione commessa mediante strumenti informatici o telematici (c.d. "estorsione informatica"), distinta dall'ipotesi base e con un autonomo trattamento sanzionatorio.

Chiunque, mediante le condotte di accesso o interferenza illecita con sistemi o dati informatici (artt. 615 *ter*, 617 *quater*, 617 *sexies*, 635 *bis*, 635 *quater* e 635 *quinquies* c.p.) ovvero con minaccia di compierle, costringe taluno a fare o ad omettere qualcosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, risponde di estorsione ai sensi del comma 3.

La struttura resta quella tipica dell'estorsione (costrizione mediante minaccia, profitto ingiusto, danno patrimoniale), ma la minaccia consiste nel porre in essere o nel prospettare specifici illeciti informatici, come l'accesso abusivo, l'intercettazione di comunicazioni o il danneggiamento di sistemi e dati.

F.1.8 Falsità in documenti informatici (art. 491 *bis* c.p.)

L'art. 491 *bis* c.p. disciplina le falsità commesse su documenti informatici, stabilendo che, se una delle falsità previste nel capo III del titolo VII (falsità in atti) riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le regole proprie degli atti pubblici, con il relativo trattamento sanzionatorio.

F.1.9 Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 *quinquies* c.p.)

Questo reato si configura quando il soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Questo reato può essere integrato da parte dei certificatori qualificati o meglio i soggetti che prestano servizi di certificazione di firma elettronica qualificata.

Pur essendo rubricata come frode informatica questa ipotesi di reato prescinde completamente da qualsiasi requisito di fraudolenza e consiste nella violazione degli obblighi stabiliti dall'articolo 32 del Codice dell'Amministrazione Digitale (d.lgs. 7 marzo 2005, n. 82).

Si tratta di un reato a dolo specifico e, pertanto, il soggetto che presta servizi di certificazione deve agire al fine di procurare a sé o ad altri un profitto ovvero di arrecare un danno ad un terzo.

F.1.10 Violazione delle norme in materia di perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D. L. 21 settembre 2019, n. 105)

Il reato previsto all'art. 1, comma 11, del D.L. 21 settembre 2019, n. 105 (conv. in L. 133/2019), punisce una serie di condotte volte ad ostacolare o condizionare procedure legate alla sicurezza cibernetica nazionale.

Il testo della norma recita come segue: *“Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni.”*

Si tratta di un illecito penale contravvenzionale che sanziona in estrema sintesi due categorie di condotte tipiche:

- la fornitura di indicazioni, informazioni, elemento o dati non veritieri
- l'omissione di comunicazioni entro i termini di dati, informazioni o elementi di fatto.

Ai fini della commissione del reato non basta la semplice falsità od omissione, ma tali condotte devono essere intenzionate dallo scopo di ostacolare o condizionare procedure amministrative previste per la sicurezza cibernetica e la protezione nazionale.

F.2 Attività sensibili

ATTIVITA' SENSIBILI	FASI	FUNZIONI INTERESSATE
Attività svolte attraverso l'impiego di sistemi e programmi informatici.	Acquisizione e installazioni di programmi informatici	Tutte le funzioni che hanno accesso a strumenti informatici e/o telematici aziendali
Controllo accessi al sistema informatico	Attività tramite l'utilizzo di una rete aziendale del servizio di posta elettronica e accesso a internet	
	Gestione degli accessi da/ e verso l'esterno	
	Gestione della rete informatica	
Accesso a dati informatici e telematici	Gestione di sicurezza dei dispositivi di memorizzazione	
	Gestione del trattamento e archiviazione dei documenti elettronici	

F.3 Sistema di controllo

I delitti hanno come presupposto la sicurezza e l'utilizzo della rete informatica intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi e precisamente:

- Tutte le attività aziendali svolte dal personale tramite l'utilizzo della rete aziendale, del servizio di posta elettronica e accesso ad Internet;
- Gestione della rete informatica aziendale, evoluzione della piattaforma tecnologica e applicativa IT nonché la sicurezza informatica;
- Erogazione di servizi di installazione e servizi professionali di supporto al personale (ad esempio, assistenza, manutenzione, gestione della rete, manutenzione e security);
- La sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati (sicurezza nazionale cibernetica).

F.3.1 Principi generali di comportamento

In generale, la prevenzione dei crimini informatici è svolta attraverso adeguate misure tecnologiche, organizzative e normative ed in particolare almeno attraverso l'applicazione dei seguenti controlli di carattere generale:

- Obbligo per i destinatari di adottare regole di condotta conformi a quanto prescritto nella presente Parte Speciale, nonché a quanto previsto dal Codice Etico e dalle procedure aziendali al fine di impedire il verificarsi dei reati trattati;
- Rispettare la normativa privacy (d.lgs. n.196/2003, Reg. UE 2016/679; D.lgs.101/2018);
- Predisposizione di adeguati strumenti e procedure atti a prevenire e/o impedire la realizzazione di reati informatici da parte dei dipendenti;
- Adottare idonee misure di sicurezza per garantire la sicurezza fisica e tecnologica dei pc, dei sistemi informatici/telematici e dei software (es: sistemi di rilevazione di incendi/gas; installazione periodica di antivirus, firewall, etc.);
- Predisposizione di programmi di formazione, informazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;
- Sottoscrizione da parte di consulenti/partners esterni ed della ditta che presta servizi informatici di specifica "Clausola 231", che li vincolino al rispetto del MOG e del Codice Etico adottato dalla Società.

In particolare, si elencano qui di seguito le regole che devono essere rispettate dalla società e dai dipendenti e dagli altri soggetti autorizzati nell'ambito delle Attività Sensibili:

- I dati e le informazioni non pubbliche, relative anche a clienti e terze parti (commerciali, organizzative, tecniche), incluse le modalità di connessione da remoto, devono essere gestiti come riservati;
- Possono accedere al server aziendale, di proprietà della società, solo i soggetti espressamente autorizzati ed in possesso di account e credenziali associate al PC;
- È vietato introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione;
- È vietato in qualunque modo modificare la configurazione di postazioni di lavoro fisse o mobili;
- È vietato acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);
- È vietato ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla società;
- È vietato divulgare, cedere o condividere con personale interno o esterno all'azienda le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- È vietato accedere ad un sistema informatico altrui (anche di un collega) e manomettere ed alterarne i dati ivi contenuti;
- È vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- È vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi;
- È vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei propri compiti lavorativi;
- È vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- È vietato comunicare a persone non autorizzate, interne o esterne alla società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
- È proibito distorcere, oscurare sostituire la propria identità e inviare e-mail riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati;
- È vietato lo spamming come pure ogni azione di risposta allo spam.

F.3.2 Regole specifiche di comportamento

Al fine di prevenire la commissione delle predette ipotesi criminose Unirock deve attenersi alle seguenti regole di condotta:

- autenticazione e autorizzazione dell'utente, che può accedere esclusivamente mediante l'inserimento di username e password;
- tracciamento di tutte le operazioni che l'utente sta compiendo sul sistema;
- accesso alla rete dall'esterno tramite VPN (La connessione mediante VPN garantisce che l'attività sul web sia criptata e l'indirizzo IP mascherato, impedendo che terzi possano intercettare o monitorare l'attività su internet, inclusi cronologia di navigazione, file scaricati, dati privati o password).

La sicurezza digitale è inoltre garantita dall'adozione di procedura e specifiche istruzioni operative sull'utilizzo dei sistemi informatici in ordine a:

- Utilizzo del Personal Computer
- Utilizzo della rete
- Gestione delle Password
- Utilizzo dei supporti magnetici
- Utilizzo PC portatili
- Uso della posta elettronica
- Uso della rete Internet e dei relativi servizi
- Osservanza delle disposizioni in materia di Privacy

Tra le misure di protezione si indicano a titolo esemplificativo e non esaustivo:

- Backup dei dati sia fisico tramite unità di backup criptata che tramite cloud gestito dall'operatore telefonico;
- Utilizzo di password;
- Installazione antivirus su ciascun PC;
- Adozione di procedure per la conservazione di dati;
- Declinazione misure di sicurezza fisica e procedura di archiviazione dei documenti;
- Attività di formazione a favore degli addetti.
- Adozione misure previste da GDPR 2016/679, D.Lgs. 196/2003 e s.m.i.

Tutte le aree individuate come aree a rischio sono presidiate da procedura / istruzioni operative / norme di comportamento la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'Odv affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

In particolare, occorre osservare la procedura aziendale Gestione Amministrativa, il Manuale Operativo Privacy e le istruzioni operative in esso contenute.

PARTE SPECIALE “G”

REATI DI RICETTAZIONE, RICICLAGGIO ED IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ’ AUTORICICLAGGIO (art. 25 *octies* d.lgs. 231/2001)

REATI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (art. 25 *octies* 1 d.lgs. 231/2001)

G.1 Descrizione delle fattispecie

Il decreto legislativo 21/2007, nel dare attuazione alla direttiva 2005/60 CE del Parlamento e del Consiglio d’Europa concernente la prevenzione dell’utilizzo del sistema finanziario a scopo di riciclaggio, ha operato un riordino della normativa antiriciclaggio presente nell’ordinamento giuridico italiano e ha introdotto nel D. lgs. 231/2001 l’art. 25 *octies*, che prevede la responsabilità degli enti per i reati di riciclaggio, ricettazione e impiego di denaro, beni o altre utilità di provenienza illecita. Il legislatore ha quindi disposto l’abrogazione dei commi 5 e 6 dell’art. 10 della Legge 146/2006 in materia di contrasto del crimine organizzato transnazionale. Di conseguenza, ai sensi dell’art. 25 *octies*, come inserito con il d.lgs. 21/2007, l’Ente è punibile per i reati previsti dagli articoli 648 c.p., 648 *bis* c.p. e 648 *ter*, 648 *ter* 1 c.p.

La Legge 186/2014 entrata in vigore il 1 gennaio 2015 ha aggiunto ai reati indicati quello di autoriciclaggio, introdotto nell’ordinamento italiano dalla Legge menzionata con l’art. 648-ter.1.

Si evidenzia inoltre che l’art. 1 del d.lgs. 195/2021, relativo alla “*Lotta al riciclaggio mediante diritto penale*” - attuativo della Direttiva Riciclaggio (UE) 2018/ 1673 - ha modificato i reati di ricettazione (art. 648 c.p.), riciclaggio (art. 648 *bis* c.p.), impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.), autoriciclaggio (art. 648 *ter*.1 c.p.), contemplati dall’art. 25 *octies* del d.lgs. 231/01. In particolare, è stato esteso il novero delle attività criminose da cui derivano i beni riciclati che, d’ora in poi, potranno provenire non più solo da fattispecie delittuose dolose, ma anche contravvenzionali e, nel caso di riciclaggio e autoriciclaggio, anche da delitti colposi. A tal riguardo si precisa che i reati contravvenzionali idonei a formare presupposto dei reati di ricettazione, riciclaggio, reimpiego e autoriciclaggio, sono circoscritti a quei reati puniti con l’arresto superiore nel massimo a un anno o nel minimo a sei mesi.

G.1.1. Ricettazione (art. 648 c.p.)

Tale ipotesi di reato si configura nel caso in cui un soggetto, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta danaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare.

L’interesse tutelato dall’art. 648 è inteso sia, in via immediata, ad evitare che una qualsiasi attività criminosa diventi fonte di successivi profitti sia, in via mediata, a limitare all’origine la spinta all’attività delittuose.

L’elemento oggettivo del reato consiste nella ricezione che è formula comprensiva di qualsiasi conseguimento di possesso della cosa proveniente da reato e quindi va inteso come comprensivo di ogni negozio, oneroso o gratuito, idoneo al trasferimento della cosa nella sfera patrimoniale dell’acquirente o, comunque, nel possesso dell’acquirente.

Il termine ricevere indica ogni forma di conseguimento del possesso del bene proveniente da reato anche se solo temporaneo.

Per occultamento si intende il nascondimento del bene proveniente dal reato dopo averlo ricevuto.

Il profilo richiesto dalla norma comprende ogni forma di utilità o vantaggio anche temporaneo che possa ricavarsi dal possesso della cosa.

La ricettazione è reato istantaneo che si consuma nel momento in cui l'agente consegue il possesso della cosa e quindi nell'ipotesi di acquisto si consuma nel momento dell'accordo della cosa e sul prezzo mentre nell'ipotesi della intromissione si consuma per il solo fatto di essersi intromesso allo scopo di far acquistare – ricevere – occultare il compendio furtivo senza che sia necessario che l'interessamento raggiunga il fine propostosi dall'agente.

L'elemento soggettivo richiesto dall'art. 648 c.p. è la consapevolezza in capo all'agente circa l'illecita provenienza della cosa.

La conoscenza della provenienza delittuosa può desumersi da qualsiasi elemento, anche indiretto: così dal comportamento dell'imputato che dimostri la certezza dell'origine illecita delle cose ricettate, sulla base dell'omessa o non attendibile indicazione della provenienza della cosa ricevuta, dal comportamento dell'agente successivo all'acquisto, dalle modalità dell'acquisto, dalla natura delle cose, dalla qualità o condizione del venditore.

G.1.2 Riciclaggio (art. 648 *bis* c.p.)

Tale ipotesi di reato si configura nel caso in cui, fuori dall'ipotesi di concorso, un soggetto 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.

Per riciclaggio si intende ogni attività diretta a far perdere al denaro oppure a beni o altre utilità economiche di provenienza criminosa la riconoscibilità della loro origine illecita e/o ad immetterli nel ciclo economico-finanziario, investendoli in iniziative economiche lecite con il pericolo di alterare i meccanismi di mercato.

Il compito di reprimere i fatti di riciclaggio è affidato soprattutto all'art. 648 *bis* e 648 *ter* collocati all'interno del titolo codicistico dedicato ai reati contro il patrimonio.

I proventi riciclabili sono costituiti da “denaro, beni o altra attività” ricomprendendo pertanto ogni vantaggio economico derivante da reato.

Le condotte rilevanti per la configurazione del reato sono tutte tipicizzate da un requisito comune perché devono essere realizzate in modo da ostacolare l'identificazione della provenienza criminosa dell'oggetto.

Per quanto riguarda l'elemento soggettivo l'art. 648 *bis* richiede la consapevolezza della provenienza criminosa dell'oggetto del riciclaggio e la volontà di ostacolare, con una condotta idonea, l'identificazione della provenienza.

Il secondo comma dell'art. 648 *bis* c.p. prevede una aggravante quando “*il fatto è commesso nell'esercizio di una attività professionale*”.

G.1.3 Impiego di denaro, beni e utilità di provenienza (art. 648 *ter* c.p.)

Tale ipotesi di reato si configura nel caso di impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti dai casi previsti dagli articoli 648 e 648 *bis*.

L'art. 648 *ter* tutela l'ordine economico che potrebbe essere turbato dall'immissione nel mercato di beni e soprattutto di capitali di provenienza illecita alterando la libera concorrenza.

La condotta richiesta per l'integrazione del reato consiste nell'impiego di proventi illeciti in attività economiche o finanziarie.

Sono da considerare economiche o finanziarie tutte quelle attività, anche di intermediazione, riguardanti la produzione o la circolazione di beni o di servizi oppure la circolazione di denaro o di valori mobiliari.

Considerato l'utilizzo del termine “impiegare” da parte del legislatore, la norma punisce ogni forma di utilizzazione di capitali illeciti con l'unica specificazione che l'impiego deve avvenire con riguardo ad attività economiche o finanziarie.

Il legislatore ha quindi inteso punire il comportamento consistente nell'adoperare i capitali illeciti in un'attività economica o finanziaria, a prescindere da qualsiasi obiettivo o risultato utile per l'agente e sul solo presupposto che lo stesso possa soggettivamente prevedere che l'impiego di capitale in qualche modo gli convenga.

La norma non fa riferimento al soggetto che opera ma al settore nel quale viene fatto l'investimento, pertanto il reato non ha limitazioni di ordine soggettivo perché risulta punibile sia chi direttamente impiega o propone l'impiego di denaro sia chi è incaricato dell'impiego di tale capitale sempre che ci sia la consapevolezza della provenienza dei beni dai delitti espressamente indicati.

G.1.4 Autoriciclaggio (art. 648 *ter* 1 c.p.)

Si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo commesso o concorso a commettere un delitto, impiega, sostituisce, 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.

Fino alla introduzione della L. 186/14, il legislatore aveva configurato le condotte di ricettazione, riciclaggio e impiego di denaro, beni o altre utilità di provenienza illecita come reati contestabili solo a soggetti diversi dall'autore del reato presupposto. La novità della L. 186/14 sta nel punire colui che dopo aver commesso o concorso a commettere un delitto o una contravvenzione impiega, sostituisce o trasferisce in attività economiche, finanziarie, imprenditoriali o speculative, denaro, beni o altre utilità provenienti dalla commissione di tale delitto o contravvenzione, in modo da ostacolare concretamente l'identificazione della loro provenienza illecita.

La responsabilità degli Enti, con riguardo al reato di autoriciclaggio si configura in tutti i casi in cui, a seguito di un delitto o di una contravvenzione, l'Ente impieghi le utilità che ne derivano per lo svolgimento della propria attività. In generale quindi tutti i reati commessi nell'interesse o a vantaggio dell'Ente che generano un'utilità possono essere considerati astrattamente presupposto del reato di autoriciclaggio.

Poiché le aree ritenute a rischio per questa parte speciale riguardano i flussi finanziari della Società in entrata ed in uscita, si richiamano anche i reati presupposto ricompresi nell'art. 25 *octies* 1 del d.lgs. 231/2001 .

Il d.lgs. 184/2021 ha, infatti introdotto le fattispecie delittuose che seguono in attuazione della Direttiva (UE) 2019/713 finalizzata a disincentivare le frodi e le falsificazioni dei mezzi di pagamento diversi dai contanti. Si riportano tra gli altri,

G.1.5 Indebito utilizzo e falsificazione di strumenti di pagamenti diversi dai contanti (art. 493 *ter* c.p.)

La norma punisce chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti.

L'ipotesi di reato in oggetto si configura, tra l'altro, in caso di utilizzo illecito di carte di credito e punisce chi le falsifica o le cede a terzi. Dalla lettura della norma in commento è punito parimenti chi si avvale di carte di credito di cui non è titolare e chi falsifichi tali carte di credito, in entrambi i casi sempre al fine di trarne profitto. In tale ultimo caso è punita anche la cessione delle carte falsificate ed ogni altra condotta atta a metterle comunque in circolazione.

G.1.6 Frode informatica (art. 620 *ter* c.p.)

Il reato di frode informatica è presente nel novero dei reati presupposto nelle due diverse e distinte ipotesi e precisamente (i) nell'art. 24 del d.lgs. n. 231/2001 qualora il danno sia commesso in danno dello Stato o di altro ente pubblico o dell'Unione Europea (cfr parte speciale A), ovvero (ii) nell'art. 25 *octies*.1 qualora commesso in danno di privati e sussista l'aggravante di un fatto illecito che abbia prodotto un trasferimento di denaro, di valore monetario o di valuta virtuale.

G.1.7 Trasferimento fraudolento di valori (art. 512 *bis* c.p.)

La norma punisce *“chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648 bis e 648 ter”*.

La Legge 9 ottobre 2023 n. 137 ha modificato l'art.25 *octies*.1 del d.lgs. 231/2001 introducendo un nuovo comma 2 *bis* che estende la responsabilità amministrativa dell'ente alla commissione del delitto di cui all'art. 512 *bis* c.p.

L' articolo del Codice penale è stato successivamente ampliato con il secondo comma dalla legge 56/2024 che prevede la medesima sanzione disposta al comma 1 per chi *“al fine di eludere le disposizioni in materia di documentazione antimafia, attribuisce fittiziamente ad altri la titolarità di imprese, quote societarie o azioni ovvero di cariche sociali, qualora l'imprenditore o la società partecipi a procedure di aggiudicazione o di esecuzione di appalti o di concessioni”*.

L'elusione fraudolenta della documentazione antimafia interessa anche la responsabilità degli Enti in quanto l'art. 25 *octies*.1 del d.lgs. 231/01 rinvia in blocco a tutto il testo dell'art. 512 *bis* c.p.

G.2 Attività sensibili

ATTIVITA' SENSIBILI	FASI	FUNZIONI INTERESSATE
Gestione attività amministrative, economiche e finanziarie	Gestione Ciclo attivo	AU Resp amm Dirigenti del ex art. 16 Dlgs.81/08 Commercialista incaricato
	Gestione Ciclo attivo	
	Gestione flussi finanziari /conti correnti	
	Gestione Note spese	
	Scelta fornitori/consulenti	
	Sponsorizzazioni/donazioni	
Gestione adempimenti dichiarativi periodici, fiscali, tributari e calcolo imposte	Registrazioni informazioni contabili	AU Resp Amm Dottore Commercialista Revisori Legali
	Rilevazione, aggregazione e trasmissione dati fiscalmente rilevanti	
	Controlli revisori legali	
	Determinazione risultato fiscale e predisposizione dichiarazioni	
	Versamento imposte, trasmissione documentazione Amm. Finanziaria e conservazione documentale	
	Rapporti Amministrazione finanziaria	
Redazione del bilancio	Redazione del progetto di bilancio	AU Dottore Commercialista Revisori Legali
	Redazione della relazione sulla gestione	

	Consegna del progetto di bilancio e della relazione ai Revisori	
	Deposito del bilancio e dei suoi allegati e delle relazioni degli amministratori	
	Approvazione del bilancio	
	Deposito del bilancio con gli allegati e del verbale di approvazione presso il registro delle imprese	
	Operazioni straordinarie	
Assegnazione di incarichi professionali	Valutazione professionista	AU Resp Amm Commercialista incaricato / Consulente del lavoro/Avvocato
	Formalizzazione incarico professionale	
	Approvazione contratto	
	Controllo avvenuta esecuzione prestazione	

G.3 Sistema di controllo

G.3.1 Principi generali di comportamento

La particolarità dei reati che vengono considerati in questa parte speciale induce a ritenere come aree a rischio tutte quelle nelle quali la Società si occupa di acquisire o impiegare risorse finanziarie. Sono pertanto considerate tali tutte le aree finanza e amministrazione.

I passaggi del denaro, sia in entrata che in uscita, avvengono tramite banche, presso le quali operano AU e Resp. Amm., con debita autorizzazione, che agiscono dopo aver controllato la documentazione sottostante all'operazione.

Ogni movimentazione finanziaria è pertanto tracciata, i documenti sono archiviati e conservati per ogni controllo si rendesse necessario.

Apposita procedura regola l'attività nelle aree a rischio

Nell'espletamento di ogni attività nell'ambito aziendale, e più specificamente nello svolgimento delle attività considerate a rischio, i Destinatari dovranno attenersi ai principi indicati nel Codice Etico di Unirock S.r.l. , nel Modello Organizzativo e alle procedure/istruzioni operative vigenti.

In particolare, la Società impone specificamente a tutti i Destinatari di attenersi ai seguenti principi:

- astenersi da comportamenti tali da integrare alcuna violazione di legge, ivi includendo le fattispecie di reato sopra descritte;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé violazioni di legge, ovvero fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarle;
- astenersi dal procedere a qualsivoglia transazione ed operazione relativa a somme di denaro o beni qualora vi siano, nelle circostanze dell'operazione o nelle caratteristiche della controparte, elementi che lascino supporre la provenienza illecita dei beni e del denaro in questione;
- tenere un comportamento corretto, trasparente, nel rispetto delle norme di legge e delle procedure/istruzioni interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori, clienti e *partners* commerciali, anche stranieri;
- rifornirsi di beni e servizi solo attraverso il ricorso ai fornitori selezionati ;
- selezionare i fornitori dopo avere raccolto informazioni sulle qualità e le caratteristiche degli stessi (si potrà fare riferimento anche ad ulteriori indici e parametri quali, a titolo esemplificativo, la presenza o meno di certificazioni);
- selezionare ed identificare i clienti valutandone in maniera continuativa l'operato e le caratteristiche;

- non intrattenere rapporti commerciali con fornitori/clienti/partner dei quali sia conosciuta o sospettata l'appartenenza diretta od indiretta ad organizzazioni criminali o comunque operanti al di fuori della liceità;
- registrare ogni movimentazione bancaria nei sistemi informativi utilizzati;
- gestire la trasparenza, la tracciabilità e la correttezza dei documenti contabili e dei relativi flussi finanziari.

È fatto divieto in particolare di:

- acquistare beni o servizi verso un corrispettivo palesemente inferiore al valore di mercato di tali beni o servizi, senza avere prima effettuato le necessarie verifiche sulla loro provenienza;
- acquistare beni o servizi da fornitori che non siano registrati nell'anagrafica della Società;
- effettuare il trasferimento di denaro, beni o altra utilità quando vi sia sospetto che essi provengano da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita degli stessi beni;
- effettuare o ricevere pagamenti in contanti, salvo che si tratti di somme al di sotto dei limiti di legge e comunque di modico valore;
- effettuare operazioni che possano apparire volte a mascherare l'origine illecita di denaro, beni o altre utilità;
- utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
- effettuare operazioni che possano apparire volte a rimettere capitali, oggetto di riciclaggio, nel sistema economico.

G.3.2 Regole specifiche di comportamento

Al fine di prevenire la commissione delle predette ipotesi criminali Unirock deve attenersi alle seguenti regole di condotta:

- a) Verificare dell'attendibilità commerciale e professionale di partner commerciali/finanziari sulla base di alcuni indici rilevanti al fine di controllarne l'affidabilità anche sotto il profilo delle transazioni economiche con gli stessi. Ad es. verifica circa l'esistenza di dati pregiudizievoli pubblici come protesti, procedure concorsuali o acquisizione di informazioni commerciali sulla azienda, sui soci e sugli amministratori o quantomeno verifica dei requisiti a contrarre di ordine generale;
- b) monitorare nel tempo il permanere in capo ai fornitori dei requisiti di affidabilità, correttezza, professionalità e onorabilità;

- c) i contratti con i fornitori e i partner devono essere definiti per iscritto in tutte le loro condizioni e termini;
- d) in occasione della stipulazione di contratti con fornitori e *partners*, questi ultimi devono dichiarare:
 - 1. di essere a conoscenza della normativa di cui al Decreto;
 - 2. di impegnarsi al rispetto del Decreto;
- e) controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso i terzi. Tali controlli tengono conto della sede legale della società controparte; degli istituti di credito utilizzati e di eventuali schermi societari o strutture fiduciarie;
- f) verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti contrattuali e tra versamento ed esatto importo oggetto dell'accordo contrattuale;
- g) verificare che i pagamenti sia effettuato tramite bonifico bancario, tranne nei casi strettamente necessari, in modo che sia garantita la tracciabilità;
- h) verifiche sulla contabilità in ordine al rispetto delle soglie per i pagamenti per contanti;
- i) assicurare che pagamenti o rimborsi di spese, compensi, note di accredito o la riduzione in qualsiasi forma della somma dovuta in favore di soggetti interni o soggetti esterni avvengano solo qualora trovino adeguata giustificazione nel rapporto contrattuale con essi costituito; siano attuati in corrispettivo di beni, servizi, prestazioni effettivamente ricevute dalla Società e siano supportati da giustificativi idoneamente documentati;
- j) verificare che il pagamento sia effettuato esclusivamente sul conto corrente indicato nel contratto o nella relativa documentazione contabile ed a favore della controparte contrattuale, essendo esclusa la possibilità di effettuare pagamenti su conti cifrati, intestati a soggetti terzi, in un paese diverso rispetto a quello delle parti contraenti o a quello di esecuzione del contratto;
- k) registrazione e conservazione dei dati relativi alle transazioni;
- l) previsione ed attuazione di presidi per la protezione dei sistemi informatici nei processi/attività interessate, in particolare per l'accesso al sistema contabile ed al sistema bancario limitato ai soggetti autorizzati (AU, Resp. Amm. , Dottore Commercialista Incaricato)
- m) verifica della congruità economica di eventuali investimenti rispetto ai prezzi medi di mercato, utilizzo di professionisti di fiducia per le operazioni.

Tutte le aree individuate come aree a rischio sono presidiate da procedure e/o istruzioni operative la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'OdV affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si riportano di seguito le procedure aziendali da seguire nelle aree di attività a rischio individuate nella presente Parte Speciale: la procedura aziendale Gestione Amministrativa, il Manuale Operativo Privacy e le istruzioni operative in esso contenute.

PARTE SPECIALE “H” REATI DI CRIMINALITÀ ORGANIZZATA (art. 24 *ter* d.lgs. 231/2001)

H.1 Descrizione delle fattispecie normative

Si definiscono reati di criminalità organizzata (o crimine organizzato) quelli scaturiti da attività criminose commesse da particolari tipi di organizzazioni, definite organizzazioni criminali, non costituite in maniera fortuita per la commissione estemporanea di reati, ma organizzate in maniera relativamente stabile con uno schema gerarchico e con un obiettivo comune.

Solitamente lo scopo ultimo di tali organizzazioni è il profitto economico, ma nell'accezione possono essere considerati gruppi come le organizzazioni terroristiche, che sono invece di matrice politica, ideologica o sociale.

I reati transnazionali che ai fini della presente legge si considerano tali qualora sia coinvolto un gruppo criminale organizzato, nonché:

- sia commesso in più di uno Stato;
- sia commesso in uno Stato, ma una parte della sua preparazione, direzione o controllo avvenga in un altro Stato;
- ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- ovvero sia commesso in uno Stato, ma abbia effetti sostanziali in un altro Stato.

H.1.1 Associazione per delinquere (art. 416 , comma 6, c.p.)

La norma punisce la condotta di tre o più persone che si associano allo scopo di commettere più delitti. È punita in particolare non solo la promozione, la costruzione o l'organizzazione dell'associazione, ma anche la semplice partecipazione alla stessa.

Pene più severe sono previste per il caso in cui gli associati ricorrano all'uso di armi e nell'ipotesi in cui gli associati siano dieci o più.

Infine il comma 6 della norma, richiamato dall'art. 24 *bis* comma 1 del Decreto, prevede ulteriori inasprimenti della pena prevista nel caso in cui l'associazione sia diretta a commettere uno dei delitti di cui agli artt. 600 (riduzione o mantenimento in schiavitù o in servitù), 601 (tratta di persone) e 602 c.p. (acquisto e alienazione di schiavi), nonché all'art. 12, comma 3 *bis*, del Testo Unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al D.lgs. 25 luglio 1998 n. 286 (disposizioni contro le immigrazioni clandestine), nonché agli articoli 22, commi 3 e 4, e 22 *bis*, comma 1, della legge 1° aprile 1999, n. 91 (disposizioni in materia di prelievi e di trapianti di organi e di tessuti).

H.1.2 Associazioni di tipo mafioso anche straniere (art. 416 *bis* c.p.)

La norma punisce la condotta di chiunque faccia parte di un'associazione di tipo mafioso formata da tre o più persone.

L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

L'associazione si considera armata quando i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito.

H.1.3 Scambio elettorale politico-mafioso (art. 416 *ter* c.p.)

La norma punisce la condotta di chi ottiene la promessa di voti in cambio dell'erogazione (o della promessa di erogazione) di denaro.

La stessa pena si applica a chi promette, direttamente o a mezzo di intermediari, di procurare voti nei casi di cui al primo comma.

H.1.4 Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 309/90)

La norma punisce la condotta di chi si associa con tre o più persone allo scopo di commettere più delitti inerenti al traffico illecito di sostanze stupefacenti o psicotrope (art. 70, commi 4, 6 e 10 DPR 309/1990).

H.1.5 Illegale fabbricazione, introduzione nello stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi ed esplosivi (art. 407, comma 2, lett. a), n.5 c.p.p.)

La norma sanziona i delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo, escluse quelle previste dall'art. 2, comma 3, della legge 18 aprile 1975, n. 110.

H.2 Attività sensibili

L'associazione a delinquere per così dire comune (art. 416 c.p.) rappresenta una fattispecie amplissima: sarebbe, infatti, un errore pensare che si abbia violazione di questa norma solo nei casi di bande armate o simili. In realtà, la fattispecie è, come detto, integrata ogni volta che tre persone diano vita ad un gruppo che si propone di commettere una serie non precisata di illeciti.

Ciò sta a dire che se più soggetti riferibili alla Società cooperassero per commettere una serie di illeciti a vantaggio della stessa, ben potrebbe esservi la contestazione, oltre a quella dei reati materialmente realizzati (c.d. reati fine dell'associazione) anche del reato di associazione per delinquere.

Ciò equivarrebbe in ogni caso ad un sensibile aggravio della responsabilità amministrativa della Società, che dovrebbe rispondere anche della violazione dell'art. 416 c.p.

Addirittura, potrebbe persino accadere che la commissione, da parte di tre o più soggetti, di delitti non ricompresi tra quelli sanzionati dal Decreto (e che quindi in sé non produrrebbero conseguenze per la società) potrebbe comunque portare alla responsabilità dell'Ente proprio per effetto della violazione dell'art. 416 c.p.

Non vi devono peraltro essere equivoci sotto un diverso profilo: perché si integri il reato non è certo necessario che i membri dell'associazione siano tutti dipendenti o comunque soggetti ricollegabili alla Società. Ben può accadere che il reato sia contestato, quindi, anche nel caso in cui soggetto appartenente ad una Società commetta alcuni illeciti a vantaggio della stessa, avvalendosi o cooperando con due o più soggetti esterni all'Ente: ciò rende certamente rilevanti tutti i rapporti con collaboratori e professionisti esterni, partner commerciali, dirigenti e dipendenti di altre società che, in ipotesi, si trovino a cooperare con Unirock.

Le principali attività sensibili, con riferimento ai reati di criminalità organizzata, che Unirock S.r.l. rilevato al suo interno sono quelle riportate nel presente Modello e quelle che potrebbero comportare un'ipotesi di associazione tra tre o più persone con la finalità di commettere uno dei reati compresi nel D.lgs. 231/2001.

Particolare rilevanza hanno le seguenti attività e funzioni:

ATTIVITA' SENSIBILI	FASI	FUNZIONI INTERESSATE
Gestione partecipazione gare d'appalto ed affidamenti	Ricerca ed acquisizione informazioni gare d'appalto, bandi di gara per appalti di lavori, contratti	AU Resp. Uff. Gare
	Predisposizione, sottoscrizione, trasmissione offerte, tecniche ed amministrative	
	Predisposizione documentazione amministrativa richiesta	
	Aggiudicazione commessa	

Gestione ed esecuzione contratti con enti pubblici	Gestione operativa della commessa	AU
	Controllo stato avanzamento lavori	Resp. Amm.
	Fornitura di beni o servizi	Dirigenti del ex art. 16
	Rendicontazione	Dlgs.81/08
Gestione rapporti con P.A.	Acquisizione informazioni per opportunità commerciali	AU Resp. Uff. Gare Dirigenti del ex art. 16 Dlgs.81/08 Delegati Ambiente e Sicurezza
	Condivisione specifiche tecniche commerciali per presentazioni offerte	
	Esecuzione commessa, controllo operatività cantieri, SAL, fornitura servizi/rendicontazione	
	Interazioni con funzionari, dirigenti, RUP, membri commissione gare P.A.	
	Ispezioni e verifiche da parte della Pubblica Amministrazione	
	Richieste autorizzazioni/ concessioni	
	Richiesta finanziamenti/agevolazioni	
Gestione del personale	Sponsorizzazioni	
	Selezione ed assunzione del personale	AU
	Valutazione dei requisiti	Resp. amm.
Gestione attività amministrative, economiche e finanziarie	Gestione contratti somministrazione	Consulente del lavoro incaricato
	Gestione Ciclo attivo	AU Resp amm Dirigenti del ex art. 16 Dlgs.81/08 Commercialista incaricato
	Gestione Ciclo passivo	
	Gestione conti correnti	
	Gestione Note spese	
	Scelta fornitori/consulenti	
	Predisposizione e redazione del Bilancio d'Esercizio	
	Gestione rapporti con Studi professionali esterni	AU

Gestione degli affari legali	Predisposizione atti e contratti	Resp Amm
	Gestione del contenzioso	Avv/ Consulente incaricato
	Accordi transattivi	
	Operazioni straordinarie	

H.3 Sistema di controllo

H.3.1 Principi generali di comportamento

Unirock S.r.l. si è sempre preoccupata di improntare la propria attività d'impresa a regole generali di condotta volte a garantire, nei rapporti anche tra i dipendenti il rispetto di principi etici e di legalità.

Tutte le procedure e le regole aziendali sono in ogni caso atte ad evitare, impedire e prevenire anche solo il pericolo di commissione di tali reati nell'interesse o a vantaggio dell'Ente.

Tutte le attività e le operazioni svolte per conto di Unirock S.r.l. devono essere improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza, trasparenza, buona fede e tracciabilità della documentazione.

La Società ribadisce l'obbligo da parte dei Destinatari di improntare la propria attività alla scrupolosa osservanza delle regole e procedure esistenti, del Codice Etico e del Modello Organizzativo.

La Società promuove attivamente il rispetto di tali principi anche da parte dei propri collaboratori, fornitori e partner commerciali.

H.3.2 Regole specifiche di comportamento

Al fine di prevenire la commissione delle predette ipotesi criminose Unirock deve attenersi alle seguenti regole di condotta:

- Verifica dell'attendibilità commerciale e professionale di partner commerciali/finanziari sulla base di alcuni indici rilevanti. Ad es. verifica circa l'esistenza di dati pregiudizievoli pubblici come protesti, procedure concorsuali o acquisizione di informazioni commerciali sulla azienda, sui soci e sugli amministratori o quantomeno verifica dei requisiti a contrarre di ordine generale
- i contratti con i fornitori e i partner devono essere definiti per iscritto in tutte le loro condizioni e termini;
- verifica della regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti contrattuali;
- in occasione della stipulazione di contratti con fornitori e *partners*, questi ultimi devono dichiarare:
 - di essere a conoscenza della normativa di cui al Decreto;
 - di impegnarsi al rispetto del Decreto (Clausola 231/01);
- controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso i terzi. Tali controlli tengono conto della sede legale della società controparte; degli istituti di credito utilizzati e di eventuali schermi societari o strutture fiduciarie;
- verifiche sulla contabilità in ordine al rispetto delle soglie per i pagamenti per contanti;

- verifica della congruità economica di eventuali investimenti rispetto ai prezzi medi di mercato, utilizzo di professionisti di fiducia per le operazioni
- verifica per i flussi finanziari in entrata sulla corrispondenza tra ordinante e soggetto destinatario delle prestazioni della Società
- verifica dell'effettività delle prestazioni rispetto alle fatture emesse
- verifica della veridicità delle dichiarazioni rispetto alle scritture contabili
- selezione del personale effettuata sulla base di criteri selettivi che garantiscano la trasparenza della scelta e l'affidabilità e professionalità del candidato

Tutte le attività sensibili delineate e le relative aree di rischio sono presidiate da procedure e/o istruzioni operative la cui violazione è considerata violazione del Modello, per cui deve essere segnalata all'Odv affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

Si richiama la procedura Gestione Amministrativa adottata dalla Società.

PARTE “I” REATI CONTRO L’ATTIVITA’ GIUDIZIARIA (art. 25 *decies* d.lgs. 231/2001)

I.1 Descrizione delle fattispecie normative

La legge n. 116 del 3 agosto 2009 (pubblicata sulla G.U. n. 188 del 14 agosto 2009), "Ratifica ed esecuzione della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione, adottata dalla Assemblea generale dell'ONU il 31 ottobre 2003 con risoluzione n. 58/4, firmata dallo Stato italiano il 9 dicembre 2003, nonché norme di adeguamento interno e modifiche al Codice penale e al codice di procedura penale", all'art. 4 introduce nel d.lgs. 231/01 l'art. 25-*decies* "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria".

I.1.1 Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità 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”.

Tale reato è anche elencato tra quelli transnazionali.

La fattispecie di cui all'art. 377 *bis* c.p. mira a tutelare la genuinità processuale di quanti sono chiamati a riferire fatti di causa davanti all'Autorità Giudiziaria. È un reato di pericolo il cui evento si verifica con la semplice offerta o promessa finalizzata alla falsità giudiziale.

La condotta tipica è costituita sia dall'offerta o dalla promessa di denaro o altra utilità che dalla violenza o minaccia.

La condotta dell'agente è punita a dolo specifico: il subornatore non solo deve avere la coscienza e la volontà dell'offerta o della promessa o della violenza o minaccia, ma deve altresì perseguire il fine di indurre il subornato alla falsità.

Il reato si consuma nel momento e nel luogo in cui l'agente esercita la violenza o la minaccia sulla persona offesa oppure offre o promette il denaro o altra utilità.

I.1.2 Favoreggiamento personale (art. 378 c.p.)

“Chiunque, dopo che fu commesso un delitto per il quale la legge stabilisce la pena di morte o l'ergastolo o la reclusione, e fuori dei casi di concorso nel medesimo, aiuta taluno a eludere le investigazioni dell'Autorità, o a sottrarsi alle ricerche di questa, è punito con la reclusione fino a quattro anni.

Quando il delitto commesso è quello previsto dall'articolo 416 bis, si applica, in ogni caso, la pena della reclusione non inferiore a due anni.

Se si tratta di delitti per i quali la legge stabilisce una pena diversa, ovvero di contravvenzioni, la pena è della multa fino a lire un milione.

Le disposizioni di questo articolo si applicano anche quando la persona aiutata non è imputabile o risulta che non ha commesso il delitto”.

Tale reato rientra nel novero di quelli transnazionali trattati dal d.lgs. 231/01.

L’interesse tutelato dalla norma è assicurare alla giustizia il regolare svolgimento del processo penale.

Nella previsione dell’art. 378 c.p. sono comprese sia le condotte attive sia quelle omissive di per se stesse idonee ad escludere o favorire le investigazioni o ad intralciare o ritardare le ricerche della polizia. La condotta consiste, dunque, nel frapporre un ostacolo, anche se limitato o temporaneo, allo svolgimento delle indagini.

Il reato di favoreggiamento personale di cui all’art. 378 c.p. è a dolo generico e richiede, quale elemento soggettivo, la consapevolezza che la propria condotta si risolva in un aiuto a favore di chi si sa sottoposto alle investigazioni od alle ricerche dell’autorità.

Il reato si perfeziona nel momento in cui il soggetto attivo ha posto in essere la condotta favoreggiatrice.

I.2 Attività sensibili

ATTIVITA' SENSIBILI	FASI	FUNZIONI INTERESSATE
Gestione degli affari legali (civili, penali, giuslavoristici ed amministrativi), contenziosi e transazioni	Predisposizione atti e contratti	AU Avvocato/Dottore Commercialista/Consulente legale incaricato
	Gestione del contenzioso	
	Accordi transattivi	

I.3 Sistema di controllo

I.3.1 Principi di comportamento

Unirock S.r.l. si è sempre preoccupata di improntare la propria attività d'impresa a regole generali di condotta volte a garantire, nei rapporti con fornitori, clienti, partners commerciali e dipendenti, il rispetto di principi etici e di legalità.

Nell'ambito delle attività sopra richiamate e della gestione dei rapporti con soggetti chiamati a rendere dichiarazioni utilizzabili in un procedimento penale in cui è coinvolta la Società, a tutti i destinatari del Modello è fatto divieto di porre in essere comportamenti che possano rientrare nelle fattispecie di reato richiamate nella presente parte speciale.

In particolare, nell'espletamento delle attività considerate sensibili, è fatto obbligo di attenersi ai seguenti principi generali di condotta:

- Divieto di indurre chiunque, attraverso violenza o minaccia o tramite offerta o promessa di denaro o altra utilità, a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità Giudiziaria o ad avvalersi della facoltà di non rispondere, al fine di favorire gli interessi della Società o per trarne altrimenti un vantaggio per la medesima;
- Prestare una fattiva collaborazione e rendere dichiarazioni veritiere ed esaurientemente rappresentative dei fatti nei rapporti con l'Autorità Giudiziaria;
- I destinatari (indagato/imputato, persona informata sui fatti/testimone o teste assistito/imputato in un procedimento penale connesso) chiamati a rendere dichiarazioni innanzi all'autorità Giudiziaria in merito all'attività lavorativa prestata, sono tenuti ad esprimere liberamente la propria rappresentazione dei fatti o ad esercitare la facoltà di non rispondere accordata dalla legge; sono altresì tenuti a mantenere il massimo riserbo relativamente alle dichiarazioni rilasciate ed al loro oggetto, ove le medesime siano coperte da segreto investigativo;
- Obbligo di agire con correttezza evitando qualsiasi comportamento finalizzato ad occultare illeciti;
- Divieto assoluto di distruggere, alterare od occultare documenti, scritture contabili o dati informatici potenzialmente rilevanti per le indagini;
- Divieto di informare soggetti indagati o sottoposti ad indagini sulle attività di controllo in corso da parte della Autorità Giudiziaria;
- Tutti i destinatari devono tempestivamente avvertire il loro Responsabile in azienda di ogni atto di citazione a testimoniare e di ogni procedimento penale che li veda coinvolti, sotto qualsiasi profilo, in rapporto all'attività lavorativa prestata o comunque ad essa attinente.

Unirock assicura, a tutti i destinatari che il fatto della loro collaborazione con gli inquirenti non potrà mai essere fonte di pregiudizio, discriminazione o valutazione negativa da parte dell'azienda.

Si richiamano la procedura aziendale Gestione Amministrativa, il Manuale Operativo Privacy. Ogni violazione delle norme di comportamento previste dalle procedure, istruzioni operative, prassi aziendali è considerata violazione del Modello per cui deve essere segnalata all'O.d.V. affinché provveda al suo accertamento e quindi a valutarne la gravità, proponendo, se del caso, l'applicazione di sanzioni.

PARTE SPECIALE “L” DELITTI CONTRO LA FEDE PUBBLICA (art. 25 *bis* d.lgs. 231/2001)**L.1 Descrizione delle fattispecie normative****L.1.1 Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.).**

La norma punisce le condotte di contraffazione o alterazione di monete nazionali o straniere, di introduzione nello Stato, previo concerto, di monete falsificate, di detenzione, spendita e messa in circolazione o comunque di acquisto o ricezione di moneta falsa allo scopo di metterla in circolazione.

La contraffazione consiste in una imitazione del vero e si realizza creando una specie metallica o una carta di pubblico credito che imiti quelle vere, idonee ad ingannare, dunque spendibili.

L'alterazione di moneta si realizza quando un soggetto altera in qualsiasi modo monete genuine col dare ad esse l'apparenza di un valore superiore o quando un soggetto altera monete genuine scemandone in qualsiasi modo il valore (v. art. 454 c.p.).

Il reato può essere posto in essere da chiunque.

L.1.2. Alterazione di monete (art. 454 c.p.)

È punito chiunque altera monete della qualità indicata nell'articolo precedente, scemandone in qualsiasi modo il valore, ovvero, rispetto alle monete in tal modo alterate, commette alcuno dei fatti indicati nei numeri 3 e 4 del detto articolo.

Il reato punisce la condotta di alterazione di monete.

L.1.3 Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.)

È punito chiunque, fuori dei casi previsti dai due articoli precedenti, introduce nel territorio dello Stato, acquista o detiene monete contraffatte o alterate, al fine di metterle in circolazione, ovvero le spende o le mette altrimenti in circolazione.

Trattasi di figura residuale rispetto a quelle di cui agli artt. 453 e 454 c.p., a cui si rinvia per le nozioni comuni a tale fattispecie.

L.1.4 Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.)

È punito chiunque spende o mette altrimenti in circolazione monete contraffatte o alterate, da lui ricevute in buona fede.

Per configurare il delitto è necessario che l'agente abbia ricevuto monete false in buona fede; però, dopo averle ricevute, l'agente deve rendersi conto della loro falsità e, dolosamente, deve spenderle o metterle in circolazione.

L.1.5 Falsificazione dei valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.)

Il reato si verifica con il compimento su "valori di bollo" quindi rientrano in questa categoria: la carta bollata, le marche da bollo, i francobolli e gli altri valori equiparati a questi da leggi speciali, di operazioni di falsificazione.

Agli effetti della legge penale, s'intendono per valori di bollo la carta bollata, le marche da bollo, i francobolli e gli altri valori equiparati a questi da leggi speciali.

Ai fini di tale fattispecie è necessario che i valori siano ancora in corso o, se fuori corso, ne deve essere ancora consentito il cambio con quelli in corso.

L.1.6 Uso di valori di bollo contraffatti o alterati (art. 464 c.p.)

È punito chiunque, non essendo concorso nella contraffazione o nell'alterazione, fa uso di valori di bollo contraffatto alterati.

Se i valori sono stati ricevuti in buona fede, si applica la pena stabilita nell'articolo 457, ridotta di un terzo.

L'uso penalmente rilevante è quello conforme alla normale destinazione (sono irrilevanti l'uso ornamentale o collezionistico).

Sono, inoltre, ricompresi dall'art. 25 bis d.lgs. 231/2001 i seguenti reati presupposto:

- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.).
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.).
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.).
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

L.2 Attività sensibili

ATTIVITA' SENSIBILI	FASE	FUNZIONI INTERESSATE
Gestione attività economico-finanziarie	Ciclo passivo /attivo	AU Resp Area Amm Delegati ex art. 16 D.Lgs.81/08
	Acquisto e uso di valori di bollo	
	Gestione denaro contante	
	Acquisto e uso di valori di bollo	

L.3 Sistema di controllo

L.3.1 Principi di comportamento

In relazione ai reati di falsità in monete (e valori) le attività ritenute più sensibili risultano essere quelle relative alla gestione dei valori. Infatti, le Aree Sensibili ove si possano configurare i maggiori rischi si possono ipotizzare nelle operazioni di gestione dei valori e ogni attività inerente alla trattazione del denaro e dei valori di qualsiasi natura con particolare riferimento a banconote, monete, valori di bollo aventi corso legale nello Stato e all'estero.

Ciò premesso appare, difficilmente ravvisabile la possibilità che gli Organi Sociali ed i dipendenti di Unirock pongano in essere, autonomamente o in concorso con terzi fatti di falsificazione e di alterazione di monete, di valori di bollo o di carta filigranata in uso per la fabbricazione di carte di pubblico credito.

A ciò deve aggiungersi che, come specificato nelle precedenti parti speciali, la Società nelle proprie attività agisce nel rispetto della legislazione vigente in materia di limitazione all'utilizzo del contante.

Pur considerando il basso profilo di rischio di commissione dei reati della presente parte speciale, si prevedono i seguenti principi generali di comportamento per i Destinatari del Modello:

- Divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate o comunque che possano potenzialmente diventarlo o favorirne la commissione;
- Operare nel trattamento di banconote e monete aventi corso legale nello Stato e all'estero, nella stretta osservanza della legge, dei regolamenti e delle disposizioni interne, con onestà, integrità, correttezza e buona fede;
- Osservare le procedure previste dalla Società in materia di uso dei contanti, ove necessario e di acquisto;
- Immediato ritiro dalla circolazione di monete, banconote e valori di bollo di accertata o sospetta falsità, secondo le modalità previste dalla legge e dal presente Modello;
- Divieto di detenere, ricevere e mettere in circolazione, in buona o mala fede, monete, banconote e marche da bollo falsificate;
- Divieto di mantenere in circolazione, ovvero agevolare la circolazione di monete, banconote e marche da bollo in relazione alle quali si sia acquisita la certezza o si abbia anche solo il sospetto di falsità

Si richiama l'osservanza della procedura Gestione Amministrativa e delle istruzioni operative la cui violazione è considerata violazione del Modello da segnalare tempestivamente all'Organismo di Vigilanza affinché provveda al suo accertamento

PARTE “M”**IMPIEGO DI CITTADINI TERZI IL CUI SOGGIORNO È IRREGOLARE (art. 25 *duodecies* d.lgs. 231/2001)****RAZZISMO E XENOFOBIA (art. 25 *terdecies* d.lgs. 231/2001)****M.1 Descrizione delle fattispecie normative**

La presente sezione si riferisce ai reati in materia di impiego di lavoratori stranieri privi del permesso di soggiorno. Si riporta di seguito la fattispecie contemplata dall'art. 25 *duodecies* del d.lgs. 231/2001, con assai remota possibilità di realizzazione all'interno della realtà aziendale di Unirock S.r.l.

Art. 22 commi 12 e 12 *bis* decreto legislativo 25 luglio 1998, n. 286 (modificato dalla L. 187/24) - Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero :

“12. Il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal presente articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, è punito con la reclusione da sei mesi a tre anni e con la multa di 5000 euro per ogni lavoratore impiegato.

12-bis. Le pene per il fatto previsto dal comma 12 sono aumentate da un terzo alla metà:

- a) se i lavoratori occupati sono in numero superiore a tre;*
- b) se i lavoratori occupati sono minori in età non lavorativa;*
- c) se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di cui al terzo comma dell'articolo 603 bis del Codice penale (condizioni di sfruttamento).”*

L'impiego di cittadini di paesi terzi il cui soggiorno è irregolare è presupposto della responsabilità amministrativa dell'Ente solo se la condotta è aggravata da una delle circostanze contemplate dal comma 12 *bis*.

La presente Parte Speciale si riferisce ai reati di razzismo e xenofobia richiamati dalle disposizioni di cui all'art. 25-*terdecies* del D. Lgs. 231/2001.

Si definisce "razzismo", in senso lato, un atteggiamento di intolleranza sociale che porta un individuo o un gruppo a non accettare l'esistenza di individui e gruppi con modi di pensare e di agire differenti dai propri, mentre il termine “xenofobia” è un'esasperazione dell'etnocentrismo, cioè della propensione a ritenere che gli usi e i costumi della propria comunità (i cui membri possono anche appartenere a razze diverse) siano superiori a quelli di qualsiasi altra e si concreta in un atteggiamento di forte avversione verso i membri delle altre comunità.

Per effetto dell'entrata in vigore della Legge Europea 2017, il novero dei reati che possono generare una responsabilità amministrativa degli enti, si è arricchito con le fattispecie criminose di cui sopra.

In dettaglio, l'art. 25 *terdecies* prevede che:

"1. In relazione alla commissione dei delitti di cui all'articolo 3, comma 3 bis, della legge 13 ottobre 1975, n. 654 (richiamo da intendersi riferito all'articolo 604-bis del Codice penale ai sensi dell'articolo 7 del decreto legislativo 1 marzo 2018 n. 21), si applica all'ente la sanzione pecuniaria da duecento a ottocento quote.

2. Nei casi di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a un anno.

3. Se l'ente o una sua unità organizzativa è stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei delitti indicati nel comma 1, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'articolo 16, comma 3."

L'art. 604 bis c.p., rubricato "Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa" stabilisce che:

"Salvo che il fatto costituisca più grave reato, è punito:

a) con la reclusione fino ad un anno e sei mesi o con la multa fino a 6.000 euro chi propaganda idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi;

b) con la reclusione da sei mesi a quattro anni chi, in qualsiasi modo, istiga a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi.

È vietata ogni organizzazione, associazione, movimento o gruppo avente tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi. Chi partecipa a tali organizzazioni, associazioni, movimenti o gruppi, o presta assistenza alla loro attività, è punito, per il solo fatto della partecipazione o dell'assistenza, con la reclusione da sei mesi a quattro anni. Coloro che promuovono o dirigono tali organizzazioni, associazioni, movimenti o gruppi sono puniti, per ciò solo, con la reclusione da uno a sei anni.

Si applica la pena della reclusione da due a sei anni se 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, sulla minimizzazione in modo grave o sull'apologia 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."

I delitti considerati in questa parte Speciale del Modello riguardano i partecipanti di organizzazioni, associazioni, movimenti o gruppi aventi tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi, nonché la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, fondati in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia - inciso aggiunto dalla stessa Legge Europea - della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra

M.2 Attività sensibili

ATTIVITA' SENSIBILI	FASI	FUNZIONI INTERESSATE
Gestione del Personale	Ricerca e selezione del personale	AU
	Valutazione dei requisiti	Resp Amm
	Gestione del Personale avanzamento di carriera	Consulente del Lavoro incaricato
Affidamento lavori e servizi ad imprese o lavoratori autonomi	Verifica idoneità tecnico professionale del fornitore	AU
	Acquisizione documentazione/certificazioni ex lege	Resp Amm Delegati ex art. 16 D.Lgs. 81/08
	Formalizzazione e stipula del contratto	Consulente legale e del lavoro

M.3 Sistema di controllo

M.3.1 Principi generali di comportamento – Impiego di cittadini terzi il cui soggiorno è irregolare (art. 25 *duodecies* d.lgs. 231/2001)

Nell'ambito delle attività sensibili sopra descritte, le maggiori aree di rischio della commissione di reati previsti dalla presente parte speciale si possono così individuare:

- Conclusione di contratti con imprese che utilizzano personale d'opera non qualificato proveniente da paesi Extracomunitari
- Attività di selezione del personale.

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali aziendali e dei Destinatari, Dipendenti, e Consulenti/Partner nella misura necessaria alle funzioni dagli stessi svolte di:

- Assumere o comunque impiegare lavoratori stranieri privi di regolare permesso di soggiorno.
- Assumere o comunque impiegare lavoratori stranieri il cui permesso di soggiorno sia scaduto e del quale non sia stato chiesto il rinnovo nei termini di legge.
- Assumere o comunque impiegare lavoratori stranieri il cui permesso di soggiorno sia stato revocato o annullato.

In particolare, è fatto obbligo per tutti i Destinatari del Modello di osservare i seguenti principi:

- I lavoratori assunti direttamente a tempo determinato o indeterminato e gli interinali devono fornire copia del codice fiscale, carta di identità, permesso di soggiorno, passaporto e più segnatamente quanto eventualmente indicato nella documentazione consegnata all'aspirante lavoratore al momento della valutazione ai fini dell'assunzione da parte della società;
- Qualora la società si avvalga di somministrazione di manodopera l'azienda chiedere direttamente alla agenzia di somministrazione copia della documentazione relativa alla regolarità del lavoratore;
- Qualora la società si avvalga di ditte appaltatrici per l'esecuzione di lavori da effettuarsi presso stabilimenti propri, l'azienda dovrà chiedere direttamente all'appaltatrice documentazione finalizzata a comprovare la regolarità del lavoratore ivi operanti;
- In tutti i contratti di appalto per l'esecuzione di lavori da effettuarsi presso l'azienda, prevedere l'obbligo a carico della società appaltatrice o del somministratore, di verificare che ogni lavoratore extracomunitario sia munito di regolare permesso di soggiorno in corso di validità;
- Controllo delle aree operative gestite da Unirock S.r.l. per le ditte appaltatrici dell'identità dei lavoratori dipendenti delle stesse, anche attraverso badge di riconoscimento dell'azienda di appartenenza.

Chiunque rilevi una gestione anomala del personale utilizzato dai Partner, è tenuto ad informare immediatamente il proprio Responsabile nonché l'Organismo di Vigilanza di tale anomalia;

M.3.2 Principi generali di comportamento – Razzismo e xenofobia (art. 25 *terdecies* d.lgs. 231/2001)

Considerate le attività svolte da Unirock la probabilità di accadimento dei suddetti reati è considerata remota poiché la propaganda politica e le forme di discriminazione religiosa e razziale sono assolutamente vietate e

condannate sia dalle regole contenute nel Codice Etico che dai principi e dalle linee guida inclusi nel presente Modello.

La Società, inoltre, attua il principio di parità di trattamento fra persone nell'ambito lavorativo e chiede che i partner commerciali ed i clienti rispettino parimenti tale principio.

In astratto, dunque, le attività ritenute più specificamente a rischio potrebbero configurarsi nell'ambito di:

- Conclusione di contratti con imprese che utilizzano personale straniero, di religioni e/o costumi differenti;
- Attività di selezione del personale.

Conseguentemente, è fatto espresso obbligo a carico di tutti i destinatari del Modello di:

- Tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure ed istruzioni operative aziendali interne, in tutte le attività finalizzate all'assunzione di personale ed al suo impiego in Società;
- Assicurare che il processo di assunzione ed impiego sia motivato da effettive necessità aziendali, che sia condotto in maniera trasparente e documentabile e che sia basato su criteri non arbitrari e quanto possibile oggettivi;

Nello specifico è fatto assoluto divieto di:

- Trattare una persona meno favorevolmente di quanto sia, sia stata o sarebbe trattata un'altra in una situazione analoga» a causa della razza, etnia, nazionalità o religione;
- Di dare disposizioni o applicare criteri o prassi apparentemente neutri che possono mettere persone di una determinata razza, etnia, nazionalità o religione in una posizione di particolare svantaggio rispetto ad altre persone, a meno che tale disposizione, criterio o prassi siano oggettivamente giustificati da una finalità legittima e i mezzi impiegati per il suo conseguimento siano appropriati e necessari».

Ogni violazione dei suddetti principi, delle procedure ed istruzioni operative aziendali deve essere tempestivamente segnalata all'Organismo di Vigilanza.